TOWSON UNIVERSITY

OFFICE OF GRADUATE STUDIES

# TOWARDS IMPROVED OFFENSIVE SECURITY ASSESSMENT
# USING COUNTER APT RED TEAMS

by

Jacob G. Oakley

A Dissertation

Presented to the faculty of

Towson University

in partial fulfillment

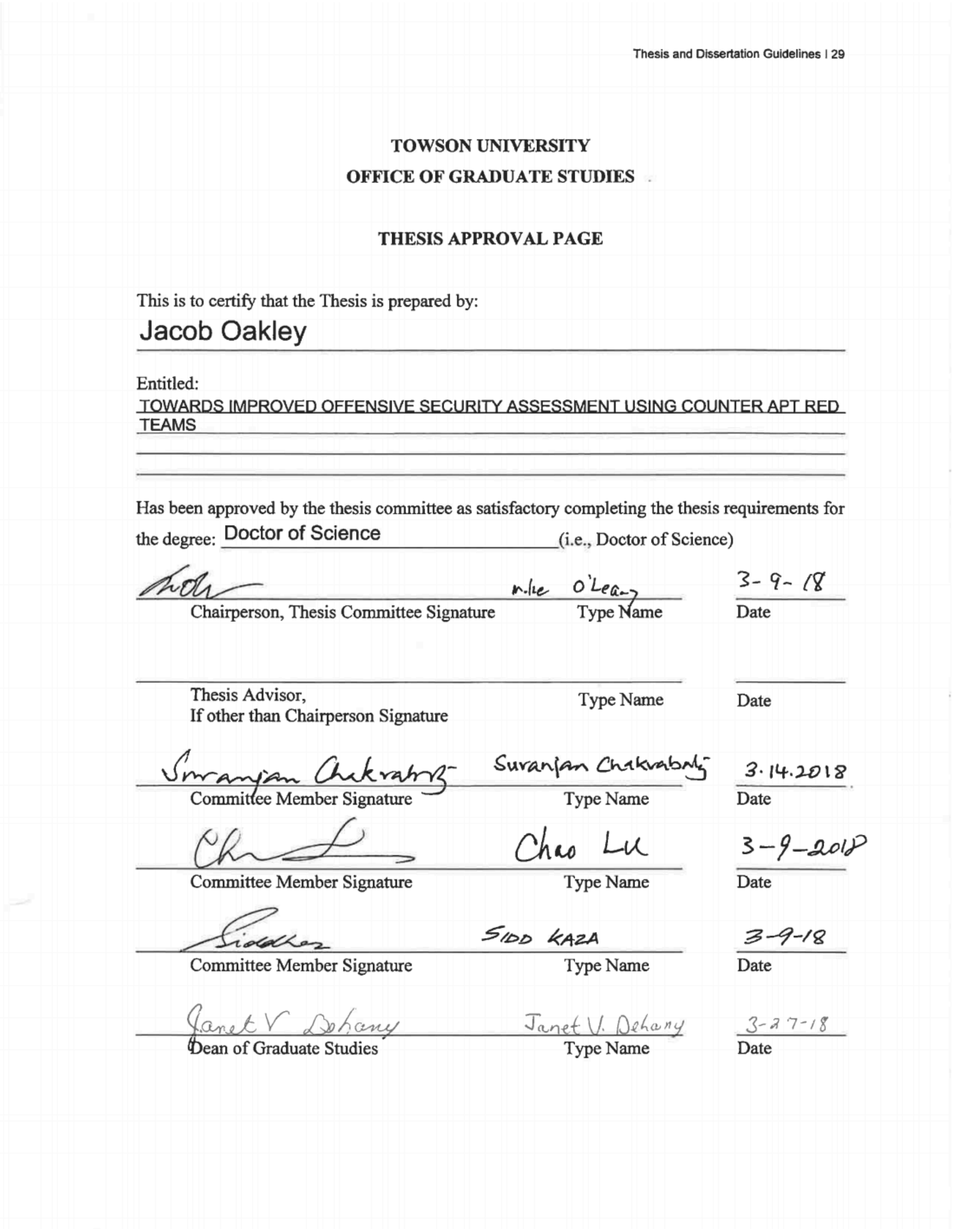
of the requirement for the degree of

Doctor of Science

Department of Computer & Information Sciences

Towson University
Towson, Maryland 21252

May 2018



**TOWSON UNIVERSITY**

**OFFICE OF GRADUATE STUDIES**

**THESIS APPROVAL PAGE**

This is to certify that the Thesis is prepared by:

Jacob Oakley

Entitled:

TOWARDS IMPROVED OFFENSIVE SECURITY ASSESSMENT USING COUNTER APT RED TEAMS

Has been approved by the thesis committee as satisfactory completing the thesis requirements for the degree: Doctor of Science (i.e., Doctor of Science)

Mike O'Leary 3-9-18
Chairperson, Thesis Committee Signature Type Name Date

Thesis Advisor, If other than Chairperson Signature Type Name Date

Suranjan Chakraborty Suranjan Chakraborty 3.14.2018
Committee Member Signature Type Name Date

Chao Lu 3-9-2018
Committee Member Signature Type Name Date

SIDD KAZA 3-9-18
Committee Member Signature Type Name Date

Janet V Dehany Janet V. Dehany 3-27-18
Dean of Graduate Studies Type Name Date

# Abstract

## Towards Improved Offensive Security Assessment Using Counter APT Red Teams

Jacob G. Oakley

Defending against cyber criminals, cyber warfare and cyber terrorism all rely on the mitigation of the motivated advanced persistent threats (APTs) that carry out such campaigns. The only pro-active solution capable of addressing these threats is ethical hacker conducted emulation during offensive security assessments such as penetration testing and red teaming. Many security industry institutions label their products or services as addressing APTs unfortunately there is no agreed upon standard for the proper processes, tradecraft or techniques involved in doing so. Additionally, academic efforts regarding APTs largely focus on reactive monitoring or automated assessment which simulate known attack sequences and do not necessarily represent realistic future attacks. This dissertation aims to provide a standard for addressing APT attacks by counter-APT red teaming (CAPTR teaming). The CAPTR team concept seeks to build upon traditional red team processes to augment the offensive security assessment process. This will allow security practitioners a level playing field to engage and mitigate the threats and vulnerabilities most likely to be leveraged by APTs. Such an assessment counters the outcome of APT breaches by prioritizing vulnerabilities that enable an actor to compromise the data most important to an organization locally and pivoting outwards to points used for access and exfiltration. When an organization identifies critical items that represent unacceptable losses they should be protected as if an actor, regardless of motivation, were intent on compromising them. Adequate identification and protection of critical items via offensive security assessments originating at such positions represents an approach more efficient and capable of mitigating the impact of an APT breach. In a threat landscape with hyper-focused actors it is the responsibility of the security field to provide an equally focused security assessment solution that goes beyond the attack simulations of traditional penetration tests or red team engagements. This dissertation discerns the need and novelty of the CAPTR teaming concept and ratifies the validity of the assessment paradigm through experimentation as well as case study.

## Table of Contents

## Table of Figures

## Table of Tables

# Introduction

Successful cyber-attacks have become increasingly detrimental to victim organizations. In some cases, over 100 Million individuals are affected, and Billions of dollars of damage done. The recent Equifax breach affected 143 Million individuals whose social security numbers and other personal information, in some cases including credit card numbers, were compromised (Haselton, 2017). The company's stock tumbled almost 13% in 24 hours resulting in a loss of nearly 2.275 Billion dollars in market cap (Melin, 2017). Breaches are now becoming capable of leading to actual death of humans whether it is ransomware preventing adequate healthcare from being given (Wace, 2017) or SCADA systems controlling manufacturing and power plants maliciously sent awry (Hinden, n.d.). Increasing the challenges of keeping up with cyber threats, malicious actors have been able to get their hands on tools of ever increasing sophistication and capabilities thanks to leaks of nation state tools such as stuxnet (Mueller & Yadegari, 2012) and wannacrypt (Microsoft, 2017) by entities such as the Shadow Brokers (Perlroth, 2017). Ethical hacker conducted offensive security assessment represents the only true proactive tool towards addressing such prolific threats.

Unfortunately, by attempting to act on level terrain to Advanced persistent threats (APTs), practitioners of offensive security assessment are doing a disservice to their own success and the security of their customers. An offensive security assessment has a set time window and must follow an established set of rules as well as insure the legality of assessment activities. Conversely, APTs such as nation states, crime syndicates and other extremely resourced and motivated actors abide by their own constraints if at all. Such actors can even resort to illegal means such as blackmail, espionage, and physical violence to enable successful cyber operations.

Though known as ethical hackers, offensive security assessors should be doing their best to cheat the competition. Malicious actors and traditional threat emulators alike spend a large amount of time and effort in attacking a whole organization in search of valuable machines and data. Security assessors should instead leverage purple team and operational resources to identify and prioritize assessment of such critical items. Further, offensive security assessors should start their campaigns from the comparative high ground, beginning assessment from high impact items instead of wasting time on the journey to them. It is in this spirit that counter-APT red teaming (CAPTR teaming) aims to shift the operational advantage away from APTs and towards detection and prevention. CAPTR teaming is an offensive security assessment model implementing three novel evaluation attributes.

- Worst case risk analysis to identify scope
- Critical compromise initialization perspective
- Vulnerability analysis and exploitation using reverse pivot chaining

## Worst Case Risk Analysis & Scoping

The CAPTR team will work with both operational and security personnel in the organization to determine appropriate scoping for the assessment. The CAPTR team scope is a prioritization of critical items which have a high impact if compromised, regardless of the likelihood of that compromise. This allows for assessment resources to be spent in an efficient and effective manner on a worst-case scenario subset of the overall organization. Successful identification of high risk items requires stakeholders from both functional and security areas of the target organization. The operational staff may know which compromise objects could bring ruin to the organization if breached. However, such operational staff may not know the extent to which devices and data within the network represent or support those objects which is where the knowledge of IT infrastructure and security staff is equally important to identifying as complete an initial scope as possible. Limiting the initial scope of CAPTR team assessment to high risk objects allows for assessors to focus on a small attack surface comprised entirely of assets of importance and prevents wasted resources being spent on anything but the most consequential attack surface. Adequate identification of priority assets during the scoping phase enables successful evaluation of critical compromise items. This leads to improvement of overall security posture via mitigation of worst case scenario threats.

## Critical Initialization Perspective

Initialization perspective is the point of presence from which an offensive security assessment begins scanning and enumerating vulnerabilities. Examples of common Initialization perspectives may be from the internet, external to the organization or from different locations within the organization. The position of the initialization perspective effects many attributes of the security assessment such as the type of attack surface first assessed, the type of threat emulated and threat of identified vulnerabilities among others.

Beginning an assessment with a scope of high risk items from the initialization perspectives of an internet based threat, a compromised DMZ server or even a successfully spear phished internal user machine can hinder the progress and success of assessment. To best address vulnerabilities that may be leveraged by APTs, concessions must be made that those threats already have or will have the ability to penetrate the perimeter and subsequent layers of the organization. With high impact compromise objects identified and the scope created the CAPTR assessment model begins assessment from the priority risk items themselves. This is known as leveraging the critical initialization perspective.  This perspective allows a CAPTR team assessment to perform immediate assessment of high risk compromise objects instead of first spending the time identifying a path to them.

## Reverse Pivot Chaining

Reverse pivot chaining is a two-part process for identifying findings that have the most consequence to those initially scoped compromise objects. A localized assessment is performed on each scoped compromise item. Then, these compromise objects are leveraged as critical initialization perspectives for outward assessment of the host organization. This outward assessment is done in an atypically targeted and unobtrusive fashion which identifies tiered levels of communicants and their relationships to the initially scoped items. These relationships ultimately represent a risk link web spreading outwards from prioritized high impact items.

Local assessment of the scoped critical objects is done using elevated privilege under the assumption that an APT could eventually achieve such context during a compromise. Local privilege escalation vulnerabilities and local misconfigurations that would allow an attacker to ultimately affect the confidentiality, integrity or availability of the compromise object are assessed at the very onset of the CAPTR team engagement window. Further, this local context is used to identify potential remote access vectors such as code execution exploits or poor authentication configurations. With access to locally stored data and operating system functions the CAPTR team assessor can efficiently identify access vectors an attacker would use against the initially scoped items without having to perform potentially risky blind scanning and exploitation.

The ability to leverage escalated execution on these devices also allows the CAPTR team assessor to determine the communication links that allow other devices and users remote access.

live data such as open sockets, running protocols and active users as well as artifacts such as authentication, application and system logging are used to aggregate a list of potential communicants to the initial perspectives and roll them into an expanding scope for the assessment. In an effort to pivot outwards The CAPTR team uses this information for targeted prosecution of communicants instead of widespread remote scanning. If access is gained to tier one communicants, the locally elevated assessment process begins anew and pivoting to next-tier links is then attempted once they are identified.

This reverse pivot chaining establishes a representation of threat relationships into a risk link web with the critical compromise items at the center. Even if remote exploitation of tier one or further outward communicants is not possible the communication link is still identified with an appropriate risk rating commiserate with its potential to enable attacker access to critical compromise objects. Such information is vital to empowering defensive security equities within an organization to mitigate and or monitor the threats identified by CAPTR team findings. This web of risk links is a unique step forward in collaboration between offensive and defensive security teams to improve security posture.

## Success of the CAPTR Team Concept in the Real World

The offensive security assessment attributes involved in CAPTR teaming have been utilized alongside multiple real world red team engagements. The red team responsible for long-term offensive security campaigns and adversary emulation in a fortune 500 technology company leveraged the CAPTR methodology to coincide with several red team campaigns. Using the CAPTR team method, extremely dangerous findings to high value systems were discovered in a time window of only several days. This is instead of the weeks or longer taken during red team engagements against the same subset of the company. In several instances the

CAPTR team assessment method was able identify findings in areas that the traditional processes were unable to progress to at all during defined engagement windows. CAPTR teaming provided previously unattainable efficiency in impacting the company security posture by prioritizing assessment of critical items within the specific subsets of the company.

## Success of the CAPTR Team Concept in Experimental Evaluation

Academic and industry research on ethical hacker conducted offensive security assessments should include a standardized, portable and repeatable experimental framework for defensible evaluation of different assessment processes. This dissertation outlines one such framework and details its construction and implementation to provide an experimental testbed for measuring the novelty and success of offensive security paradigms.

Comparative evaluation of the CAPTR team offensive security concept was accomplished using this experimental framework. A host organization network was created in a lab and clones of it assessed using traditional red team and CAPTR team methods. These assessments yielded recommendations to the host organization to mitigate identified security threats. These changes were implemented to the respective clones of the original network. Then, both the CAPTR team and red team secured networks as well as a control network with no changes were attacked by a highly skilled APT emulating ethical hacker to test the security posture of the organization.

The experimental data that was collected indicated that the CAPTR team process provided findings unique to those of established offensive security assessment methods. In identical assessment scenarios there was only one finding in common between the two assessment methods out of a total of sixteen. The findings and resulting recommendations from the CAPTR team assessment ultimately empowered administration of systems that mitigated 400% the overall threat than was done by the red team assessment method. Further, the CAPTR team method protected all initially scoped compromise items throughout the attack campaign where the red team did not.

## CAPTR Teaming Concept

The CAPTR team works with an organization to identify items of dire consequence referred to as critical or lethal compromises. CAPTR teaming allows for organizations to evaluate such items of severe impact as a priority during offensive security engagement. Lethal compromise items are not the only type of equity included in the initial scope of a CAPTR team assessment, as any scoped object that is critical, lethal or otherwise important to the organization will be prioritized for evaluation. Lethal compromise items do however represent the epitome of the cost benefit gains an organization can accomplish by leveraging the CAPTR team concept to protect such assets.

### Lethal Compromise

Lethal compromise is meant to be interpreted as literal and figurative with regards to the target organization. In a literal sense a lethal compromise item could be a device or data that if affected could lead to a human being dying. This could be something medically related such as gaining access to remotely monitored insulin pumps and supplying lethal doses (Ray & Cleaveland, 2014). It could also be loss of control in a SCADA environment where robotic implements could crush a human or controllers could be tampered with leading to a chemical plant explosion (Narayanan, 2015). In the figurative sense a lethal compromise item is one that can cause an organization to cease to function. This lethality could be due to unpayable amounts of HIPAA fines due to information disclosure (Health and Human Resources, 2017) or FCC fines in other industries (Vedder Price, 2012). Whether causing human or organizational mortality such items must be treated as if they were potentially the target of an APT campaign and evaluated as such.

## Cost Benefit

Identifying potential vulnerabilities that are present to the lethal threats within an organization by leveraging less resources in an expedited assessment window is the apex of the CAPTR team concept. Prioritization of initially scoped compromise items and then the efficient assessment of those items and their communicants using the CAPTR team method represents a widely applicable cost benefit over traditional assessment methods. The reporting mechanism enabled by the relational risk data the CAPTR assessment gathers regarding initially scoped items and paths of potential access to them enables security and monitoring teams. Further, non-technical management are empowered to make cost effective security related budget decisions utilizing the risk link web.

As an example, candidate of CAPTR team assessment, take the below organizational diagram.

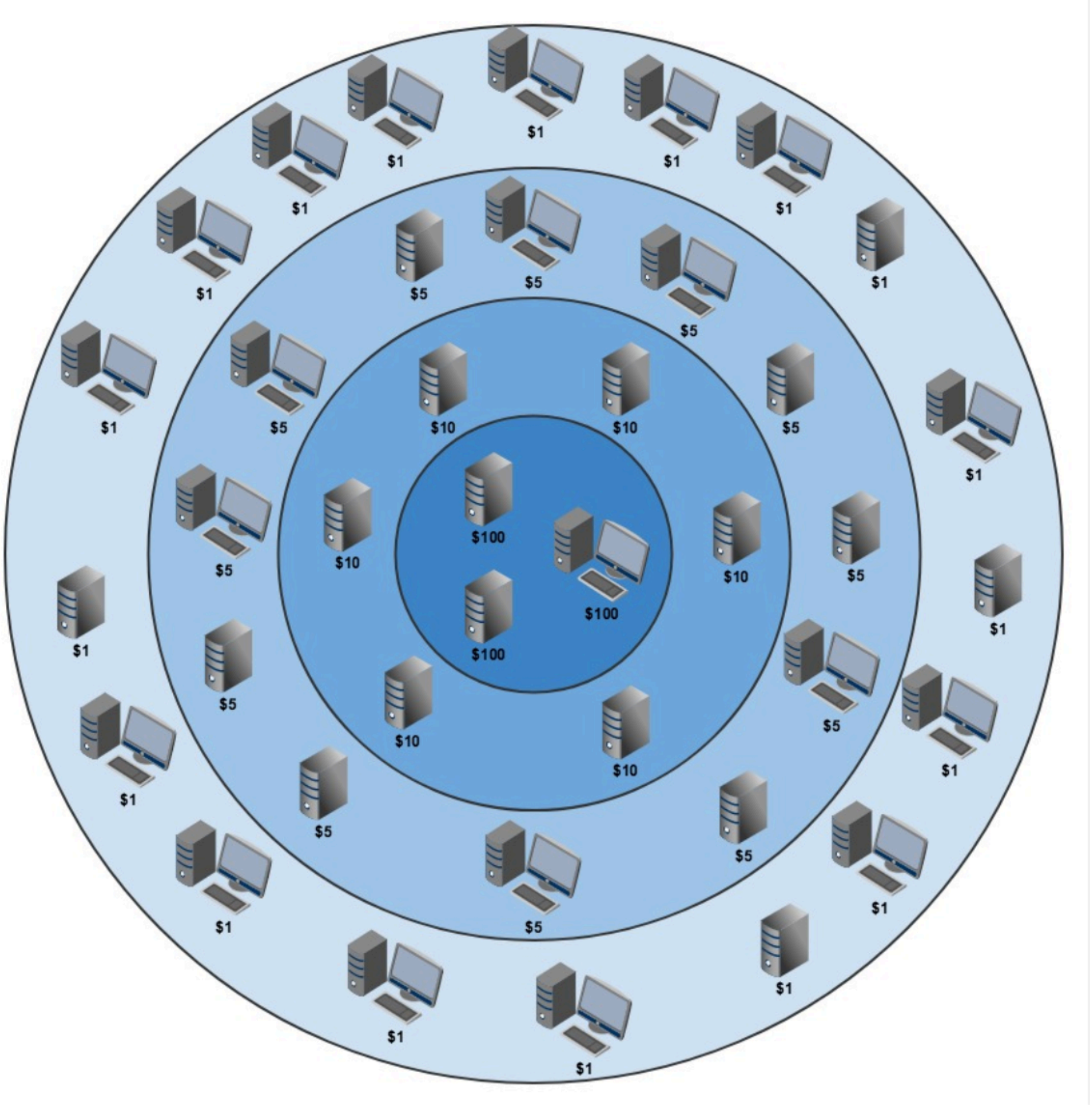


**Figure 1: Organization Object Risk Values**

This is a diagram of organizational resources separated into bands based on their cost to the organization if compromised. This is a simplified depiction and the U.S. dollar is simply representative currency of the risk value the objects have to the organization. There are 3 objects with a risk value or $100, 6 with a risk value of $10, 12 with a risk value of $5 and 18 with a risk value of $1. The total risk value for all the objects in the organization is $438.

Below are overlays of the previous diagram showing the likely outcome of scoping for both a CAPTR team engagement and a traditional offensive security engagement such as red teaming or penetration testing.

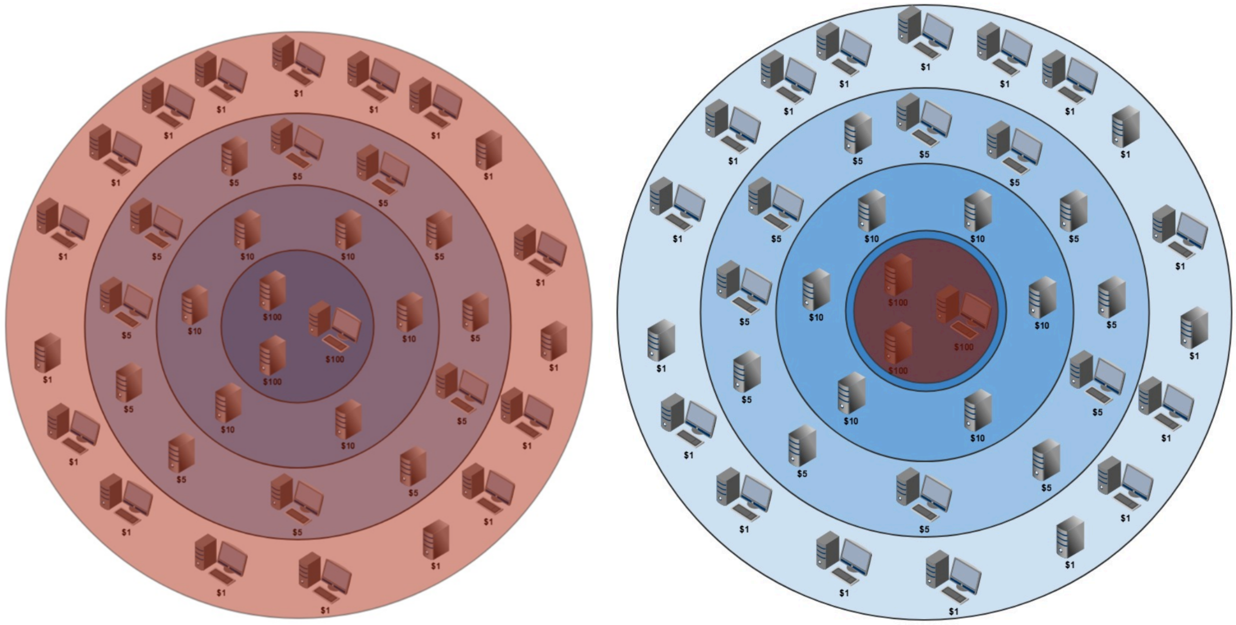


**Figure 2: Traditional Offensive Security Scope and CAPTR Team Initial Scope**

On the left is a representation of typical scoping for a traditional offensive security engagement. Since the aim of such engagements is to simulate an attack on an organization in an effort to uncover any weaknesses (Choo, et al., 2007) the entire organization is subject to assessment and therefore included in the scope if possible. The CAPTR team scope is limited to items of critical importance which in this case are the three objects in the organization with risk values of $100. Although high value items are included in both scopes, it can be certain in the CAPTR team assessment that they will be assessed. In the traditionally scoped engagement the likelihood that every item is assessed is highly dependent on assessor skill and the window of time allotted the assessors.

Next consider the below representations of example findings from both types of engagements.

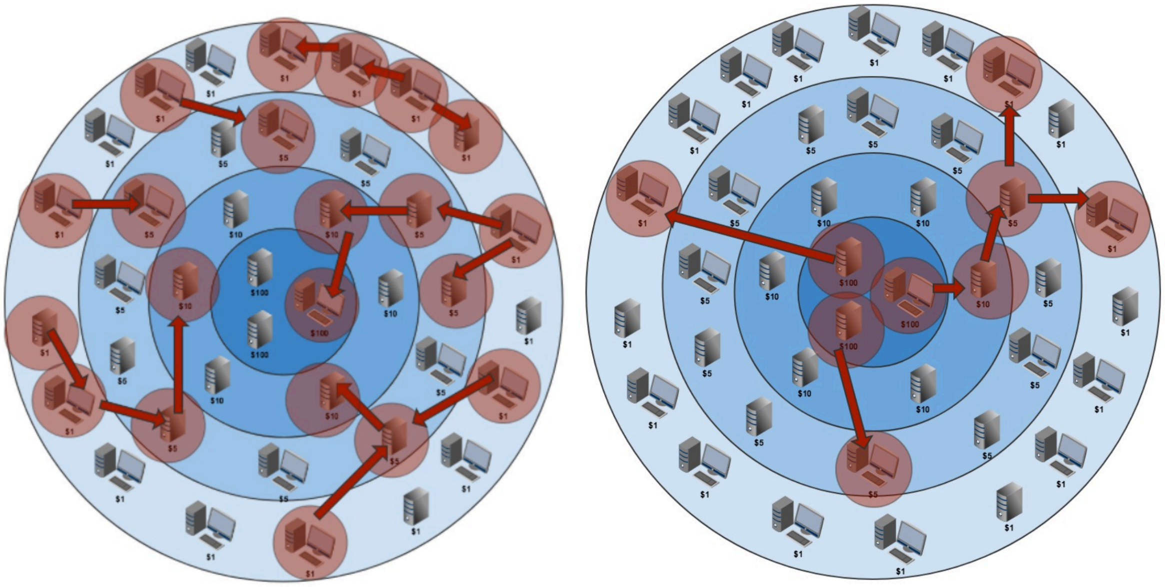


**Figure 3: Traditional and CAPTR Team Example Findings**

On the left are example findings resulting from the scope used by traditional offensive security assessments and on the right are the findings resultant from the CAPTR team assessment. The red circles over objects represent their compromise during engagements and the red arrows depict a pivot to another device via information found on the previously assessed host. In an effort to assess weaknesses in the entire organization the traditional assessment method did compromise one of the high value targets as well as many others. This shows the potential for a traditional assessment to compromise and progress to many hosts within the organization but perhaps not to all of those identified as being particularly high in value to the organization. Conversely the scope of the CAPTR team assessment allows for those high value systems to be assessed from an elevated privilige at the onset. This initial scope also leads to the identification of communicating hosts that pose potential access vectors an attacker could take to attack the high value items. Those are then assessed and compromise if possible and the process then continues for the duration of the assessment window. This method potentially compromises fewer hosts than traditional models however the value of compromised assets is likely much higher. Also, by identifying communication relationships between lower value objects and high value objects the CAPTR team model can identify which low value hosts actually pose a high value risk to the organization due to their risk relationship with the critical items in the over all web of compromise carried out by the team.

In the above figure the traditional offensive security assessment of typical scope resulted in a compromise of 21 objects in the organization with a sum total of $171 in risk value associated with them. The CAPTR team assessment of its initial scope resulted in compromise of 9 objects in the organization with a sum total of $323 in associated risk value. These are just examples but illustrate potential outcomes of processes using traditional and CAPTR Team offensive security methods. In similarly timed engagement windows CAPTR teaming would realistically lead to the assessment and compromise of at least those most valuable items included in its initial scope totalling $300 in risk value. To identify findings with this level of impact the traditional offensive security assessment would have to go on long enough to engage at least two of the three high value items as well as all others within the organization.

To understand the benefit the CAPTR team process provides in translateable recommendations to host organiations again consider the CAPTR team example findings diagram shown larger below.

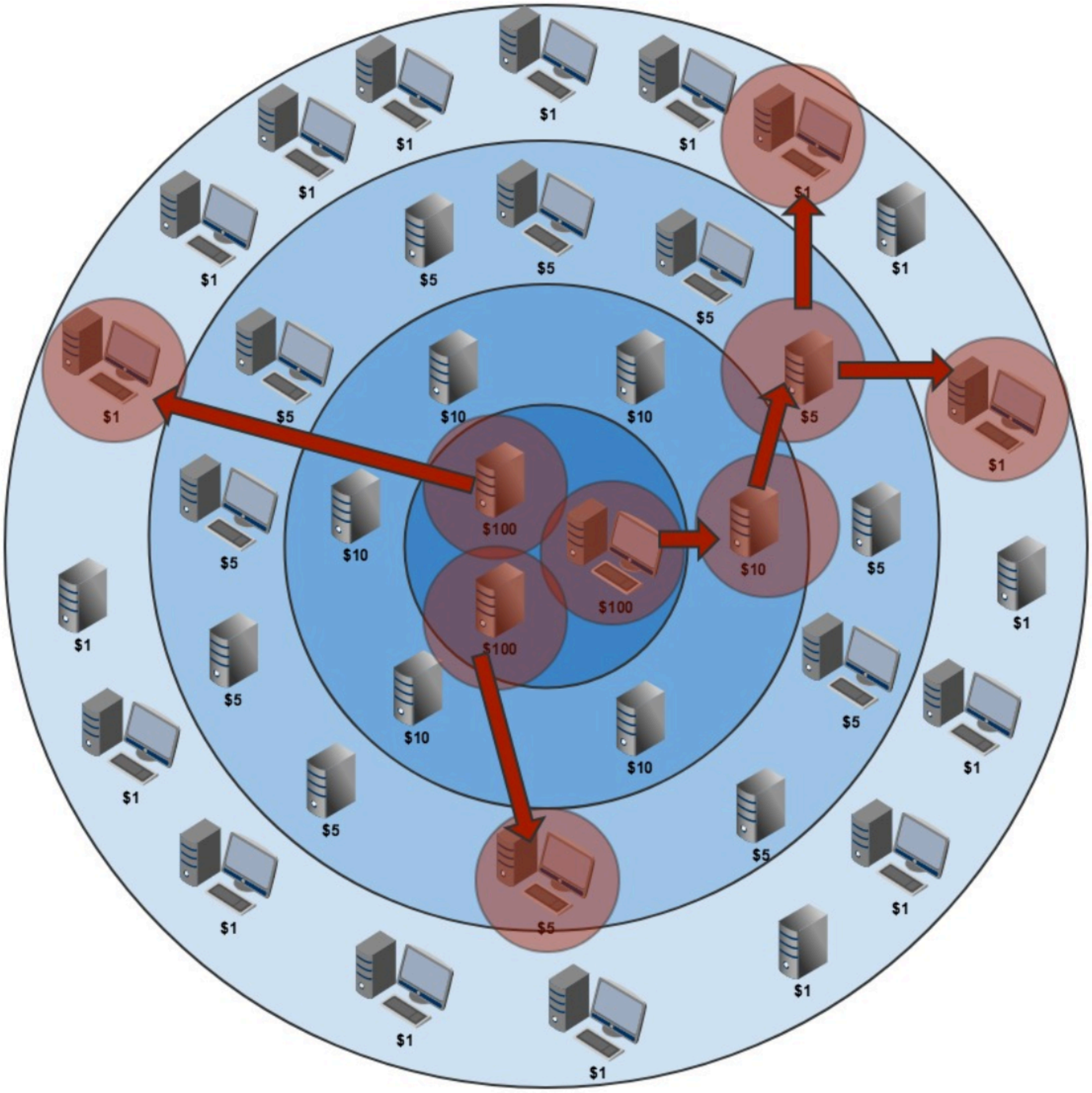


**Figure 4: CAPTR Team Example Findings**

The findings in the above diagram will be discovered in an order that reflects their distance from those initially scoped critical items and their different communicants. Findings on the high value items are of grave concern to the organization and should be addressed quickly. The next tier of hosts is comprised of those that directly communicate with the initially scoped items. In this diagram for example an object with a risk value of $1 is found to directly communicate with a high value item from the initial scope. The risk web provided by mapping communicating hosts and their tiered relationship to the critical items allows even non-technical managers to easily understand the value of fixing the identified $1 object. At face value, a vulnerability in a $1 value object may be simply accepted instead of mitigated as part of the risk analysis based on offensive security findings. This is due to the fact that the organization might not view spending $10 to fix a problem on a $1 machine a worthwhile investment of resources. The CAPTR team model however represents its results in such a way that the $1 machine vulnerability is actually identified as being a potentially $100 problem due to its relationship with the initially scoped critical items. Now a potentially unaddressed critical vulnerability is prioritized in a way reflecting its ability to impact the overall risk value associated with an organization.

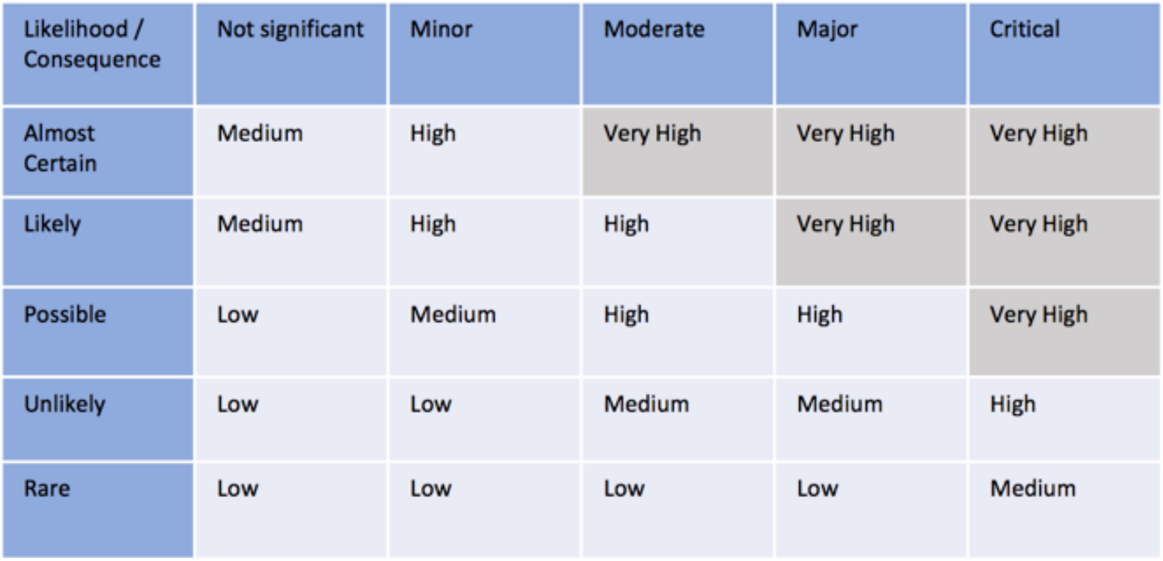
## CAPTR Teaming Process

The process for CAPTR team assessments is unlike that of a typical red team. First a model driven risk analysis like the CORAS approach (Lund, et al., 2011) is conducted to prioritize worst case scenario items within the initial scope. This risk assessment involves not only operational and IT staff from the organization but also the offensive security professionals who will conduct the assessment. A local assessment is then conducted on the machines to identify privilege escalation as well as potential remote access vulnerabilities. Once this phase is completed the CAPTR team will utilize passive reconnaissance enabled by locally accessible information to identify reverse pivot points and expand the engagements scope outward to identified communicants.

Next, any successfully exploited remote code execution vulnerabilities will be leveraged to allow the team interactive access to the pivot devices. Then the team can use that access to find any necessary privilege escalation techniques local to these pivot machines. This reverse pivot chaining process is repeated as many times as possible during the engagement to create an access web leading back to the initially scoped items.

## Risk Assessment & Scoping

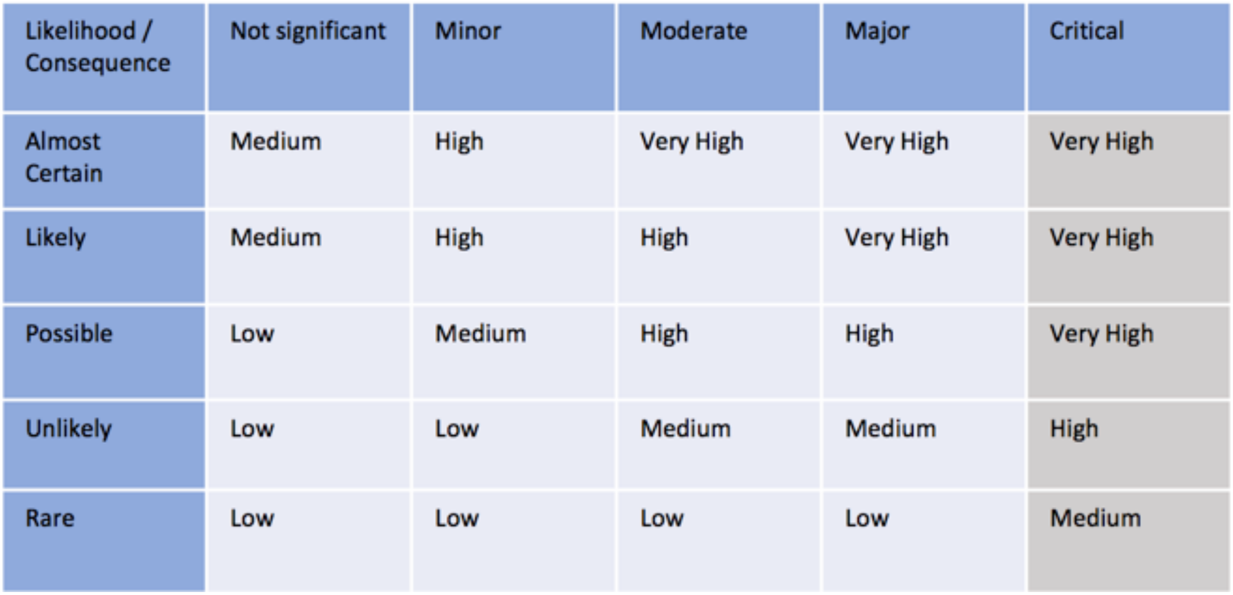
The identification of scope by the CAPTR team is a multi-part process focused on identifying those items that pose lethal or critical impact if compromised. The scope in a CAPTR team assessment is intended to allow assessment resources to hone in on a limited and prioritized subset of the overall organization. Traditionally in risk management and prioritization the leadership of an organization will use a standard risk matrix to determine which items present the highest risk (the shaded regions below) and to address those first.



| Likelihood / Consequence | Not significant | Minor | Moderate | Major | Critical |
|---|---|---|---|---|---|
| Almost Certain | Medium | High | Very High | Very High | Very High |
| Likely | Medium | High | High | Very High | Very High |
| Possible | Low | Medium | High | High | Very High |
| Unlikely | Low | Low | Medium | Medium | High |
| Rare | Low | Low | Low | Low | Medium |

*Figure 5: Red Team Risk Focus*

The CAPTR team helps the organization leadership understand that the likelihood does not matter critical items and to assume compromise is possible and probable. If an APT is intent on targeting items of lethal or critical impact to the organization, it is only a matter of time until these items will be at risk. This should move risk prioritization towards addressing those items that fall in the critical column of a typical risk matrix (shaded below) as the likelihood of attempted and eventually successful compromise by an APT is accepted to be almost certain in worst case scenario analysis.



| Likelihood / Consequence | Not significant | Minor | Moderate | Major | Critical |
|---|---|---|---|---|---|
| Almost Certain | Medium | High | Very High | Very High | Very High |
| Likely | Medium | High | High | Very High | Very High |
| Possible | Low | Medium | High | High | Very High |
| Unlikely | Low | Low | Medium | Medium | High |
| Rare | Low | Low | Low | Low | Medium |

**Figure 6: CAPTR Team Risk Focus**

Consider a law firm, the COO of the organization and senior partners might outline that the records of privileged attorney client information and planned defenses for future court dates are of critical if not lethal impact to their organizations continued existence. Those individuals however are unlikely to know where all the places that information is stored are or how that storage and access is managed. Therefore, the process of scope identification relies on not only these operational individuals but also the IT and security staff to identify what items constitute the initial scope of critical and lethal compromises. In talking with the IT staff of the organization it might be identified that compromise of any given number of devices could provide access to the confidential information indicated as lethal by the company leadership.

The ability to resolve this multi-sourced information is a unique requirement and function of a CAPTR team. The team will meet with operational staff involved in the functions of the organization as well as security and IT staff. The perspectives of operations, organizational security and the offensive security expertise of the CAPTR team members will be applied in a model driven risk analysis to determine which items in comprise the subset of devices and data that should be prioritized for assessment. The items derived from this process are considered the initial scope of the CAPTR team assessment. In a CAPTR team engagement it is imperative that the scope be identified as correctly as possible since it has great impact on the overall process of evaluation during a CAPTR team assessment. Missed items not included in the initial scoping of CAPTR team assessment are likely to not benefit from the efficient application of resources during the engagement.

**Initialization Perspective**

The critical perspective starts at a point or points of presence that are identified as posing the greatest risk to the organization. An attack that affects the availability, integrity or confidentiality of these items is likely to bring down or cripple an organization. Thus, the focus of an assessment from this perspective is to identify vulnerabilities local to such devices that would enable an attacker to compromise the critical item. The assessment is then expanded to the points in the organization that would allow an attacker to pivot to the critical items and continues outward.

This purposed perspective allows for mitigating the impact of a breach regardless of its source. No matter the vulnerability that allowed an attacker into an organization, or the locality of an insider threat, should affect this initial assessment perspective from enabling threat mitigation. Beginning security assessments at the goal of a compromise instead of assessing the potential starting points and subsequent pathways provides CAPTR teaming this ability.

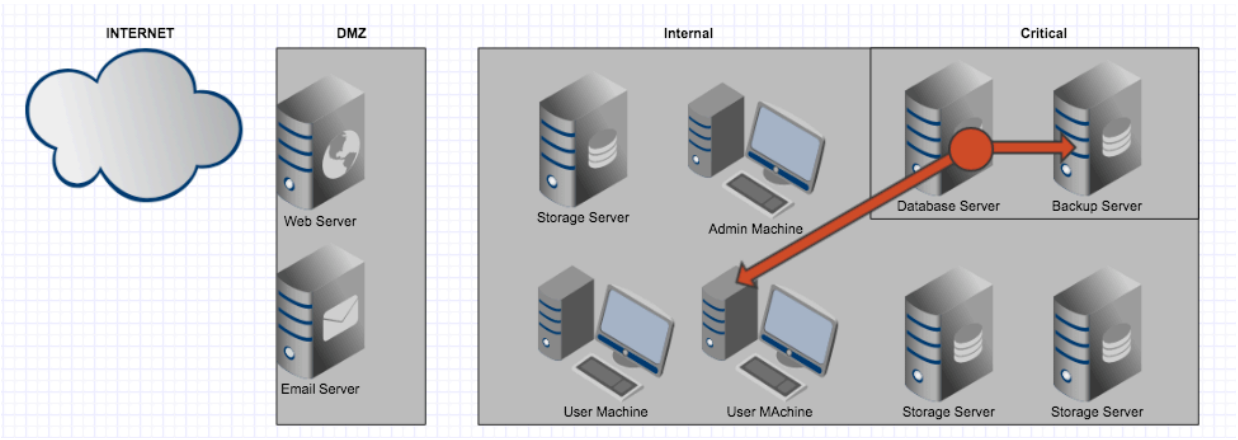


**Figure 7: Critical Perspective**

## Evaluation

After the scope is created, analysis is performed from a locally privileged access to enumerate vulnerabilities which enable immediate impact on the confidentiality, integrity or availability of these compromise items. The goal of this local evaluation is to identify any vulnerabilities that would lead to an attacker being able to escalate privilege and complete the compromise once on the device. This could be in the form of privilege escalation exploits such as semtex (US-CERT, 2013) (sd, 2013) for Linux or MS14-058 (Microsoft, 2014) (Strategic Cyber LLC, 2017) on Windows or even something as straight forward as poorly configured permissions on the machine which locally stores lethal compromise data.

Once the identification of any ability to elevate attacker privilege and capabilities is completed on the lethal compromise devices the team will begin surveying the machine for vulnerabilities that could potentially lead to remote access. This will be done utilizing system provided details on running processes, open ports, as well as services the device hosts. These details will result in findings of vulnerabilities based on the version of running programs as well as potential misconfigurations that would allow an attacker to exploit on to the machine from another. With the configuration files and logs locally accessible to the CAPTR team, identification of misconfigurations also is extremely efficient. Additionally, the local access enables the assessors to identify all potential avenues for communication with the device and any version related information with the simple execution of system commands. The information that leads to findings at this phase of the assessment are also entirely reliable as the source of indicative information is determinate from the host itself and not heuristically guessed by a remote scanning tool.

The CAPTR team will continue its assessment looking for reverse pivot points in the organization that lead to the lethal compromise items. This involves analyzing the local machines using uncovered data to conduct passive reconnaissance identifying the ways in which the machine is remotely accessible. This could entail checking authentication logs, network connections, capturing network traffic, and using any other artifacts of external communicants. Once a list of devices and users are identified as reverse pivot points they will be rolled into the scope of the CAPTR team assessment. The connection between these newly identified and previously scoped items is recognized as a high-risk link that could be leveraged by attackers seeking to access the lethal compromises.

Each identified reverse pivot point is remotely enumerated for potential exploitation. Any vulnerabilities identified as providing remote access to these pivot points are then leveraged to gain interactive access. Privilege escalation will then be pursued if remote access is attained. Once again local assessment is conducted. This is done both to identify any additional potential remote access vectors the pivot point may have but to also identify the reverse pivot points that would provide remote access to itself. This allows for an expansion of the link web to sequential tiers of access. Another benefit of this process is that the outward identification of pivot points and their ability to access scoped items is performed without intensive remote scanning and produces little network traffic during the entire assessment.

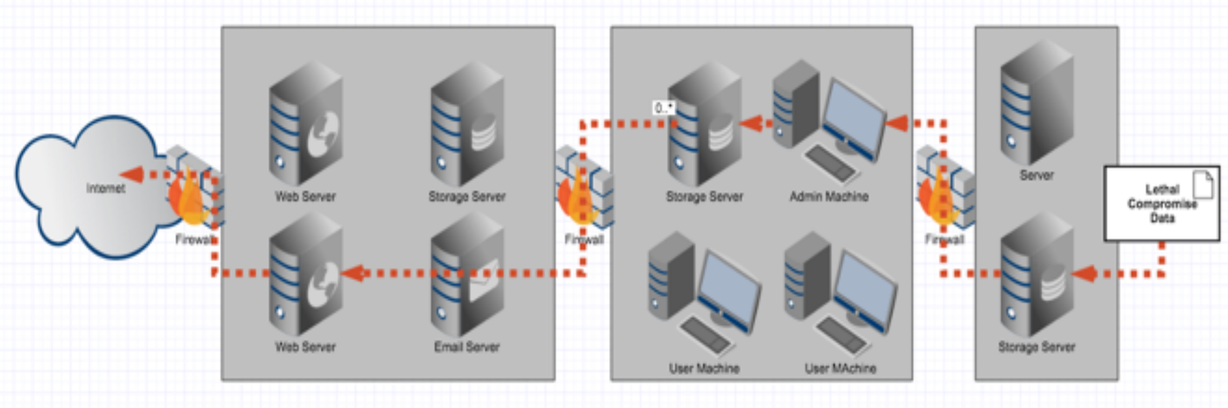


*Figure 8: CAPTR Team Process*

**Post Evaluation**

Like traditional red team penetration tests, after a CAPTR team finishes its evaluation of the organization it will generate a report based on its findings.  In a typical penetration test report the vulnerabilities and findings are outlined but the order of the findings is based on the severity according to the penetration testers perspective. This may not be indicative of which of the reported items the organization deems necessary to mitigate and which it might consider acceptable risk.

In a CAPTR team report the findings are reported in the order they are found. Since the evaluation is initialized at the lethal and critical compromises the order of the report will be prioritized based on proximity to these items. This highlights the importance in the creation of initial scope since compromise items identified by customer leadership and information technology representatives determine the assessment as well as the reporting mechanisms. The severity of reported issues starts with the items that allow immediate access to the identified compromise items and follows the assessment path as it moves away from them.

There is an added benefit to the evaluation portion to the CAPTR team assessment as well. In addition to reporting identified vulnerabilities that the organization should remedy the process of the CAPTR team assessment also produces a web of risk links. All links from initially scoped compromise items to the first pivot points are the highest risk, with follow on pivot links representing lesser risk. Also, the pivot points with the most links outward also present a higher risk than those with none or few. The inclusion of this risk representation in the report means that even if implementation of remedial efforts takes time there can be an immediate focus by defensive monitoring entities to hone in on those high-risk communication links. This is done by providing links in the form of source, destination and services data that should be monitored while and after remediation efforts to fix identified vulnerabilities are under way. Even if or after all vulnerabilities are remediated and mitigated these links still represent ways in which the lethal compromise items are communicated too and the path a future attack may have to take. Below is an example risk web showing more critical findings in red and transitioning to orange and yellow as the distance between the initially scoped items and the findings grows.

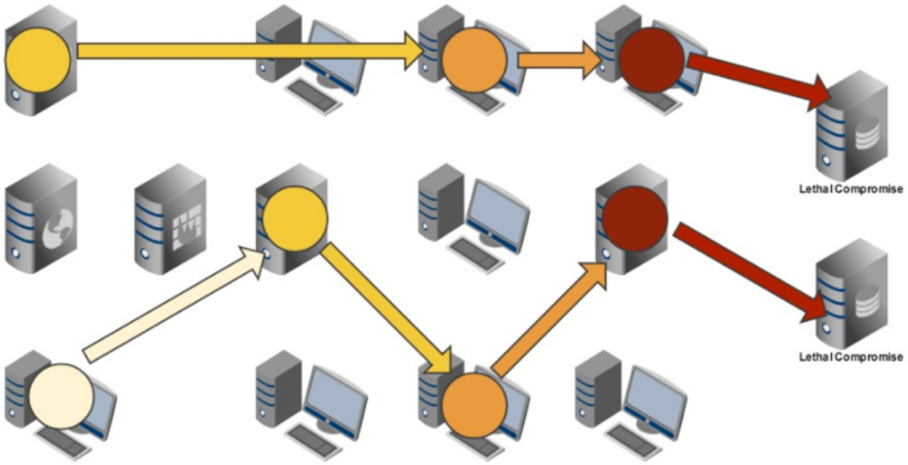


*Figure 9: Example of Risk Link Heat Map*

## Related Work

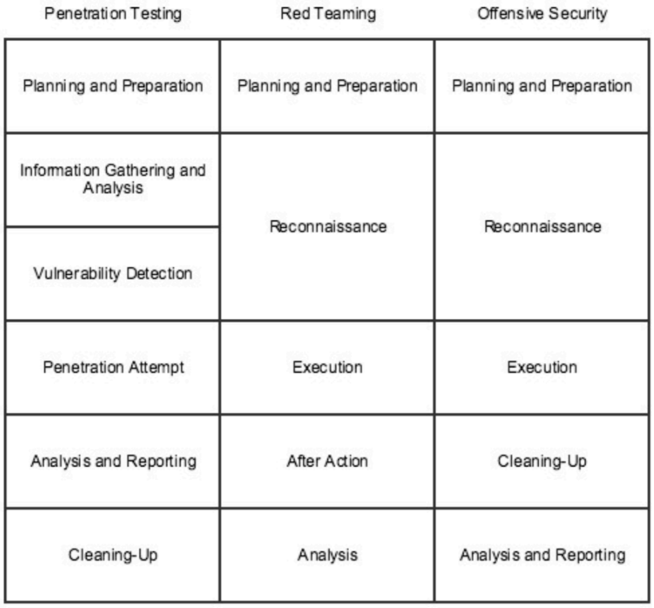
Offensive security assessments conducted by ethical hackers are represented by two commonly known engagements, Red teaming and penetration tests, which are now widely accepted components of the greater security framework for many organizations. The particulars of how these respective assessments are carried out may differ from vendor to vendor or organization to organization yet there is commonality in these processes of offensive security assessment. Semantically the two processes of red teaming and penetration testing are at times referred to almost interchangeably by some and as different representations of the offensive security process by others. For the purpose of comparison to automated technologies bearing both labels, red teaming and penetration testing will be referred to using the umbrella term offensive security assessment in this context.

There has been some academic work in regard to offensive security assessment in a non-automated sense. There has been research to address the growing role of virtualized environments with regards to the established offensive security assessment lifecycle (Guarda, et al., 2016). Additionally, research has been presented focusing offensive security assessment processes towards specific technologies by applying the known assessment lifecycle to routers (Kucuksille, et al., 2015) and SCADA Wi-Fi  (Francia, et al., 2012). Unfourtunately, this research is focused on very specific technology inplementations and assessing them with known security assessment methods, not innovating the assesment lifecycle itself. There is a definitive need for more research efforts innovating the manual offensive security process itself.

With regards to automation efforts there has been diverse work in academic and indsurty circles. The security industry has seen the development of tools specific to offensive security testing (Strategic Cyber, LLC, 2017) (harmj0y, et al., 2017) and even offensive security tailored operating systems like Kali Linux (Offensive Security, 2017). There has also been several efforts aimed at automation of penetration testing utilizing some of these tools and third party software as well as others to be discussed later in this dissertation. Academia has a strong body of research towards creating automation of offensive security assessments utilizing different technologies and tools. These fall roughly into three catergories. There are those centered around non-exploitative assessment modeling as well as both exploitative pivoting and non-exploitative non-pivoting enumeration frameworks.

## Offensive Security Assessment Lifecycle

Before delving into the different attempts at automation it is first necessary to provide a baseline for the manual assessment process itself. Security authority The SANS Institute lists the phases of penetration testing as Planning and Preparation, Information Gathering and Analysis, Vulnerability Detection, Penetration Attempt, Analysis and Reporting, and Cleaning-Up (Wai, 2002). The NATO Cooperative Cyber Defense Centre of Excellence lists the phases of a cyber red team engagement as Preparation, Reconnaissance, Execution, After-Action and Analysis (Brangetto, et al., 2015). Both processes are very similar and can be distilled into a simplified offensive security assessment process. These three process phase representations are shown in the figure below.



| Penetration Testing | Red Teaming | Offensive Security |
|---|---|---|
| Planning and Preparation | Planning and Preparation | Planning and Preparation |
| Information Gathering and Analysis | Reconnaissance | Reconnaissance |
| Vulnerability Detection | | |
| Penetration Attempt | Execution | Execution |
| Analysis and Reporting | After Action | Cleaning-Up |
| Cleaning-Up | Analysis | Analysis and Reporting |

**Figure 10: Assessment Process Phases**

Focusing on the generalized Offensive Security assessment phases shown above in the right column the phases are relatively straight forward in their labeling. The Planning and Preparation phase is where the scope, rules of engagement, resources and other items are identified and agreed upon between the assessor and the target organization. The Reconnaissance phase is the process where the ethical hackers identify targets and potential vectors of access on to those targets from an established starting position. This position may be external or internal to the organization. The Execution phase is where identified vulnerabilities in enumerated systems are leveraged to gain interactive access to those targets. Once the operational portion of an assessment is drawing to a close the Clean-Up phase is used to remove any artifacts created by assessor exploitation and redirection attempts as well as removal of any implants or tools installed on the machines. Lastly, the Analysis and Reporting phase is where the results of the assessment are compiled and analyzed and then presented to the host organization so that they may be acted upon. It is also important to note that the assessment process shown above, is in reality not quite so linear.

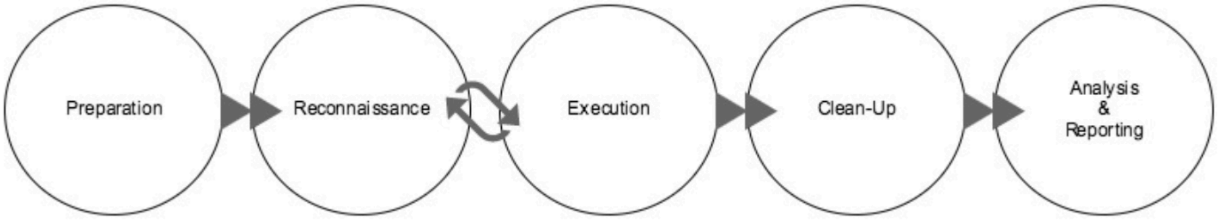


**Figure 11: Offensive Security Assessment Lifecycle**

The actual lifecycle of a manual offensive security assessment involves a process more similar to that shown in the figure above. The Reconnaissance phase is repeated any time new access is gained via the Execution phase of the assessment. This allows for the assessor to pivot deep into an organization and assess as much of the whole target set as possible. The ability to repeatedly identify and gain access to systems at varying levels of an organization is the hallmark of an effective offensive security assessment engagement.

## Red Team Automation in Academia

As mentioned, academia has championed the cause of providing cost efficient security assessment through attempted automation of red team or penetration testing processes and concepts. These can be roughly separated based on the attributes of the concepts. Some paradigms involve and discuss actual vulnerability enumeration and exploitation. Others focus more on modeling the offensive security process in such a way that analytics and automation may be possible without manual prosecution of an organization. Further those methods involving vulnerability enumeration and potential exploitation can be further divided into those that pivot post exploitation to follow-on enumeration and those that do not exploit or pivot.

### Model Based Solutions

Two specific research works were chosen to represent this form of automation efforts. There is work towards security metric quantification and analysis using fast model-based penetration testing as well as an ontology-based big data approach towards automation.

In fast model-based penetration testing, detailed relationships are established between all possible machines in a network. Potential attack vectors are assumed via service and device interactions and all permutations of possible attack paths are simulated to establish a quantitative metric for security concerns. Testing all possible permutations an attack could take throughout the organization and using such data to represent findings (Singh, et al., 2004). The hope of this method is that it could present results similar to those of manual assessment.

The disadvantages to this method are that to achieve a reliable quantitative representation a very detailed set of attributes must be accounted for on each and every device. Deviation from data submitted to the model simulations will result in largely inaccurate findings. In a large lab network this simulation model was able to accurately find attack vectors and weight them based on likelihood. It seems unlikely though that in a real network such detailed information would be available for each and every device. Moreover, human users in an organization of any size are constantly altering the state of machines and differing the potential access vectors at any given time. This means that reliable simulation of any real network of substantial size would produce unreliable findings.

In the ontological-based model for automated testing the concept of big data is use. In this model the intention is to automate a large portion of security assessment based on leveraging huge data sets from large scale networks of heterogeneous systems. The resulting relationships identified in big data analysis create the network ontology and allow for automated interpretation of relationships between systems where attacks may happen and proliferate throughout the network. (Stepanova, et al., 2015)

Similar to the fast model-based framework the ontological-based model is also extremely reliant on the entry of accurate information into the automated analysis process. The types of large scale networks containing many heterogeneous system types that this method is created for works very much against the underlying concept. In a network such as this, success of the paradigm relies on an ability to aggregate data from all types of heterogeneous systems and use it to determine relationships as a basis for assessment. Even with large scale data aggregation technologies such as Splunk (Splunk, Inc, 2017) or ELK Stack (Elasticsearch, 2017) such a network would pose extreme challenges in gathering similarly structured data in a way where it can reliably represent all the heterogeneous systems and then analyze all data as a whole. Additionally, even if successful these approaches do not include the Execution phase of the offensive security assessment process. Without proof of concept exploitation, results from these analytical processes may represent many false positive risk relationships and lead to ineffective use of the security staff resources in verification of those findings.

Such model-based techniques represent leaps in the architecting and analysis of network risk relationships but are not necessarily effective stand-ins for ethical hackers. These methods of network modeling do however pose great potential for improving monitoring capabilities in a network. Also, such technology could help in steering the focus of manual offensive security assessment towards testing of high risk links or relationships as a matter of precedence in an organization if accurate data could be ingested by the model.

## Non-Pivoting Technologies

This type of attempted offensive security assessment automation focuses on creating techniques and tools for assessing vulnerabilities on a particular application or system. Non-pivoting technologies are represented in two types. There are those that are used to evaluate a particular type of application or service on a system. There are also those attempted automation technologies that assess a set of target systems for vulnerabilities however neither act on those vulnerabilities to gain interactive access to the target systems and do not pivot from them deeper in to the network.

Examples of application or service focused non-pivoting technologies are SOFIA and Pentest Ninja. SOFIA is an automated security oracle for black-box testing of SQL-injection vulnerabilities. It uses automated technology to attempt to bypass any SQL sanitization and then perform SQL injection in any application running such software. The tool does not act upon identified vulnerabilities to achieve remote code execution or further exploit the machine hosting the SQL service (Ceccato, et al., 2016).  Pentest Ninja is a tool for automated hunting and testing of both cross-site scripting (XSS) and SQL injection vulnerabilities on web applications (Relan & Singhal, 2016). Once again however, the tool does not leverage the identified vulnerabilities to gain more information or access files on the service hosting machine.

Examples of non-pivoting technologies that target devices and not specific applications are NetSecuritas, ‘Penetration Testing in a Box’ and use of the w3af tool to achieve automated penetration testing. NetSecuritas is tool that leverages network topology and policy in conjunction with vulnerability scanners to create attack graphs for the network in an effort to provide automated penetration testing of an organization. This is achieved by scanning the provided network topology for services vulnerable to exploits in a vulnerability database (Gosh, et al., 2015). This technique does not exploit the targets and conduct further reconnaissance to further identify compromises in an organization. It also suffers from the same issues of other methods in that it does not perform proof of concept exploitation.

The 'Penetration testing in a Box' concept involves the creation of a mini-computer on a device such as a Raspberry Pi (Raspberry Pi Foundation, 2017) to create a device that can be planted in a host organization network and enable a reverse SSH tunnel out to the penetration tester / testing device. This would allow for semi-automated penetration testing using automated vulnerability scanners on the penetration testing machine (Epling, et al., 2015). Here, the tool simply enables remote access for a penetration tester and leverages third party tools to conduct automated vulnerability scanning.

The example which uses the w3af tool is an attempt to automate penetration testing. This technology leverages a live operating system on either a CD/DVD or USB drive that when mounted to an organization machine conducts automated vulnerability scanning from that perspective. This technology once again does not provide proof of concept exploitation however it has the unique ability to forego the need for pivoting as the technology can be run from devices at any level of the organizations security infrastructure. Since it does not result in interactive access any evaluation of scanned hosts misses important details on host file systems such as poor permissions on files containing passwords and keys and local configuration data.

Although several of these non-pivoting tools are being portrayed as penetration testing automation it is clear that they are primarily vulnerability scanners in one fashion or another and lack the execution phase of the offensive security process. All of the aforementioned technologies could afford offensive security assessors greater efficiency in the Reconnaissance phase of an assessment but do not themselves represent capabilities that could be considered automation of complete offensive security assessment.

### Pivoting Technologies

These types of technologies represent a level of functionality nearest to that of actual offensive security assessment. This is due to the ability to act upon discovered vulnerabilities and use them to pivot to other devices furthering the automated assessment of an organization. CALDERA is the best representation of this type of technology. It takes the vulnerability scanning capabilities of the previously discussed technologies a step further by providing logic for leveraging identified exploits to get access to vulnerable machines and continue scanning and exploiting from this new interactive context in an intelligent manner. The logic used to achieve this is via the ViRTS execution infrastructure and the LAVA logical action model (Applebaum, et al., 2016). This technology answers the issue of proof of concept exploitation where the other technologies could not.

The weakness of this technology with regards to assessing an overall network is that the intelligence driving it relies on targeting logic and an ability to act on that intelligence with vulnerabilities from a vulnerability database or framework. This is certainly a beefed-up vulnerability scanner capable of pivoting around a network following targeting based on supplied logic. However similar to other technologies it misses analysis of local systems for misconfigurations and credentials once access is gained. There is no onus on looking for clear text credentials stored on the filesystem or garnering further intelligence via operating system objects such as user command history or locally listening services. Though certainly addressing the Execution phase of offensive security assessment, this technology adds no capacity for the post operation Clean-Up and Analysis phases which would still be conducted by humans and the logic input for targeting intelligence is still largely dependent on human input.

## Red Team Automation in Industry

The security industry has also implemented automation into some of the vulnerability assessment toolkits which in some ways mirror the efforts by the academic community. Examples of this type of technology can be found in Immunity's Canvas exploit automation framework (Immunity, 2017) and Metasploit db_autopwn (Feid, 2009). These two examples are simply automated vulnerability scanners which scan hosts and attempt to throw every exploit associated with identified services regardless of whether the service is in fact vulnerable. A tool that implements logic similar to that of the CALDERA project is Cobalt Strike's Hail Mary implementation which can continue scanning and enumeration after pivoting to successfully exploited hosts. Here Cobalt strike differs though, using the Metasploit vulnerability database in a more intelligent manner, choosing exploits based on likelihood of vulnerability exploit success and stability using information gained from the scanning portion of the tool (Mudge, 2013). These efforts suffer to similar drawbacks of their academic equivalents by not having an ability to address the local contents of exploited machines to further provide intelligence to more appropriately and easily continue an organization level compromise. Additionally, Metasploit has recently deprecated the db_autopwn functionality for multiple reasons.

## General Disadvantages of Automated Red Teaming

Aside from the disadvantage of not being able to leverage human intuition during an assessment, automation technologies face several other obstacles for widespread acceptance.

Offensive security engagements are not only used to identify vulnerable systems but also to test the abilities of an organizations security and monitoring teams. The innate abilities of ethical hackers to practice stealth and tradecraft mirrors the movements and actions likely to be taken by a malicious attacker. Automated technologies may be able to exploit and enumerate systems but will not reflect what an actual attacker looks like as it quietly pivots and ultimately conducts exfiltration of data from the network. It is extremely important for an organization to not only identify vulnerabilities but also find any shortcomings in detecting and mitigating attackers as well.

The examples examined have also shown that vulnerabilities that lead to compromise in an organization are not as narrowly scoped as those enumerated by the discussed technologies. Vulnerabilities are not limited to errors in coding that lead to buffer overflows or code injection and execution. They are often misconfigurations of permissions or artifacts left behind by users or administrators of systems that can be leveraged by attackers. As such, they cannot be reliably identified and exploited by a scanning engine and exploit database. Many vulnerabilities are often introduced by humans and not present in the code of software and as such a human has the best chance of deducing and utilizing such vulnerabilities to provide as complete and realistic offensive security assessment of an organization as possible

There is also a risk to an organization posed by leveraging any automated exploitation technology. A human assessor may notice the hostname of a device to be something akin to prod-sales.company.org and deduce it is likely a production server related to sales. If the vulnerabilities best suited to the enumerated host have a risk of crashing system processes or the machine itself such as MS08-067 (Microsoft, 2008) or MS17-010 (Microsoft, 2017), the human assessor may note the vulnerability but not pursue proof of concept exploitation without talking with the host organization to de-conflict the risk. This logic and human deduction based on host name would be difficult to replicate with automation logic.

Lastly, there is a lack of ability to provide clean-up on systems affected during a security engagement. It is important post-operation for the network to return to a state of normalcy. Failure to clean systems of installed tools and operations related logging could cause complications to any investigations of real compromise that the organization may face at a later time. Even worse, tools left installed and running on devices could cause degraded performance as well. This issue affects not only the stealth during an offensive security assessment but also the after-action impact of the assessment on the host organization.

## Concluding the Case for Human Red Team Assessment

It is important to understand that this analysis is not intended as a denigration of the discussed technologies. Instead it is an effort to show them as a holistic body of work, extremely important to furthering information security capabilities, but not representative of actual offensive security assessment. As stated earlier the purpose was largely to make the case for the importance of human assessors in vulnerability identification and exploitation. Intuition and insight provided by ethical hackers is extremely valuable in any effort to identify weaknesses in and the ability of an organization to combat malicious actors.

## Initialization Perspectives

Organizations undergo cyber security assessments to prepare for the dangers posed by malicious threat actors. Utilization of security assessments is increasingly demanded by government and industry regulations (AppliedTrust, n.d.). These offensive security assessments aim to identify and leverage vulnerabilities before an attacker finds them. This is done by using ethical hackers to exploit identified vulnerabilities and simulate an attack against the organization. These offensive security assessments are intended to provide true pro-active capabilities enabling organizations to address the identified issues prior to them being exploited in a breach by a real attacker.

Typically, offensive security assessments occur in the form of red team engagements or penetration tests. Though there are variances in definitions, red teaming is used to find exploitable gaps in operational concepts with the overall goal of reducing surprises (choo, et al., 2007). Alternatively, penetration testing is typically focused specifically on the identification and exploitation of vulnerabilities (Applebaum, et al., 2016). A largely influential factor behind how an offensive security assessment navigates and assesses a target organization is the initial perspective from where it begins. This section will show correlation between the perspective from which ethical hacking is initialized and the effectiveness of that test. There are several well-known perspectives from which offensive security assessments begin. The decision between which perspective or perspectives best suits the needs of the organization is dependent on the threats faced by that organization and the equities it is trying to protect. This section will categorically compare typical security assessment perspectives of external, DMZ and internal points of presence.

This comparison is to frame the need for the critical perspective which utilizes the paradigm of assessing worst-case scenario threats. This is a method already utilized in other industries such as finance and communications to insure the system doesn't fail when subjected to the highest level of stress possible (ghosh & juneja, 2006) (Naghmouchi, et al., 2016). In cyber security, this requires beginning an assessment from identified items of lethal or critical impact to an organization if compromised. Assessment from this perspective allows for the most important items to be assessed first. Expansion of the attack surface explored during the test expands outwards to points of presence within the organization that allow for an attacker to pivot to the critical or lethal compromise items. This type of critical or lethal perspective is also utilized in the TREsPASS Project which is technology-supported automated risk estimation by predictive assessment of socio-technical Security (The TREsPASS Project, 2017). Offensive security assessment could similarly benefit from such a perspective.

There is a growing trend of insider threat involvement in security breaches (Heiser, 2017) which is something security assessments must adequately address. According to CERT an insider threat is a malicious insider that is a current or former employee, contractor, or business partner who has or had legitimate and authorized access to organization's information systems and advertently misused or abused that privilege (CERT, 2009). However, a more complete representation of insider threats actually breaks into three separate categories of negligent insiders, malicious insiders, and insiders compromised by malicious external actors (Imperva, 2016). The initialization perspective of an assessment impacts the ability of mitigating such threats.

This section will detail initial assessment perspectives of external, DMZ and internal points of presence. Next, each perspective will be contrasted by its ability to assess and exploit vulnerabilities in an organization. Then, the perspectives will be compared by their efficiency and manner of attack surface scrutiny. Lastly, disadvantages and advantages of each perspective will be outlined. It is important to note that offensive security assessment is a human conducted process involving tradecraft and skills as much as vulnerability identification and exploitation tools. As such, the process is more art than science. Yet, it is one of the most important tools available to proactively secure a network. The initialization perspective affects nearly all facets of manual offensive security assessment and this research provides analysis on the potential benefits of differing or transitioning attack perspectives.

The initial perspective of an assessment is the point or points of presence from which the assessment will begin and what the initial focus of the ethical hackers will be. Differing perspectives have been adopted to allow for assessments to continue to provide as realistic an attack simulation as possible. This means that as the attack methodologies of attackers changes so to must those used in security assessments.

### External Initialization Perspective

External perspective is the most traditional form of security assessment. External assessments typically start from an internet-based point of presence and focus at the outside perimeter of organizational security. This is an efficient way to emulate some of the more prolific threats organizations faced in times when connecting organizations to the internet was in a much less mature state.

These early threats consisted of internet-based worms (Yegneswaran, et al., 2003). With an attack surface consisting of web and database services hosted on the internet, worms such as Code Red, Nimda and SQL Snake wreaked havoc on internet connected organizations in the early 2000's (Eeye Security Inc., 2001) (Poore, 2001) (SANS, 2003). To help protect organizations from similar threats it was imperative to assess security in a similar fashion.  As such, early security assessments focused on this perspective as it represented the largest source of threats.

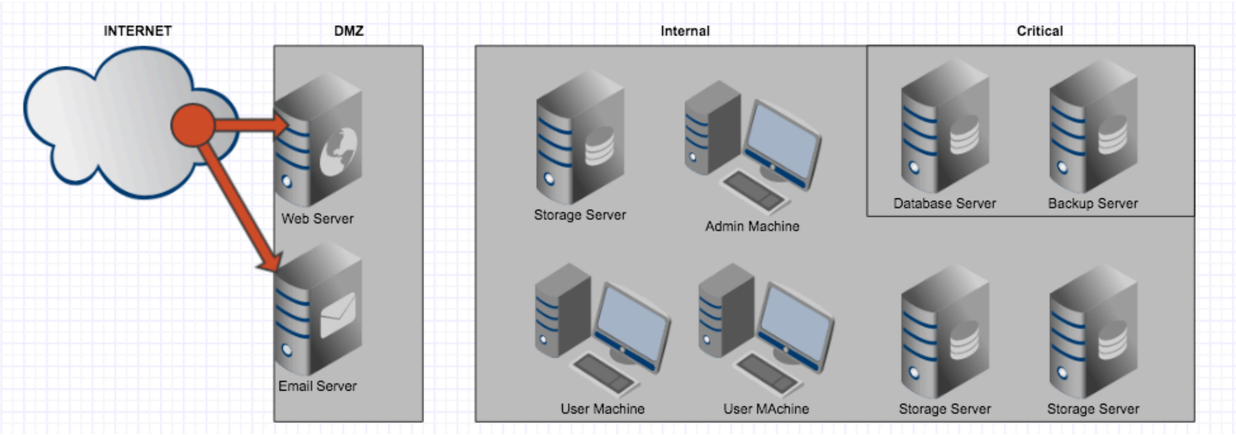


**Figure 12: External Perspective**

### DMZ Initialization Perspective

DMZ perspective is required to assess networks in response to the popularity of implementing a DMZ in network security. Due to attacker focus on compromising internet facing services of an organization security evolved with creation of a DMZ or de- militarized zone where devices hosting these services could be stored and secured in isolation from areas of an organization where users and other devices exist (Bauer, 2001).

Assessing a network with the DMZ perspective entails beginning the assessment with a point of presence in the DMZ itself and a focus on exploiting not only internet facing servers from this but also evaluating the ability to attack the internal organization itself from within the DMZ. This insures ensures there is a security assessment of the ability for a malicious actor to pivot from one DMZ-hosted internet facing device to another within the DMZ, as well as the ability for attackers to move from the DMZ to the internal network.

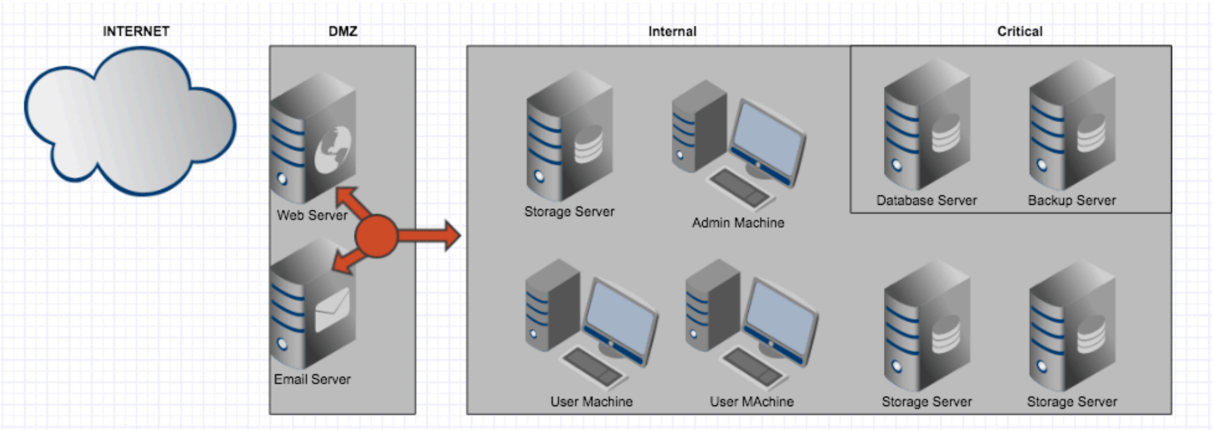


**Figure 13: DMZ Perspective**

### Internal Initialization Perspective

Internal perspective utilizes points of presence from within the network itself. This perspective is typically manifested with user context on a machine within the network and the focus of an assessment from this perspective is to assess ability to pivot location and elevate privilege within that internal network.

The need for this perspective is a direct result of the increase in compromises originating from this type of access. Two main attack facilitations that drive the need for this perspective are those resulting from insider threats and those attacks which assume such a mantle as a result of social engineering and user executed malware. The fact that socially engineered malware execution represents the lion’s share of access vectors for cyber incidents (Verizon, 2017) (Industrial Control Systems Cyber Emergency Response Team, 2016) also drives the need for this assessment perspective.

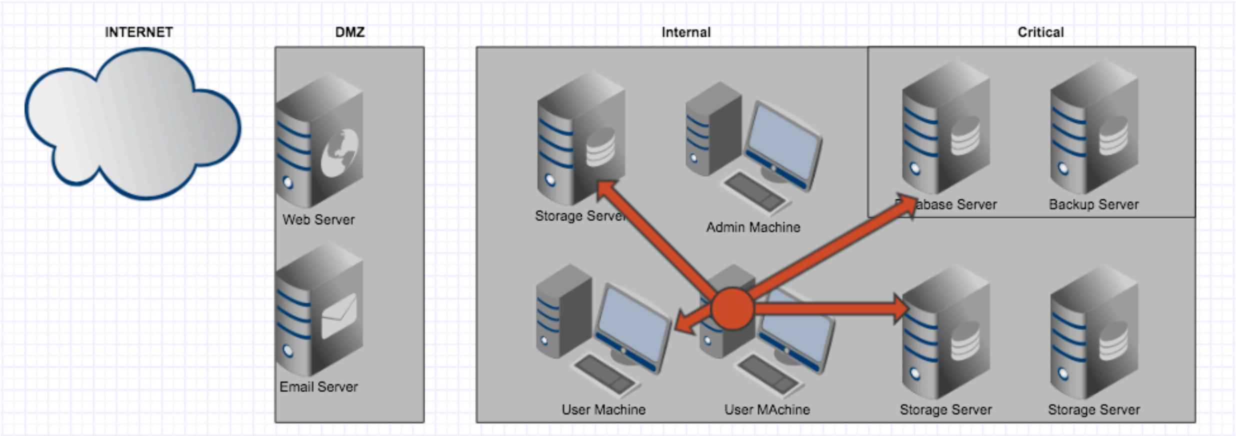


**Figure 14: Internal Perspective**

### CAPTR Team Critical Initialization Perspective

As outlined the CAPTR team use of critical perspective starts at a point or points of presence that are identified as posing the greatest risk to the organization. The focus of an assessment from this perspective is to identify vulnerabilities local to such devices that would enable an attacker to compromise the critical item. The assessment can then be expanded to the points in the organization that would allow an attacker to pivot to the critical items and continues outward.

This purposed fourth perspective is aimed at mitigating the impact of a breach regardless of its source. No matter the vulnerability that allowed an attacker in or the locality of an insider threat should affect this assessment perspective. Beginning security assessments at the goal of a compromise instead of assessing the potential starting points provides an enhanced ability to mitigate a myriad of threats.

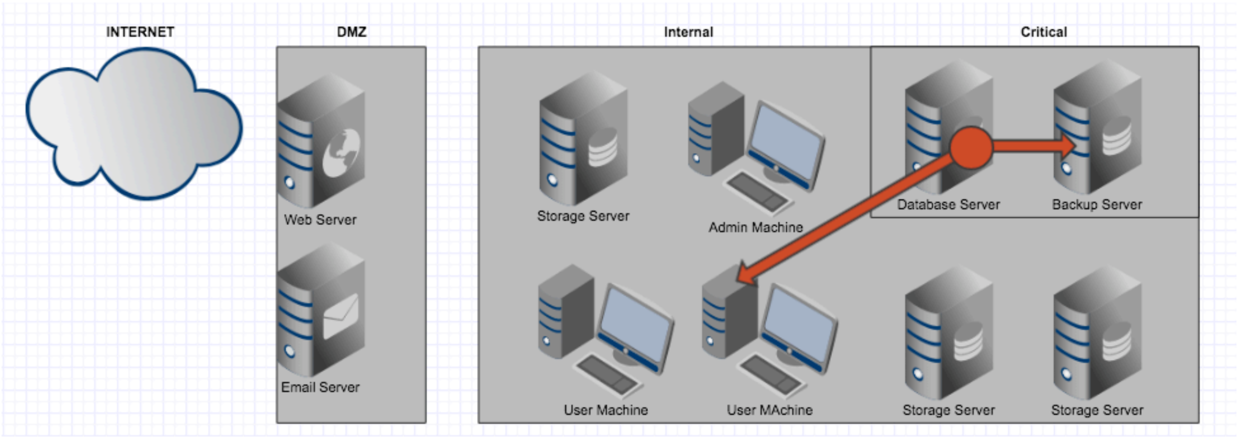
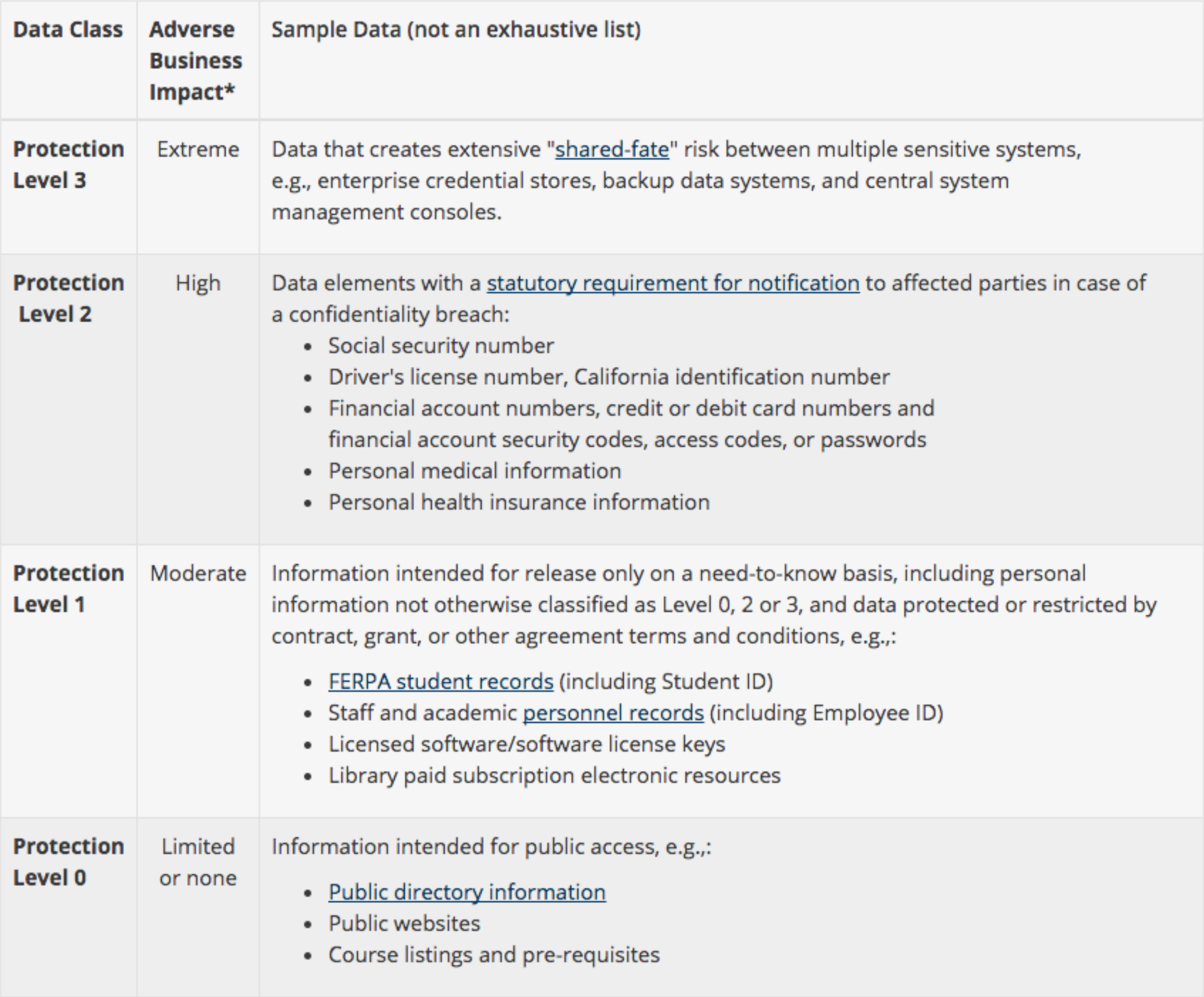


**Figure 15: Critical Perspective**

## Initialization Perspective Effect on Risk Assessment

In an effort to classify and contrast the four differing initial perspectives for security assessments a qualitative risk assessment will be utilized. Impact is a measure of how damaging different compromises would be to the organization (Lewis, 2013). The other half of rating risk is the likelihood a given impact will occur (Lewis, 2013). The metric of time is used to show likelihood and represents the amount of time spent assessing from a given perspective that it will take to yield compromises of information with differing impacts and indicates the likelihood an attacker may be able to do the same.

To qualify the impact of the findings these assessment perspectives may lead to, a classification system created by University of California, Berkeley will be used (Anon., 2013) to determine the impact related to compromised data.



| Data Class | Adverse Business Impact* | Sample Data (not an exhaustive list) |
|---|---|---|
| Protection Level 3 | Extreme | Data that creates extensive "shared-fate" risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles. |
| Protection Level 2 | High | Data elements with a statutory requirement for notification to affected parties in case of a confidentiality breach:<br>• Social security number<br>• Driver's license number, California identification number<br>• Financial account numbers, credit or debit card numbers and financial account security codes, access codes, or passwords<br>• Personal medical information<br>• Personal health insurance information |
| Protection Level 1 | Moderate | Information intended for release only on a need-to-know basis, including personal information not otherwise classified as Level 0, 2 or 3, and data protected or restricted by contract, grant, or other agreement terms and conditions, e.g.,:<br>• FERPA student records (including Student ID)<br>• Staff and academic personnel records (including Employee ID)<br>• Licensed software/software license keys<br>• Library paid subscription electronic resources |
| Protection Level 0 | Limited or none | Information intended for public access, e.g.,:<br>• Public directory information<br>• Public websites<br>• Course listings and pre-requisites |

**Table 1: UC Berkeley Data Classification Standard**

To identify which type of information each perspective is likely to identify an overlay is created showing which parts of the network are likely to contain which levels of data protection classification.

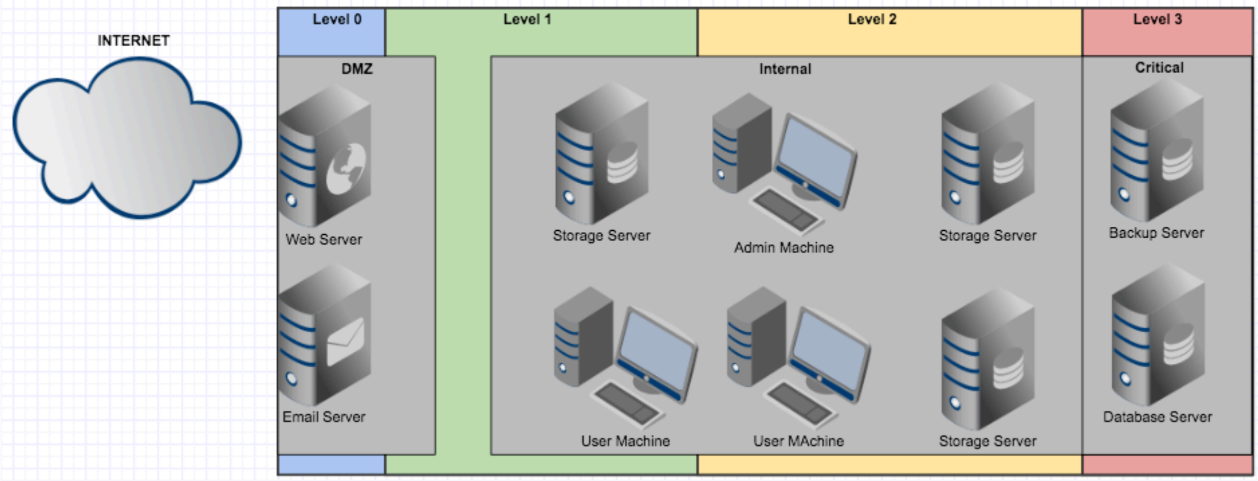


**Figure 16: Data Protection Level Locality**

As mentioned earlier the expression of likelihood will be shown as the time it would take an assessment from a given perspective to identify findings that have a given impact. For instance, if an assessment perspective has the ability to almost immediately find data with a given protection level then there is a high likelihood the perspective being used will have that impact. If the perspective requires time and pivoting to get to differing data protection levels the likelihood would be low.

It is important to understand that the passing of time during an assessment is likely to transition the assessing perspective as well. An assessment may have the external initial perspective to the network and then via exploitation gain access to a device in the DMZ. From that point forward the assessment is a representation of multiple attack perspectives. This process can continue as an assessment progresses further into the network. The defining delta involved is time, transitioning perspectives and indicating likelihood.

**External Perspective Effect on Risk Assessment**

The external initial assessment perspective has a focus on the outer perimeter of the network and may only move on to other parts of the organization after identifying and leveraging vulnerabilities in the outer most layers of the organization. As such early on in the assessment there is a high likelihood that only Level 0-1 data findings will result. Time may allow the test to compromise data of higher levels via pivoting deeper into the network but as the required duration of the test increases the likelihood then drops.

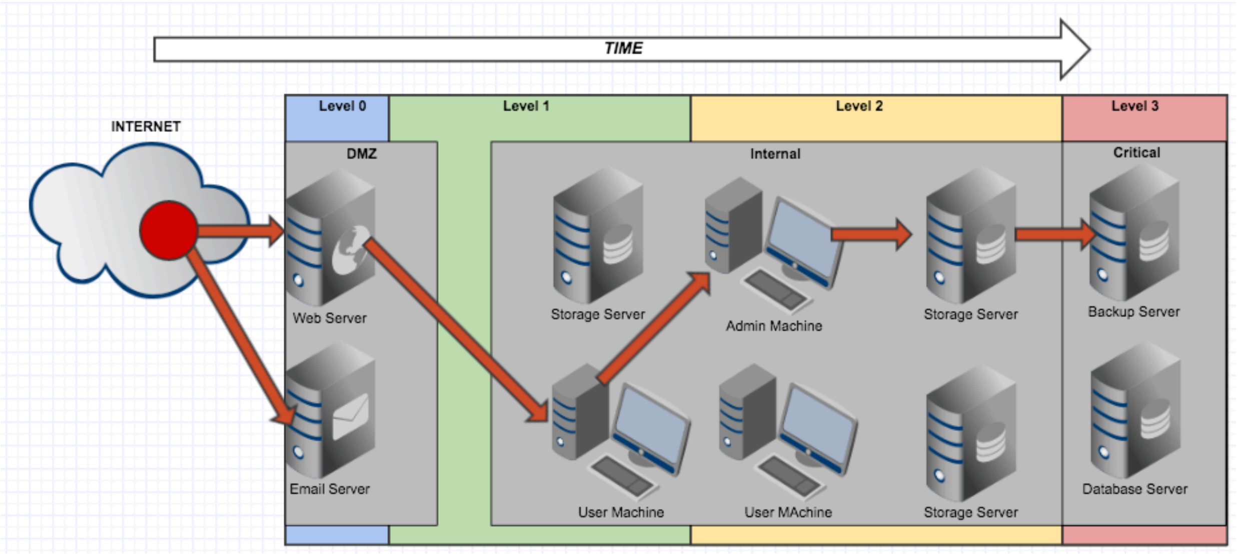
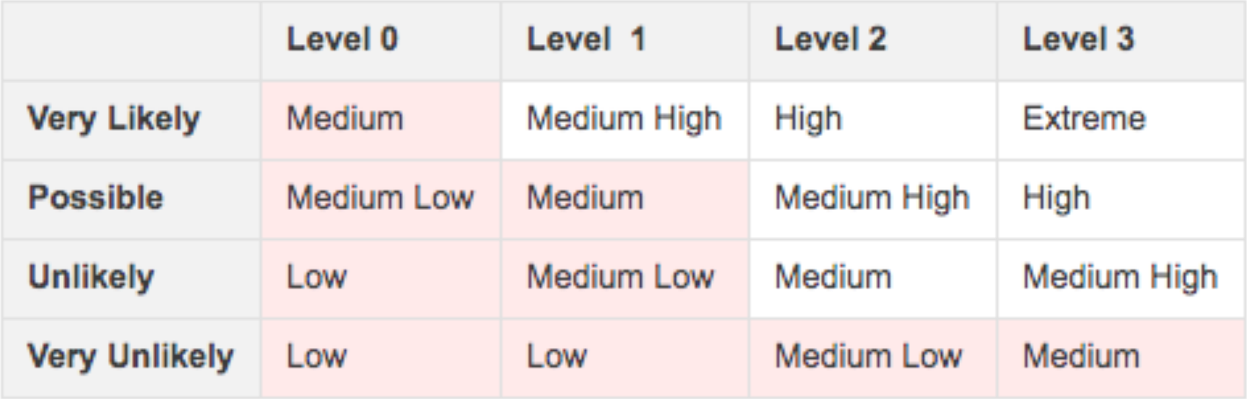


**Figure 17: External Perspective Timeline**

Using the above timeline representation of an assessment that began with an external point of presence a risk assessment matrix can be created to illustrate the impact and likelihood of threats addressed. Below, cells shaded in red indicate the levels of risk assessed. The impact is represented via the protection level associated with data that can be compromised. As stated earlier the likelihood is demonstrated by how long an assessment needs to realistically compromise a given level of data. Since the external perspective is far from where level 3 data is found in a network the time it would take to reach is greater and is therefore unlikely.



| | Level 0 | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|
| Very Likely | Medium | Medium High | High | Extreme |
| Possible | Medium Low | Medium | Medium High | High |
| Unlikely | Low | Medium Low | Medium | Medium High |
| Very Unlikely | Low | Low | Medium Low | Medium |

**Table 2: External Perspective Risk Matrix**

This risk matrix shows that the external perspective provides a high likelihood of identifying findings that could lead to the compromise of level 0 information. Even though the impact of level 0 information is low the almost assured likelihood creates a medium level of risk associated with findings found from this perspective. This perspective is less likely to lead to higher level data as it requires time to discover additional vulnerabilities allowing the assessment perspectives to pivot deeper into the organization. As shown in the external perspective risk matrix, the level of risk likely to be assessed is low to medium.

### DMZ Perspective Effect on Risk Assessment

The DMZ perspective has an advantage over the external perspective as it initially starts from a point of presence already within the DMZ of the organization and does not have to discover a finding that will allow it to pivot into the DMZ from the internet.

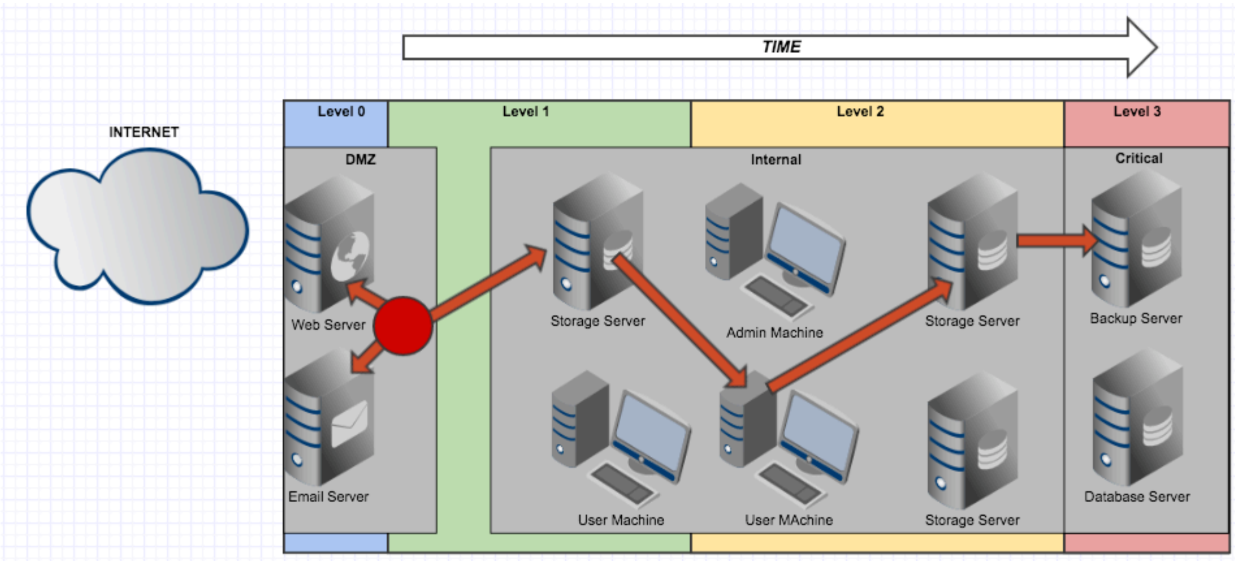
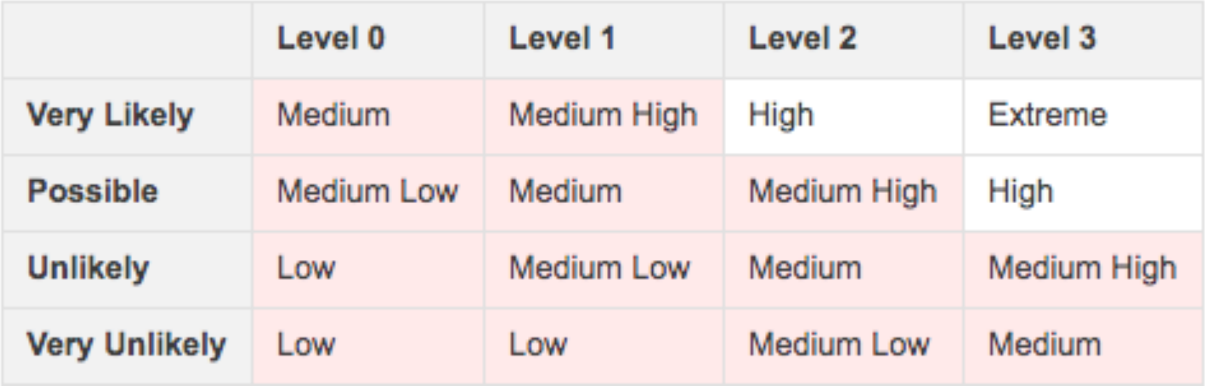


**Figure 18: DMZ Perspective Timeline**

Since an assessment from this perspective does not need the time to pivot inside that an external perspective requires, the timeline of such an assessment begins already within the perimeter of the network.



| | Level 0 | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|
| Very Likely | Medium | Medium High | High | Extreme |
| Possible | Medium Low | Medium | Medium High | High |
| Unlikely | Low | Medium Low | Medium | Medium High |
| Very Unlikely | Low | Low | Medium Low | Medium |

**Table 3: DMZ Perspective Risk Matrix**

This means that findings related to high levels of data protection are more likely as they require less time to identify and increasing the likelihood that impactful threats are found. The DMZ perspective has the greatest potential to evaluate a medium level of risk.

## Internal Perspective Effect on Risk Assessment

With an initial perspective from a point of presence in the middle of the network this perspective is afforded the ability to result in findings early on of level 1-2 data. This position also has the side effect of making an assessment with this initial perspective actually less likely to discover findings that lead to level 0 information than the two perspectives discussed previously. As with the previous two perspectives time is required to get from this initial perspective to a pivot with the capacity to compromise level 3 data.

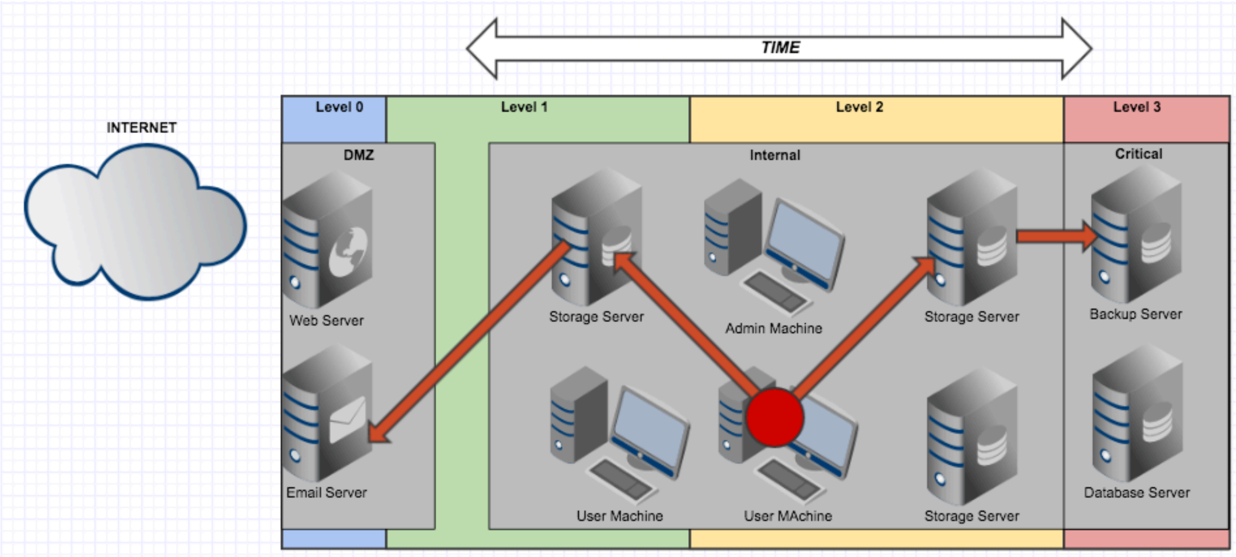
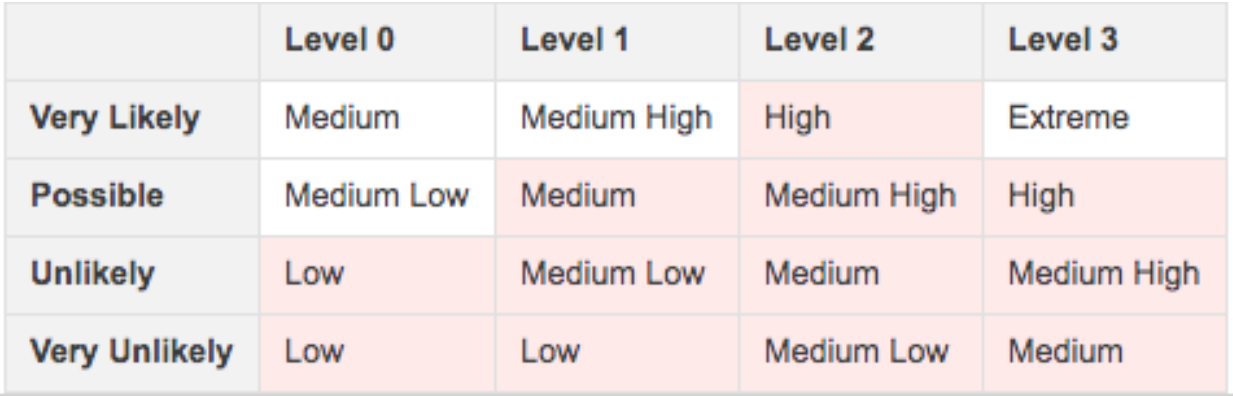


**Figure 19: Internal Perspective Timeline**

This timeline shows that for an assessment with this initial perspective to lead to findings regarding level 3 data still requires time, as does level 0 data. It is therefore most likely to find data of level 1-2.



| | Level 0 | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|
| Very Likely | Medium | Medium High | High | Extreme |
| Possible | Medium Low | Medium | Medium High | High |
| Unlikely | Low | Medium Low | Medium | Medium High |
| Very Unlikely | Low | Low | Medium Low | Medium |

**Table 4: Internal Perspective Risk Matrix**

Since it is not very likely that level 3 data will be compromised by vulnerabilities discovered from this perspective it still does not represent an extreme level of risk assessed. However, the internal perspective clearly represents a large cross section of the potential risk that can be faced. As a result, the levels of risk evaluated are likely to be medium to high and potentially low as well.

### CAPTR Team Critical Perspective Effect on Risk Assessment

An assessment using the critical initial perspective begins deep in the network at the most valuable points. This means that opposite to the other three perspectives, findings of level 3 data compromise will be identified in the beginning. Unfortunately using this perspective requires time to get to point in the network that contain level 0-2 data.

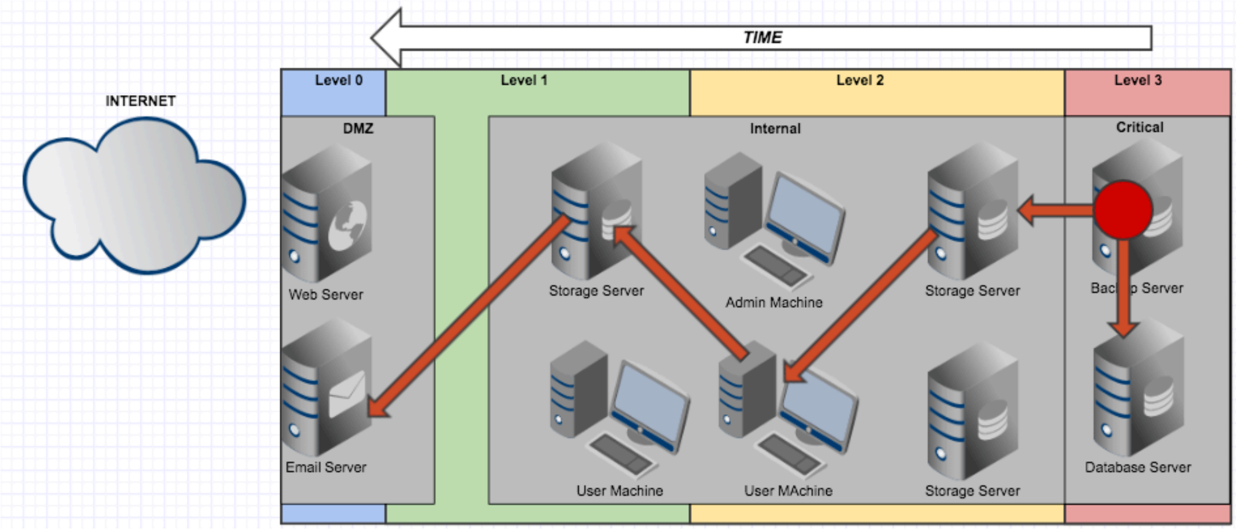
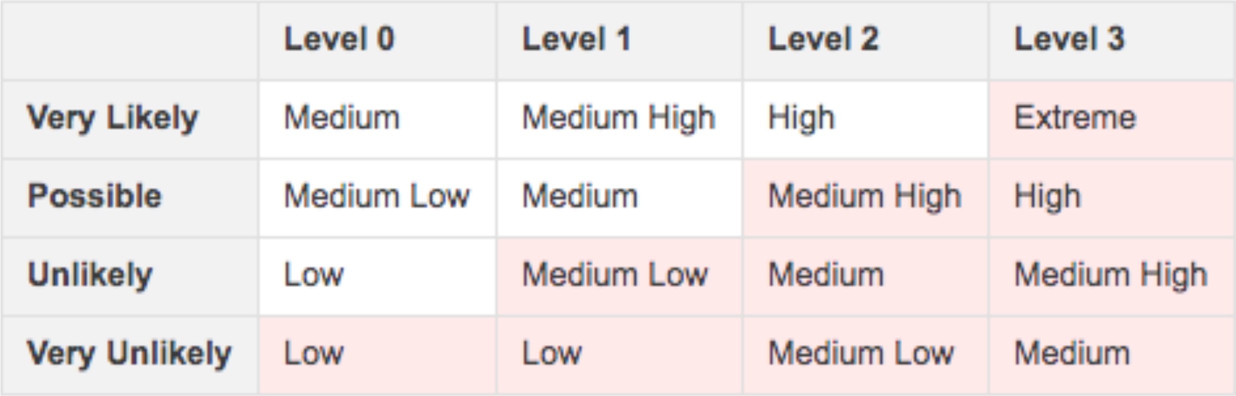


**Figure 20: Critical Perspective Timeline**

Use of this perspective decreases the likelihood that data of level 1-2 will be discovered during the assessment and is much less likely to encounter findings of level 0 data. In regard to overall assessment efficiency of an organization this initial perspective is probably the least effective at covering all levels of risk.



| | Level 0 | Level 1 | Level 2 | Level 3 |
|---|---|---|---|---|
| **Very Likely** | Medium | Medium High | High | Extreme |
| **Possible** | Medium Low | Medium | Medium High | High |
| **Unlikely** | Low | Medium Low | Medium | Medium High |
| **Very Unlikely** | Low | Low | Medium Low | Medium |

**Table 5: Critical Perspective Risk Matrix**

It is efficient at finding level 3 data as it begins on devices hosting such information. This assessment perspective is therefore much more likely to discover findings that result in compromise of level 3 data and as such represent an ability to assess the most extreme levels of risk faced by an organization.

## Initialization Perspective Effect on Attack Surface Coverage

The next comparison to be made between the initial perspectives is the ability of each to scrutinize attack surface during an assessment. This is an extremely important attribute in justifying the validity of a security assessment. Although an assessment may not yield results that cover extremely valuable compromise items it may still be effective if it was able to assess a large portion of the organizations attack surface. The attack surface is comprised of the ways in which an adversary can enter the system and potentially cause damage (Manadhata, et al., 2006). It is extremely important to reduce the attack surface adversaries can utilize (Sun & Jajodia, 2014). It is the responsibility of the security assessment to cover attack surface, evaluating it for vulnerabilities.  Since attack surface represents the opportunity attackers have to compromise the security of systems (Stuckman & Purtilo, 2012) reducing that opportunity is a must for any security apparatus.

All attack surface must not be treated equally though as different parts of the overall attack surface represent potential immediate access to different levels of data. Attack surface consists of all the different points where an attacker could get in to a system (The Open Web Application Security Project (OWASP), 2015)  and that system may be an organization as a whole, or individual devices within it. As Stuckman and Purtilo state, “an attack surface metric does not directly measure exploitability (a system with a small attack surface but many vulnerabilities could be more exploitable than a system with a larger attack surface)” [20]. As an example, there is a wider attack surface represented by internet facing surfaces as they are subject to a much higher amount of attack and enumeration attempts. Yet, as has been shown, vulnerabilities allowing access to internet facing servers may not necessarily be initially crippling to an organization. A dissection of how each initial perspective affects the way attack surface is analyzed will further the case for each of them as valid security assessment perspectives as well as how they together comprise the necessary parts of adequate cyber security evaluation of an organization

### External Perspective Effect on Attack Surface Coverage

The SANS Technology Institute defines attack surface as exposure, the reachable and exploitable vulnerabilities (SANS Technology Institute, 2016). The internet facing portions of an organization are the most exposed and are reachable by the largest audience of users and attackers. As such the internet facing layer of the network can be classified as having the most attack surface. Vulnerabilities present here may not lead to the direst of consequences if exploited yet this is the most likely place they will be found. The nature of creating services available to internet users is something most modern organizations have had to accept as adding to their risk faced. External perspective for security assessment offers the most straight forward method for evaluating this surface.

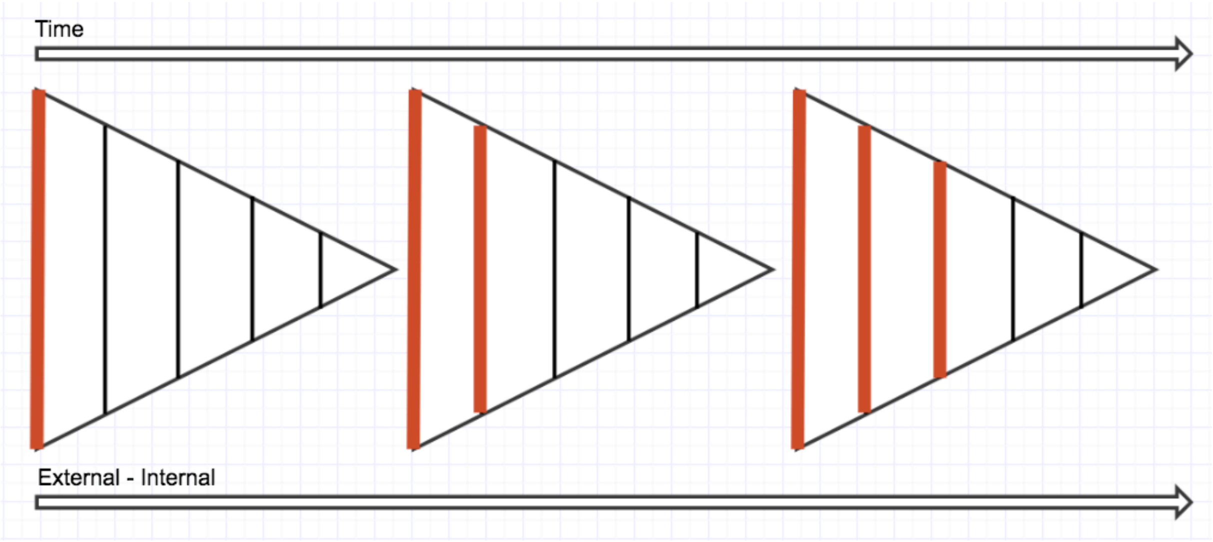


**Figure 21: External Perspective Attack Surface Analysis**

The external perspective allows for covering large swaths of the attack surface an organization presents however there are periods of time before this assessment reaches deeper into the network if at all during a test. The figure above shows the attack surface evaluated in red and how the assessment transitions to deeper portions of the attack surface with time. At initialization, the first attack surface pyramid shows how the external perspective only sees the external attack surface of the organization. The second pyramid represents the middle of an assessment from the external perspective and how it will have reached an ability to assess attack surface deeper within an organization. The third and last pyramid shows the end of the assessment and how it has assessed parts of the organizations deeper attack surfaces but not all of it.

### DMZ Perspective Effect on Attack Surface Coverage

Beginning an assessment in the DMZ removes the need for a vulnerability that allows the assessors to pivot past internet facing defences. As such, assessments with this perspective are more immediately able to assess the other devices in the DMZ and identify their vulnerabilities presented via lateral enumeration.

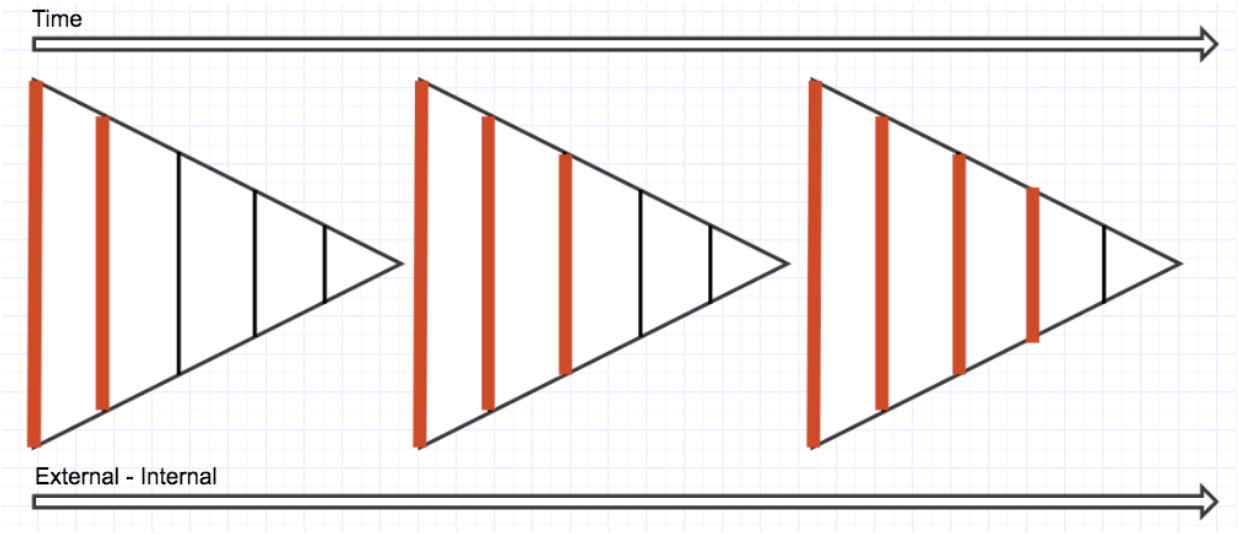


**Figure 22: DMZ Perspective Attack Surface Analysis**

As Fig. 15 indicates a DMZ perspective test requires no time to begin assessment of devices in the DMZ. It is also able to begin probing the internal network in a quicker fashion than the external perspective. This is due to the external perspective needing the bulk of the organizations external attack surface must first be addressed before moving on. One potential obstacle faced by this assessment perspective however is that it could fail to identify vulnerabilities present to internet-based scans and attacks as devices in the DMZ should be talking to the internet but not each other (Chapple, 2012).

### Internal Perspective Effect on Attack Surface Coverage

Assuming the mantle of the insider threat the internal assessment, perspective is the benefactor of starting even deeper in the network and having access to more attack surface. This also means that like the DMZ perspective the ability to assess an organizations internet facing threat vectors are not easily done and in fact could be quite time consuming from this context.

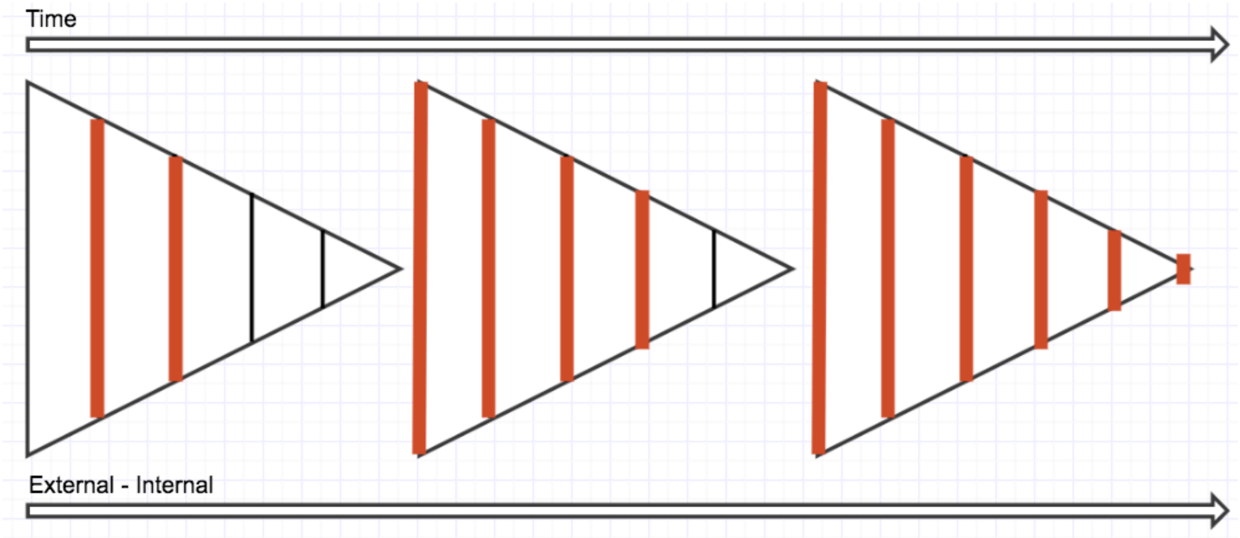


**Figure 23: Internal Perspective Attack Surface Analysis**

The benefit of internal assessment perspective as an initial point for an engagement is that the attack surface analysed in the immediate environment is likely to lead to vulnerabilities that can compromise data an organization has no intention of being made publicly available. This is contrary to the external and DMZ assessment perspectives which may find a lot of less meaningful vulnerabilities across a larger more internet accessible attack surface.

### CAPTR Team Critical Perspective Effect on Attack Surface Coverage

The critical perspective analyses by far the least amount of an organizations attack surface. Diametrically opposed to the external perspective which begins focusing on an extremely large surface the critical perspective focuses on a prioritized portion. From this point, it is unrealistic to assume that an assessment beginning from this perspective will be able to assess internet facing services in any reasonable timeframe. This method is intended to provide most efficient analysis of the most dangerous attack surface relative to the high impact objects.

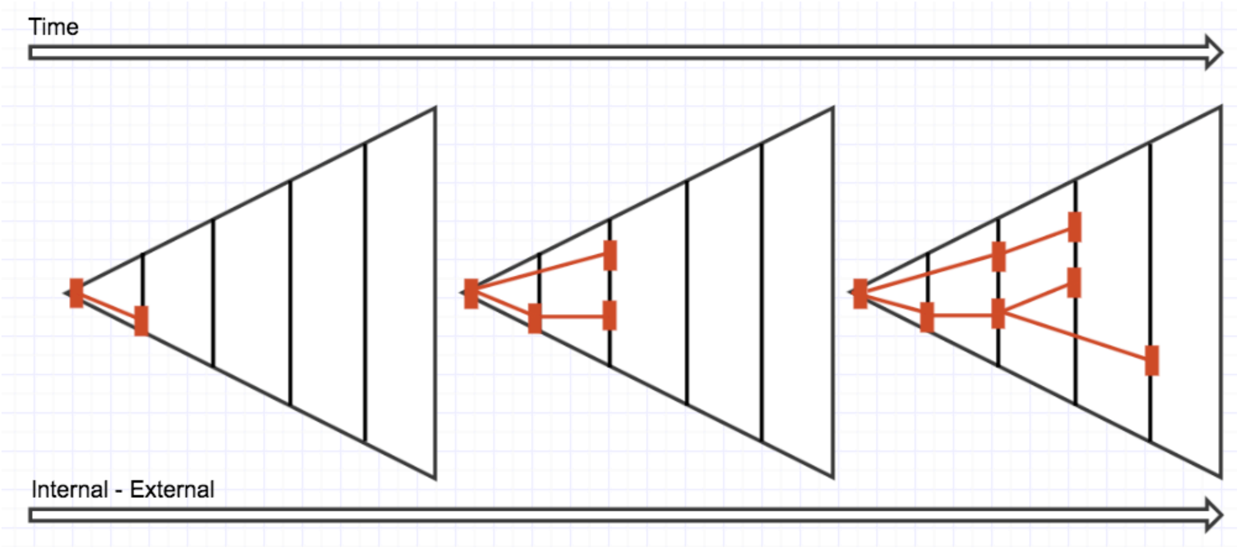


**Figure 24: Critical Perspective Attack Surface Analysis**

The way a critical perspective assessment approaches different parts of the organizations attack surface also varies from the other three methods. For example, the most value can be gained from the external perspective when it finds as many vulnerabilities in the internet facing perimeter of an organization as possible. This likely means that assessors would not leverage identified vulnerabilities to move deeper into an organization until they deem the entirety of that external surface has been evaluated. This attempted complete attack surface coverage is a necessary part of the other assessment perspectives. The critical perspective does not need to evaluate the next layer completely. The critical perspective instead focuses on how attackers could pivot to the data or machines of unacceptable loss. Instead of looking for all the vulnerabilities in attack the surface it focuses on those points that enable the access to pivot towards lethal and critical items of compromise.

## Initialization Perspective Advantages / Disadvantages

The purpose of security assessment is intended to reduce an organizations overall risk and each of these perspectives are valuable in their own right. The sum of these methods should then result in an effective security assessment strategy that covers as much of the organization attack surface as possible and identifies as many threats as possible. This then allows the organization to mitigate the maximum amount of risk.

When attempting to compile a comprehensive security assessment not all initial perspectives may be realistic due to any number of circumstances. It is therefore imperative to go beyond the value of each with regards to attack surface and risk assessment and delve into additional advantages and disadvantages of each. This will allow assessors to not only know which perspectives are most needed, but which are most feasible in any given assessment scenario.

### Advantages / Disadvantages: Introduction of Risk

In any security assessment prior to testing, the extremely important steps of establishing the scope and rules of engagement must be completed. These items identify the techniques and methods and especially what is to be tested (That Security Blog, 2016). The scope of the assessment and the rules of engagement are established as part of the pre-engagement interactions (pentest-standard, 2014). This means that before the security of an organization can even start being evaluated there are strict processes detailing how the test will be performed. Different initial perspectives present different complexities with regards to understanding and agreeing upon a scope and rules for the test. These two items of scope and rules of engagement are how an organization finds an acceptable level of risk that may be introduced by the test.

This risk manifests itself in two ways. First, a security assessment may bring risk to an organization by possibly denying a service which may involve introducing large delays, excessive losses, and service interruptions (Mirkovic, et al., 2006) through assessment activity. Second, the access needed by the assessor to conduct the assessment from a given perspective may increase the overall attack surface or its severity.

### *External Perspective & Risk Introduction*

The attack surface initially evaluated by the external perspective is intended to be made up of devices and services purposefully made available to the internet. This means they should be expectant of attacks and large amounts of traffic. There are even external entities that help mitigate internet-based denial of service to subvert the risk posed by any internet sourced traffic which would include that of the assessor (Brustoloni, 2002).  However, the added strain imposed by scanning and exploitation attempts can still bring devices down. Though low, this source of risk must be considered since loss of one of the internet facing services likely impacts external and internal users of the organization. Since the assessor does not need an established internal access to conduct the assessment from an external perspective there is no additional attack surface added by the execution of such assessments.

### *DMZ Perspective & Risk Introduction*

Similar to the external perspectives the DMZ perspective initially focuses on devices and services intended for internet-based traffic. The risk posed by potential outages caused by the assessment is similarly low. No additional risk should be presented by the assessor accessing devices in the DMZ as the purpose of the DMZ is to isolate accessible hosts from the rest of the organization (Schmidt, et al., 2007). There is a slightly higher chance of unintended consequences from scanning and exploitation attempts as the DMZ assessment perspective tests devices from a lateral position in the DMZ instead of from the internet. There is a chance that devices are not prepared to handle this lateral traffic which could cause issue. This perspective requires an established point of presence within the DMZ to begin assessments from. Although this allows the assessor to start one level deeper into the organization the risk is still negligible. The access handed to the assessor is isolated from the internal network by nature of being in the DMZ and therefore poses little additional risk due to the additional attack surface of its initial assessment vector.

### ***Internal Perspective & Risk Introduction***

Assessments from the internal perspective are immediately able to interact with devices and services not intended for public perusal. These devices are much less likely to cope with heavy scanning or exploitation attempts and therefore there is a risk to assessing devices from this perspective. A denial of service here is more likely to result in lack of availability for internal users compared to external users. Additionally, an outage caused by this assessment is more likely to impact organizational functions. The internal perspective also poses an increase in attack surface. With the necessity access being granted by the organization or a successful introduction of malware, an assessor using this perspective introduces additional means of access into an organizations interior.

### ***CAPTR Team Critical Perspective & Risk Introduction***

Relative to the other initial perspectives the critical perspective represents a high level of risk to an organizations ability to function. The items that constitute the point of presence where such an assessment begins are those identified as extremely critical to an organizations ability to exist. Any issue caused to such devices by the assessment are likely to prove damaging to an organizations ability to function normally. The risk created by an increase to attack surface is also relatively high. Like the internal perspective the critical perspective requires the introduction of an access vector by the organization to begin the assessment. The attack surface added to the organization by this access vector is more dangerous as it is a direct line to the critical comprise items. A compromise of the access vector used by the assessor would be extremely dangerous to the organization and extreme care should be taken with this type of assessment.

### Advantages / Disadvantages: Coordination Burden

In addition to the coordination required to form an acceptable scope and rules of engagement there is also the potential for further burden of coordination before and during an assessment. As mentioned before, different assessments may require collaboration with organizational staff to enable access required for an assessment. There is also a need to maintain communications in varying levels during an engagement to insure there is no confusion between real attack attempts by malicious actors and those of the assessor.

#### *External Perspective & Coordination Burden*

With no need to have an organization enabled point of presence to start evaluation this perspective requires little to no collaboration to begin the assessment. There is also minimal need for ongoing communications with the organization staff while engaging from this perspective. The assessor would need to communicate with staff if a vulnerability was discovered that allowed for transition to a new perspective inside the organization to avoid confusion between a real attack and the assessment.

#### *DMZ Perspective & Coordination Burden*

Initially this assessment perspective does require collaboration to introduce an access point within the DMZ from which to conduct the test. Similar to the external perspective ongoing collaboration however is in a limited fashion and typically only to provide de-confliction.

### *Internal Perspective & Coordination Burden*

Access to conduct an assessment from this perspective is typically achieved in one of two ways. An exploit event and outcome are simulated to give the assessor contextual access to an internal point of presence. There is also the ability of an assessor to conduct a social engineering campaign in an attempt to get users in the organization to visit a malicious site or open a malicious email that allows the assessor to then gain internal access. There is a need initially to enable access or an ongoing need to monitor the organization to ensure that such a campaign is not confused with a real attempt by an attacker. Additionally, there may be a need to ensure that any notice of the campaign by users in the organization does not impact its ability to compromise others and still allow the assessment to begin from that perspective.

### *CAPTR Team Critical Perspective & Coordination Burden*

This assessment has no way around requiring organization collaboration to create an initial access vector. Unlike the previous examples of perspectives requiring organization enabled access this assessment perspective presents more challenges. In other perspectives, the organization may simply execute a tool for the assessor to enable access. There is a high level of risk involved and atypical traffic requirements potentially necessary to enable access deep within an organization at its critical points. The organization and assessor must create an access vector that creates as little additional risk to the organization as possible and the staff are likely to favour ongoing cognizance of the assessor's activity.

## **Advantages / Disadvantages: Emulated Threat**

Security assessments such as red teaming and penetration tests are attempting to emulate an attack (Wood & Duggan, 2000) (Kirsch, 2013). The different perspectives discussed provide and assessor the ability to represent different types of threats to an organization. According to

Rusell and Gangemi attackers can be classified in four primary methods of Organized Attackers, Hackers, Amateurs and Insiders (Russel & Gangemi, n.d.).

Organized attackers are the ones with resources and motivation and are specifically targeting an organization. This category also represents advanced persistent threats or APTs which are intent on breaking into an organization with the goal of stealing or compromising information (Siddiqui, et al., 2016). Hackers may be perceived as benign explorers, malicious intruders, or computer trespassers (Hafner & Markoff, 1991). The main difference between hackers and organized attackers is the resources backing the attacker. Amateurs are also known as "script kiddies" and are less skilled often using existing tools and instructions that can be found on the internet (Han & Dongre, 2014). It is worth noting then how each perspective provides emulations of these different threats. An assessment started with any of the four initial perspectives has the potential, as time is spent on the engagement, to obtain a point of presence in an organization that facilitates assessment from a different perspective. The following statements are strictly with regards to the initial focus of each perspective and the threats they are immediately emulate.

### *External Perspective & Emulated Threat*

With no need for access to the network to perform an assessment the type of threat this perspective most readily represents is amateurs.

### *DMZ Perspective & Emulated Threat*

Representing a need for an already successful exploitation of a vulnerability that would provide an attacker the ability to pivot into the DMZ of an organization this perspective closely resembles the ability and intentions of a hacker.

### *Internal Perspective & Emulated Threat*

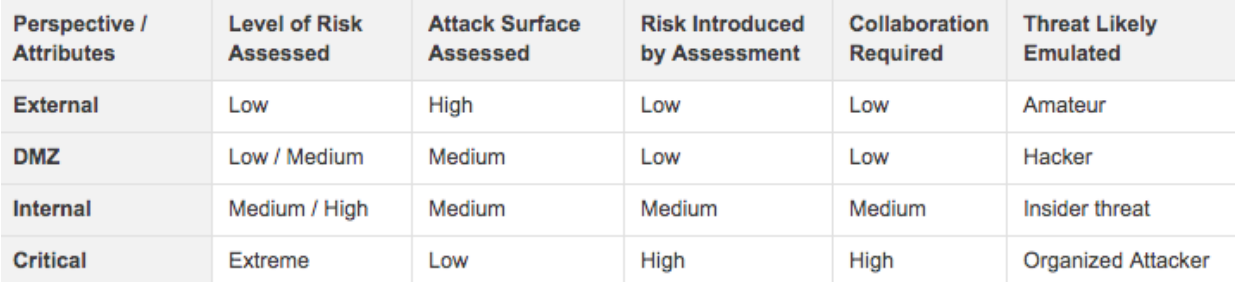
The Internal perspective represents multiple threats. Here the insider threat is represented since the access needed for an assessment from this perspective requires access to a device within the organization. Additionally, due to the ability of hackers to target individuals who work in an organization using social engineering to deploy their malware it is realistic to assume the threat of hackers can be represented by the initial focus of this perspective.

### *CAPTR Team Critical Perspective & Emulated Threat*

This perspective is intended to emulate the targeting of the availability, confidentiality or integrity of critical items. It is therefore most likely to represent the threat of an organized attacker. There is a need to gain access or begin from within the network as an insider or hacker might. Then attackers would continue that by pivoting deep into the network with the goal of compromising specific items required by the actor's motivations.

## Taxonomy of Initialization Perspectives

This analysis indicates that all four initial assessment perspectives bring advantageous and disadvantageous aspects to cyber security evaluations.



| Perspective / Attributes | Level of Risk Assessed | Attack Surface Assessed | Risk Introduced by Assessment | Collaboration Required | Threat Likely Emulated |
|---|---|---|---|---|---|
| External | Low | High | Low | Low | Amateur |
| DMZ | Low / Medium | Medium | Low | Low | Hacker |
| Internal | Medium / High | Medium | Medium | Medium | Insider threat |
| Critical | Extreme | Low | High | High | Organized Attacker |

**Table 6: Taxonomy of Initial Perspectives**

All four perspectives together comprise the most complete representation of manual attack simulation by ethical hackers against organizations. This taxonomy also indicates that the proposed critical perspective is an assessment initialization point that provides a valid evolutionary step in allowing for better mitigation of insider and advanced threats.

## Traditional Red Team Process

he EC Council organization which awards individuals with the "Certified Ethical Hacker" certification describes the phases of a penetration test as Reconnaissance, Exploitation, Post-Exploitation (EC-Council, 2017). This process is typically executed from one of two points of presence. Traditionally the assessment will start from a point on the internet completely external to the organization and attempt to gain access from that vantage. A red team assessment or penetration test against an organization is typically going to follow a process of gather information, identify vulnerabilities, and attempt to exploit. If this process leads to compromise of a layer of the defense, then it is started again from the newly gained point of presence in that layer.

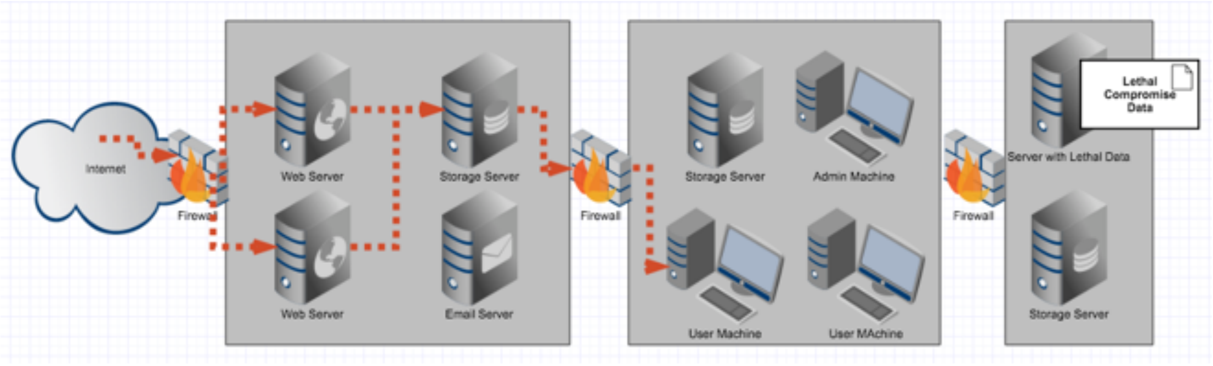


*Figure 25: Red Team Process*

In recent years phishing has become the most utilized means to maliciously access an organization. Verizon's 2016 Data Breach Investigations Report indicates that the attack surface provided by malicious emails known as phishing has grown to become more prevalent than any other method of attack (Verizon, 2016). The report also states that almost a third of phishing emails get opened showing just how effective this attack method can be.

As a result, penetration tests have evolved to incorporate spear phishing as an addendum to the normal attempts at access. In these tests, the penetration test phases begin with a point of presence of being on a user machine after that user has opened a malicious email. In some cases, the penetration test also incorporates the phishing attempts to evaluate the likelihood that members of the organization will open malicious emails.

It is worth noting in traditional red team assessments that layers deeper within the defenses may never get evaluated if the outermost accessible layer is not compromised and bypassed by the red team. This is due to the methods involved in red teaming as written described by The NATO Cooperative Cyber Defense Centre of Excellence (Brangetto, et al., 2015) “penetration testing happens, against the team’s own systems. Like adversaries, starting from the outer layer of the network”. Thus, a layer without identified vulnerabilities ends the progression through the organization.

## Traditional Red Team Shortcomings

There are several reasons why shortcomings exist in relying solely on traditional red team assessments to evaluate cyber security and mitigate the impact of APTs. These issues are due to a constantly evolving threat landscape where, “cyber war now exists, and cyber criminals benefit from the arms race” (Investopedia, 2017). A list of vulnerabilities exposed during an assessment can become outdated days after the test is concluded. Another reason is that typical red team activities focus on emulation of attackers and not all aspects of internal threats. This is supported by (Brangetto, et al., 2015)“cyber red teams focus on ‘how systems fail’ instead of ‘how systems work’. Starting from the outermost layer”. Lastly there is a focus on disclosing identified vulnerabilities yet little or no focus on identifying and preventing exfiltration of data.

Many security vendors suggest that their assessment methods incorporate or address APT attacks. The issue is a lack of publicly available documentation into how these security vendors or organizations are exactly doing so. This is not surprising since such techniques are likely valuable trade secrets that give an edge over competition. There is also little specific or general work in academia towards improving offensive security assessment performed by ethical hackers. The CAPTR team assessment provides an academically researched effort into improving manual offensive security assessment by ethical hackers with a focus on APT mitigation.

## Zero-Day Vulnerabilities and Exploits

A zero-day exploit is code that takes advantage of a zero-day vulnerability. A zero-day vulnerability is one that is unknown to the software maker or security vendors (Zetter, 2014). In the process of a penetration test the red team will scan for vulnerabilities and attempt to leverage them and gain access to the organization. Wai suggests testers should have a collection of exploits and vulnerabilities at their disposal (Wai, 2002). The issue is that such a collection will not incorporate zero-day exploits as they have not been disclosed or discovered yet.

In fact, on their website MITRE wrote “Due to the ever-increasing volume of public vulnerability reports, the CVE Editorial Board and MITRE determined that the Common Vulnerabilities and Exposures (CVE®) project should change the syntax of its standard vulnerability identifiers so that CVE can track more than 10,000 vulnerabilities in a single year.”

(MITRE, 2015). Further, in their 2016 Internet Security Threat Report, Symantec (Symantec, 2016) revealed that in 2015 there were 54 zero-days discovered. This means that each year there are thousands of zero-day vulnerabilities discovered and each week there is at least one new weaponized zero-day exploit. It was an increase of more than 100% from the previous year and if that trend continues it could mean a new zero-day exploit every few days in years to come.

Given this data it could be assumed that once a red team completes a penetration test, less than seven days later there is a chance that a weaponized vulnerability exists as a new threat to the organization. There must also be an assumed notion that portions of the network that were unreachable by the red team may have low hanging fruit vulnerabilities that were not able to be assessed due to some device(s) not having vulnerabilities between the assessors and those items. In this instance if the devices that stopped the red team assessment are vulnerable to a new zero day, an attacker may be able to have unprecedented impact using those low hanging vulnerabilities. This is a generally an accepted part of red teaming that unevaluated portions may contain vulnerabilities.

### Insider Threats

In simulating an attack red teams can miss one of the largest sources of cyber compromise and data loss which are insider threats. In their report, Intel Security reports that 43% of compromises were resulting from internal actors (Intel Security, 2015). Over half of those compromises were intentional with the rest being accidental. The accidental internal compromises are in some part addressed by certain red team assessments such as when the team attacks a network from a point of presence simulating access gained by spear phishing.

The same can be said of running a spear phishing campaign during a penetration test however this may limit successful testing of defenses if no users open the malicious email during the time of the test.

Intentional insider threat is a point of attack that traditional red team assessments do not evaluate since they are typically tasked with simulating the attacker and not a defector or already present malicious actor. This means that in a report from a penetration test there could be an entirely unevaluated attack surface that comprises over 20% of all sources of data breach. These types of compromises are also some of the more impactful ones as stated by Carroll “Intentional compromise of information by an insider may very well be the bigger of the two threats since the insider knows what he or she can use to their profit from or simply to damage the organization” (Carroll, n.d.).

**Exfiltration**

With a focus on identifying, exploiting and reporting vulnerabilities the red team penetration test leaves a very important piece of cyber compromise and data breaches often unevaluated. The ability to exfil data out of a network once it’s compromised is the goal of an APT and is one of the characteristics that sets APTs apart from other hackers. There is a chance the actor attacking an organization is doing so for fun or curiosity, but any motivated attacker is there to either destroy or gather information. Being able to impact a hacker siphoning data out of the network is potentially more valuable to an organization than identifying the vulnerability that let the hacker inside from the internet.

The average time it takes to discover an attack is 146 days according to Mandiant’s FireEye report from 2016 (FireEye, 2016). This length of time between successful compromise and eventual detection highlights the need for security assessments to affect exfiltration of data. In a white paper, Clayton wrote “Once the intruders have seized control of target systems, they may proceed with the theft of intellectual property and other confidential data.” (Clayton, 2011). Since red team assessments follow an outside-in approach they can be poorly positioned to assess potential ways to get information from deep inside an organization out. This is a large portion of an APT attack that is not often simulated by traditional red team assessment and therefore not often reported by it either. Since Secureworks reports exfiltration as a key characteristic of APT compromises (SECUREWORKS, 201) this is an issue that cyber security tests need to evolve to assess. The red team has to exploit its way deep in to the network to get close to or compromise critical items to the organization. If the red team isn’t able to find vulnerabilities to get all the way to critical data, it will not be able to provide exfiltration points and pathways from the devices hosting critical data.

### Efficiency

In an offensive security assessment, identifying and exploiting vulnerable devices is what generates the reportable items at the end of a test. That does not mean that every device exploited during a test is of the utmost importance or that an organization will care or bother to address an issue found with all the devices in a report. It is possible that during a test, hours may be spent exploiting an identified vulnerability on a device only to learn it is a decommissioned server with no relevant data and hosted in a cloud environment connected to no other devices in the company. Even ignoring potential time sinks during red team operations it is not the only issue with regards to efficiency. The red team is trying to find all the holes in the defenses of an organization and an APT is only trying to find one. This means that by nature the red team is going to spend more effort on finding more vulnerabilities than the specific one that could lead an APT deeper into an organization. NIST states that “Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability.” (Scarfone, et al., 2008).

This is a correct and necessary approach to assessing security given the breadth of malicious activity any organization with an internet presence faces. It is important to note that many vulnerabilities could be discovered during a red team penetration test, none of which enabled access to critical items. As such, these tests are not well suited to evaluating the very particular items that could be leveraged by APTs as opposed to those utilized by conventional hackers, script kiddies and automated attacks. The priority of a red team is to identify vulnerabilities in the organizations attack surface most likely to be exposed to attackers. The most attacked part of a network are the parts accessible from the internet. The attack surface of the internet facing layer of organizations is constantly growing, adding to the challenge. It is not only the public websites that companies now must worry about. Stevens reports 93% of companies surveyed use the cloud and 88% of them utilize public clouds such as Amazon Web Services or Microsoft Azure (Stevens, 2016). This is a growing trend according to Boulton (Boulton, 2016), with Berger and Jones indicating that “Use of online networks containing large volumes of internal and external data has become the norm for every business.” (Berger & Jones, 2016). This will continue to increase the advantage APTs have over red team assessments as Guarda, et al. similarly concludes “Virtual Environments have a higher exposure to cyber-attacks” (Guarda, et al., 2016).

**Introduced Risk**

There is risk inherently involved in conducting offensive security assessments. Exploitation requires using potentially unstable exploits such as buffer overflows in system processes like MS08-067 (Microsoft, 2008) or kernel race conditions like Dirty COW (US-CERT, 2016) (Verton, 2016) which can crash the target system. When a red team engagement closes in on those items of critical or lethal importance to the organization which might be the target of APTs, the risk goes up. This is the cost of business when there is a security need for offensive security assessment. There are mitigating factors during an engagement to help prevent risk such as scoping and rules of engagement which are determined before the test begins. There is still risk to in scope items and unforeseen consequences of remote exploitation and privilege escalation techniques when going after high risk targets in an effort to simulate attacks by APTs.

## CAPTR Team Addressing of Red Team Shortcomings

CAPTR teaming is an augment to the security assessment process currently undergone utilizing red teams and penetration tests. It provides a unique evaluation process that mitigates the areas found lacking in traditional red team assessment.

### Addressing Zero-Day Vulnerabilities and Exploits

The potential for zero-day vulnerabilities turning into zero-day exploits presents the possibility of holes in defenses that will escape analysis. The CAPTR team method allows for some mitigation of the impact of new zero-days on the effectiveness of the assessment. Consider the below diagram portraying a simplified example red team engagement.

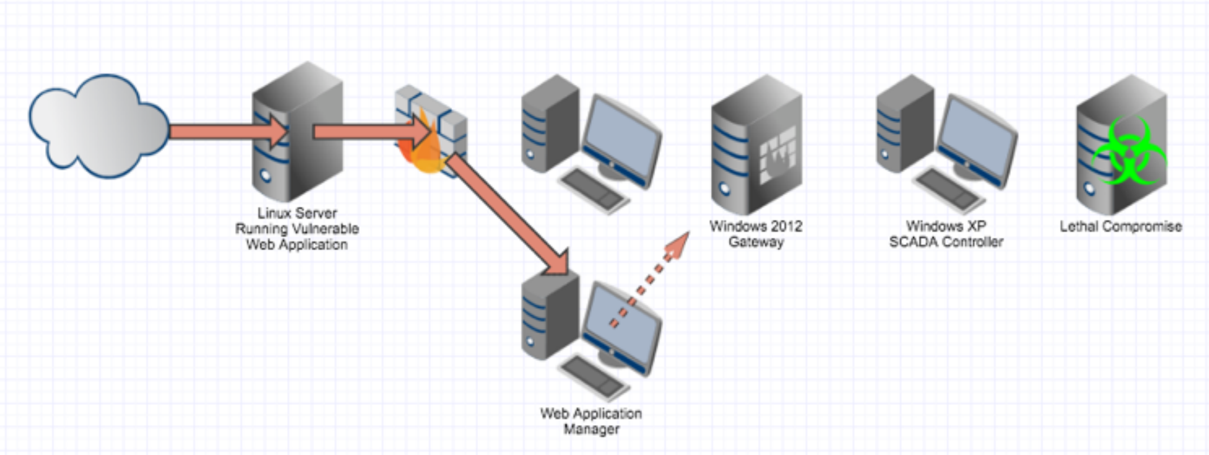


*Figure 26: Red Team Path*

Here the red team exploited an internet facing web application server and from there pivoted to the web application managers personal machine after capturing his credentials and identifying his IP address when he logged in to the server to check on it. Next the red team tries to move deeper into the network towards the lethal compromise in this case a SCADA device controlling bio-hazardous waste distribution. Unfortunately, a Windows 2012 gateway is between the red teams pivot point and the lethal compromise and currently has no known remote code execution exploits. In this example, the red team never gets to enumerate the SCADA controller to see that it is vulnerable to a commonly known remote code execution vulnerability such as the earlier mentioned MS08-067. Shortly after the assessment the MS17-010 zero-day vulnerability and exploit is disclosed on the internet and an APT who compromised another user in the network via spear phishing uses it to get past the Windows 2012 gateway. Now the APT can easily exploit the vulnerable SCADA controller and ultimately the SCADA device itself because that device is vulnerable to the semtex privilege escalation technique allowing an attacker to stealthily cause a catastrophe.

Next consider the below diagram portraying an equally simplified CAPTR team engagement.

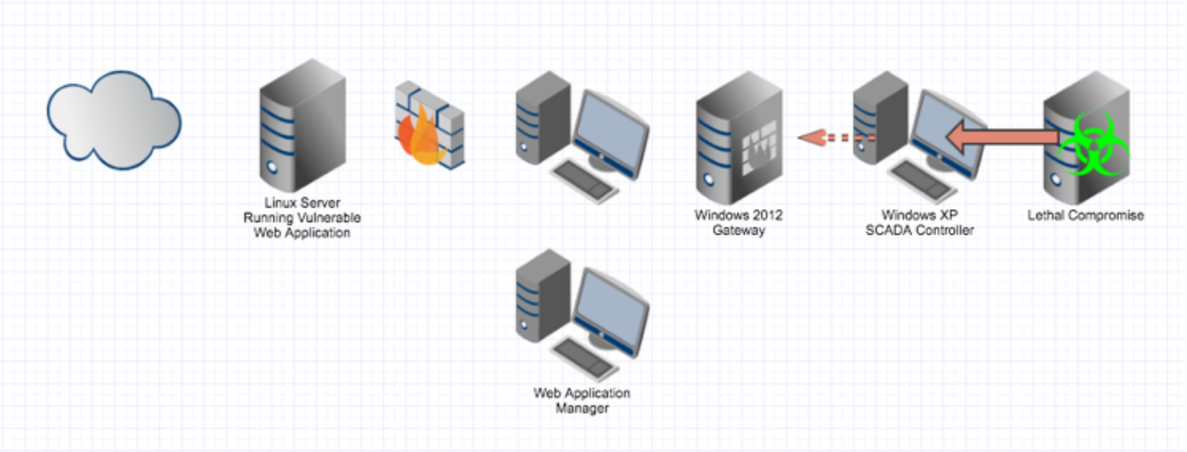


*Figure 27: CAPTR Team Path*

Here the CAPTR team started its assessment on the lethal compromise SCADA device. It discovered the local privilege escalation vulnerability on the SCADA device. It also identified the SCADA controller in connection information available via the operating system. Next the team identified and exploited the Windows XP SCADA controller however it was unable to pivot further outward due to the same issue of the Windows 2012 gateway having no remote code execution vulnerabilities. The same scenario occurs where MS17-010 becomes publicly available and the APT breaks past it. This time however the APT will be challenged and possibly unable to get on to the SCADA controller or escalate privilege on the lethal compromise since their vulnerabilities were already addressed. This gives the defensive team a leg up in preventing and detecting the APT's efforts against the lethal compromise item and pivot point even with the release of the new zero day. There is no perfect solution to zero days, they will be uncovered, and devices will be made vulnerable. CAPTR teaming does not in any way protect the entire organization from them. It does however insure that the lethal compromise and internal pivot points are assessed first. This provides as much mitigation as possible to a zero-day blowing open highly vulnerable and unevaluated portions of the network that an APT would then get through easily.

**Addressing Insider Threats**

Even an actor internal to an organization will likely have to leverage some vulnerabilities to gain access to those compromise items deemed critical or lethal. Since the CAPTR team assessment begins with the last line of defense and progresses out from there, even a limited set of defenses between an internal actor and these items will have been evaluated by the CAPTR team. An internal actor may not always be a typical insider threat. Weisman defines an insider threat as “a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network” (Weisman, 2014). This does not cover APT hackers who have already established a foothold which should also be considered.

There is an added benefit to this method of focusing on insider threats which are not members of the organization but potentially APTs that already have a foothold in an organization. FireEye describes the final stage of an APT attack stating that “evidence of the APT attack is removed, but the network remains compromised” (FireEye, 2017). This situation played out in the hack of Sony allegedly by North Korea (Fidler, 2014) of and the OPM hack allegedly by China (Levine & Date, 2015). In both cases after initial discovery of the compromise for nearly a year updated and relevant data was taken from these organizations. In a situation such as this CAPTR team assessments will allow an organization to prevent access to the valuable items by identifying likely pivot points within the organization.

Consider the assessments in the CAPTR team path and red team path figures. The APT already had established itself as an insider threat but was initially unable to exploit the lethal compromise or its last pivot point. Since the CAPTR team had already assessed these items and provided mitigations the insider threat faced a greater challenge even after the release of the zero day. There are certainly situations where an attacker or even a disgruntled employee used legitimately authorized accounts to breach parts of an organization and in such a case a CAPTR team, just like a red team, will provide no additional security. The added mitigation comes in situations as those mentioned where an insider whether an APT or a disgruntled employee needs some additional vulnerability to enable their malicious activity. The CAPTR team assessment process identifies vulnerabilities closest to the lethal compromise items and provides defensive entities knowledge about likely pivot points any classification of insider threat may leverage.

## Addressing Exfiltration

Since data exfiltration is the main goal of APTs (Trend Labs, 2013) it is something that the CAPTR team paradigm must work towards impacting in a way traditional red teams cannot. Common methods for stopping exfiltration are egress filtering per Kirsch (Kirsch, 2013) or monitoring with a tool like Splunk (Splunk, 2017). The CAPTR team seeks to test these types of defenses with attempts to achieve covert exfil of data as close to the compromise items as possible and at each point pivoted to.

It is the continued attempts to move outwards from within the organization as the assessment expands that allows CAPTR teams to identify exfiltration issues a red team cannot. Additionally, critical and lethal items of compromise cannot be exfiltrated if there is not access to them. Inherent to the CAPTR team model is initiating the assessment of security starting with these items. Even if an attacker gains access to the organization exfiltration of the most critical data will be mitigated by lack of access following recommendations by the CAPTR team assessment. Additionally, the risk link heat map provides guide to the monitoring and blue team staff of the organization that they can utilize to focus monitoring efforts and tailor alerts to accommodate likely pivot points where data may be brought across and then exfiltrated from the network.

## Addressing Efficiency

It is not that red teaming is a poor use of resources. Red teaming is an integral part of protecting organizations from cyber threats. According to McGeehan red team operations “will exercise incident response capability in a way that further improves all facets of a security program” (McGeehan, 2015). As outlined earlier, there is room for improvement with regards to advanced persistent threats. A core improvement upon the existing security institution of red team assessment by utilization of the CAPTR teams is in efficiency. This is achieved by prosecuting an organization in such a way that identifies those vectors an APT will use in compromising an organizations most precious items.

This efficiency problem is an issue of attack surface. The red team must account for vulnerabilities across the entire surface of each layer of defenses. This forces time to be spent in a way that represents all and any attacks instead of the very specific attacks an APT may enact to achieve end the goal of data theft (SECUREWORKS, 201)the CAPTR team instead focuses not on the whole attack surface of each layer but only the points of presence in each layer that allow an attacker to pivot to or towards a position capable of enabling critical or lethal compromise.

To further illustrate the efficiency point, take the following scenario. A red team identifies a vulnerability in a web application that manages a cluster of database nodes. The red team spends days testing the exploit and then getting on to the server cluster as a proof of concept and to see what data is there. It turns out there is no data in the databases. Worse when t team that it doesn’t matter because that server cluster is scheduled to be decommissioned the following week. This example is theoretical but illustrates the possibility that there are devices a red team may spend a significant portion of time on that end up being wasted findings at the end of the assessment. The CAPTR team model creates a very small scope hand in hand with the organization and focuses on those devices and ones that allow pivoting to them. As such any finding that enables access or provides increased privilege is almost assured to be of importance to the organization and makes more efficient use of the time spent on the offensive security assessment and reporting considerations.

*Figure 28: Attack Surface to Assess, CAPTR Team*

### Addressing Introduced Risk

The CAPTR team assessment process inherently introduces less risk to the host organizations high risk environments. The fact that assessment begins locally from the items identified as lethal risk means there is no threat to them during the offensive assessment by remote code execution vulnerabilities crashing or disrupting them. A traditional red team requires hefty scanning tools such as NMAP (NMAP.org, 1997) to identify targets of interest. The CAPTR team relies on passively attained information on the lethal compromise items to guide the assessment to pivot points where the passive information gathering and targeting process is repeated. The much-reduced reliance on remote scanning tools and remote exploitation of extremely critical systems allows the CAPTR team to provide an offensive security assessment against the high-risk environments likely to be targeted by APTs while introducing as little risk to those systems as possible.

## Evaluation Methodology

Technology and techniques in information security traditionally lend themselves to straightforward assessments of success via measureable results. The ability to determine whether or not a new technology provides a better metric as a solution to a problem is a foundational portion of any argument for its acceptance. The following analysis of established security paradigms and their respective evaluation via experimental methods will highlight the need for a differing process to provide defensible measurement of success or failure of human reliant offensive security techniques such as CAPTR teaming.

## Monitoring Technologies

Monitoring solutions whether focused on network traffic, system activity or user behavior are event driven. The ability to accurately identify and record events is the basic premise of security monitoring.  Improvement on the ability of current technologies to do this can be measured in quantitative statistics such as volume of events, diversity of events or efficiency of monitoring activities with regards to event data collection or resource utilization. For instance, in a paper title “Optimal Positioning of Active and Passive Monitoring Devices” the authors conducted traffic simulation and were able to illustrate the success of their monitoring device deployment model by measuring how it improved detection rates when compared to other related polynomial algorithm driven monitoring paradigms (Chaudet, et al., 2005).

## Encryption Technologies

There is an always evolving race between encryption solutions and the development of computing methods and machines to break them in a short enough span to make them obsolete. Any new paradigm seeking to improve encryption is evaluated against the quantitative measure of time it takes current computing resources to break it. To a lesser extent there are also efficiency concerns with how much resources and time are required for the encryption and decryption of data using the technology. In both cases a clear quantitative benchmark is set by previous technologies that a new paradigm can surpass to establish validity. In the paper “Automated Analysis and Synthesis of Authenticated Encryption Schemes” the authors provided a mathematical framework to generate authentication encryption schemes with guaranteed and provable security of data based on the encryption scheme applied (Hoang, et al., 2015). Such work established quantitative metrics that are easily used to prove the success of such encryption technologies. In a separate paper “Targeted malleability: homomorphic encryption for restricted computations" the authors seek to improve efficiency of different encryption schemes (Boneh, et al., 2012). In both papers encryption scheme success was measured by quantitative metrics.

## Firewall Technologies

The success of firewall solutions is based on the ability to filter and act upon communications streams. Success is measured via analysis of what communication streams are and are not adequately handled by the firewall as well as how efficiently this can be done with regards to time and system resources. Such a standard also allows for a reasonable expectation of measureable success metrics for any new firewall paradigm to prove itself against. This concept of measuring firewall filtering success is represented in its basic form by determining the ability of given rules to act on data as in the paper "Integrating static analysis and testing for firewall policies" (Formyduval, 2009). Though simplified to specific rules, this concept of static analysis and testing of traffic handling, applies to broader firewall technology concepts.

## Offensive Security Assessment Techniques

Unlike other security technologies, offensive security assessment does not easily provide statistical metrics indicative of effectiveness. The art and tradecraft involved in such security assessments mean that the same individuals could assess the same type of network multiple times and have different paths, discoveries and recommendations. Additionally, the statistics that could be measured do not necessarily reflect the quality of work. If one type of assessment found one hundred vulnerabilities and another type found ten it might be deduced that the one which found one hundred was the better assessment method. If the one hundred vulnerabilities were extremely minor and did not lead to any compromise of data or devices and the ten findings of the other assessment method all allowed for remote compromise of extremely important machines and data, it would instead seem the better assessment method. This example clearly illustrates that the number of findings is not always a metric indicative of a good offensive security assessment.

Further, the identification of vulnerabilities is not the end of an offensive security engagement. To provide protective mitigation for an organization the assessment results should provide recommendations on how to fix the identified vulnerabilities to mitigate the risk they pose. Comparing the uniqueness of recommendations from two separate assessment methods should show novelty of an assessment concept. If a new assessment method can be shown to identify differing recommendations for securing an organization compared to established methods, it is at least validated in its diversity. If a new assessment method can show recommendations in keeping with those provided by established means but in a more efficient, safe or otherwise improved fashion it could also be validated.

Similar to the issue presented by quality of findings or number of findings, the recommendations themselves do not protect the organization. The changes recommended by an assessment need to be implemented into an organization and the overall security of that organization evaluated to establish whether or not the assessment provided recommendations that led to mitigation of security threats. Not only is the offensive security assessment process heavily reliant on human involvement but the validation of its results requires implementations by yet another group of humans performing systems administration. Then the organizational security must be re-evaluated by a third group of humans to establish if there was change in the security posture.  Here there is an issue where typical analysis of quantitative data is not only insufficient but likely unavailable in the way other security technologies might measure performance.

Success of the CAPTR teaming concept can be shown with defensible evaluation of the human tradecraft driven offensive security assessment. To accomplish this a framework for evaluating one offensive security assessment process compared to another is provided. This allows for measuring their individual success and comparable novelty.

## Identifying Requirements for Defensible Evaluation

Industry presents several suggestions on how to pick the right offensive security vendor (DARKReading, 2013) (IT Governance, 2018) but not a way of evaluating the methods those vendors utilize in offensive security assessment. Even the National Institute of Standards and Technology doesn't include penetration testing or red teaming services in its Guide to Selecting Information Technology Security Products (NIST, 2003). Normal comparative analysis of quantitative performance will not lend itself towards validation of a new offensive security assessment paradigm. A standard evaluation process is integral to determining success of a security method (Anderson, 2015), so a process must be defined.

Before designing an experiment to verify the novelty and quality of a concept, experiment defensibility requirements need to be established. The following requirements towards defensibility should be met to standardize the actions of the human actors in offensive security assessments.

- Controlled and realistic environment
- Defensible security assessments
- Defensible systems administration
- Emulation of a motivated and sophisticated attacker
- Measureable results and metrics

### Controlled & Realistic Environment

Since the goal of an experiment regarding offensive security is to identify how well an offensive security assessment provided mitigation for threats it must be conducted in an environment that represents real world targets. If assessments were done against unrealistic target networks, there would be no translation to success or failure of the paradigm in actual implementations. Control is important with regards to both users and administrators of a given network as well as outside actors attempting to compromise it. If the assessors conducting one type of assessment for instance were able to leverage a communications path opened by the user running a Virtual Private Network (VPN) the assessment might have findings from a separate part of the organization. If assessors running another type of assessment against the same organization encountered no users running the VPN software during the time window for the assessment they would never have a chance to generate the same findings and recommendations. This type of unfairness in an uncontrolled environment can be shown by any number of other examples such as outages in one location or another. For instance, a certain machine could be powered off during one assessment and during the other the machines might all powered on. It is therefore clear that any evaluation of different offensive security assessments must be conducted in realistic, controlled and identical environments.

### Defensible Security Assessments

When comparing the effectiveness of two different offensive security assessments the performance of those assessments must be as defensible as possible. Imagine a scenario where one type of security assessment is conducted by someone with almost no experience in vulnerability assessment and computer exploitation and the other assessor has over ten years of such experience. The less experienced assessor is not likely to have as many or as impactful findings and is less likely to provide quality recommendations to mitigate those findings. That would be a poor basis to judge the quality of an assessment method against. Any experiment intent on evaluation offensive security assessments must therefore insure that the security assessments are performed by equally qualified individuals.

The recommendations of the security assessors must be within the bounds of reason for an actual offensive security assessment. An assessor could posit the recommendation of unplugging the organization network from the internet or blocking all ports on device firewalls which would certainly mitigate risk of remote exploitation. However, such recommendations are not likely to be applicable to any real-world scenario as they would hinder the operations of the host organization and therefore would not be part of a real security solution.

### Defensible Systems Administration

To determine the impact of assessor recommendations on the security posture of the organization systems administration must be performed to implement changes based on those recommendations. This must also be carried out as realistically as possible. There could be a scenario where the administrator took over one hundred hours to implement the changes from one assessor. If the other assessor recommended changes that only took the administrator ten hours to complete, the comparison between the successes of either version of changes on the network might not be equal.

There is also a possibility that the recommendations from one type of offensive security assessment are outside the realm of realistic expectations for systems administration in the network. If the systems administration were performed improperly it could provide no added security or potentially make a network more vulnerable and therefore prevent comparison of the networks security performance with the assessor recommended changes. Any experiment aiming to determine the success of different offensive security assessment methods must insure that systems administrative implementation of recommended changes is performed in an equal, appropriate and realistic manner.

Changes implemented by systems administration must also be accurate representations of the intent of the assessor provided recommendations. If the systems administrator misinterpreted what the assessor recommendation was asking, it would also skew any ability to defensibly compare the success of one type of offensive security assessment over the other.

### Emulation of a Motivated and Sophisticated Attacker

With regards to evaluating the mitigating factors introduced by systems administrators based on the assessor produced recommendations, the need for an emulated motivated and sophisticated actor is extremely important. Implementing security changes and then waiting to see if non-emulated attackers are able to compromise different portions of an organization is not defensible.  It would be nearly impossible to guarantee a situation where a real cyber-attack was conducted with motivation against host organizations secured by the assessor recommendations. It would also be nearly impossible to determine the true motivation of real actors. The actor going after one network may be only a curious hacker or even an automated attack script and the attack against a second network could be an APT intent on some data or user within the network. Use of non-emulated actors creates an untenable situation for an experiment to present reliable or realistically defensible results.

Emulation of the malicious actor allows the experiment to provide an equally motivated attack campaign against networks secured by assessor recommendations and then as equally and defensibly as possible determine the ability of those changes to thwart the attacker. There is a necessity of both offensive security assessment secured networks to face equal levels of sophistication during the malicious attack campaigns waged against them. Equal motivation and sophistication of threats faced during experimentation is only available via emulated threat actors. This emulated actor should also represent a realistic threat commiserate with what real world organizations may face. Regardless of actor motivation, if the capabilities for computer exploitation do not extend beyond the use of automated exploit frameworks, the experiment may result in a false sense of security where the network actually possesses little to no defense against real world threats.

### Measureable Results and Metrics

If all other requirements for defensible experimental evaluation of offensive security assessments can be accomplished there is still the need to provide a measureable metric. Such a metric must determine the level success or failure that assessor recommended changes had in enhancing the security posture and threat mitigation of an organization. Without such a metric, there is no way to determine a quantitative difference between offensive security concepts.

Without measuring the comparative effectiveness of offensive security assessments there is no way to validate a new paradigm as being an improvement upon existing methods in a given situation. As discussed earlier such a metric must go beyond number of findings by assessors. For the same reasons success or failure cannot be measured by the amount of machines compromise by the emulated actor. If the emulated actor compromised ten unimportant user machines in one network yet in the other compromised two servers, the email server and the file store server, the two would seem to be more dangerous to the organization than the ten.

To determine validity of an offensive security assessment concept in comparison to others, measureable metrics representing realistic impact to the organization must be identified.

## Evaluation Mediums

Potential underlying test beds for such an experiment have four possible categorical mediums. The basic traits of these potential experiment mediums are based on the real or simulated nature of the environment and the real or simulated nature of the malicious actors. A real environment is considered for the purpose of this categorization to also have real systems administrators and a simulated environment is considered to have its own simulated systems administration.

### Real network with real attackers

If this scenario were used for an evaluation medium it would suffer from many drawbacks with regards to satisfying the defensibility requirements this dissertation has levied. With a real network and real attackers, the environment will be realistic and translate to real-world situations. However, there would be no experimental control over the organization or its network. Security assessment would not be defensible as too many environmental variables could differ across the different engagements. Using real systems administrators means that different administrators could perform different changes for the different actors and they may not want to comply with assessor recommendations if they do not agree with them. This would not allow for evaluation of the recommended changes. Relying on real attackers to engage the organization during experimental windows means there is no guarantee on similar attacks as the sheer breadth of variance in entities targeting organizations can be over 8000 in as little as a year (Polychronakis, et al., 2008). It can be difficult to determine if a motivated attacker is trying to compromise the host organization during the evaluation period. Further, it would prove almost impossible to determine the level of sophistication of attackers between different evaluation windows if attackers were present at all. Any metrics gathered during an experiment on such a medium would be unreliable at best and unsatisfactory as experimental results towards the validation of offensive security assessment methods.

### Real network with simulated attackers

If this scenario were used for an evaluation medium it would also suffer from drawbacks with regards to satisfying the defensibility requirements this dissertation has levied against experimental validation. It is worth noting however that the supplement of simulated attackers for real ones does increase the potential for this option.

With a real network and simulated attackers, the environment will be realistic and translate to real-world situations. Like before, there would be no experimental control over the organization or its network. Security assessment would not be defensible as too many environmental variables still exist that may differ across the engagements of the different offensive security assessment methods being evaluated. Using real systems administrators still provides the possibility different administrators could perform different changes for the different assessors and they may not want to comply with assessor recommendations if they do not agree with them. This is the same type of issue that makes it difficult to judge the effectiveness of security policies in an organization (Mallouli, et al., 2007). Using simulated attackers allows for an equal level of motivation and sophistication with regards to attacks against the secured networks however the presence of real users and real security measures used by the organization still presents pitfalls for successful attack simulation and evaluation. Any metrics gathered during an experiment on such a medium would still be unreliable as too many variables are left uncontrolled and potentially unequal between engagements.

### Lab network with real attackers

If this scenario were used for an evaluation medium it would suffer from limited drawbacks with regards to satisfying the defensibility requirements in the attempt at validation of offensive security assessment paradigms. Use of real attackers on a controlled lab network does increase the defensibility of experimentation however it still has issues.

A lab network in lieu of a real organization network, using real attackers, would in the immediate seem to present satisfaction for a controlled and realistic environment this is not fully the case. Multiple real attackers could be acting against the organization at the same time and create the potential for hampering each other's progress as well as possibly creating situations that would allow for unnaturally expedited compromise of systems. There is also liability concern in such experiments where attackers could leverage the lab network for further exploitation of other targets (Mokube & Adams, 2007). The lab network can be created in the image of a real organization and therefore translate to real-world situations. Yet, the inability to guarantee behavior of the actor means there is no ability to guarantee control of the lab network throughout the experiment. As long as security assessment of the lab network was conducted prior to being connected to the internet to face real attackers the assessment of the network will at least be defensible as environmental variables can be guaranteed to be equal during the assessment periods. As was the case previously with use of real attackers, motivation and sophistication cannot be guaranteed to be defensibly equal across the different engagements of the experiment. In such a setting it can be difficult to distinguish between what was malicious activity or simply user mistakes which is a challenge seen in experiments using labs and honeypots with real attackers (John, et al., 2011).

Since there is no guarantee on the effort of the attacker across given engagements the metrics do not defensibly represent the effect of different assessor recommended changes on the security of networks.

### Lab network with simulated attacker

In a scenario conducted on this medium, an experiment is capable of achieving all of the defensibility requirements levied by this dissertation.

Utilization of a lab network allows for a controlled environment. As long as it is created in the image of a real organization, it will be realistic, and findings of experiments conducted on it will translate to real-world scenarios. Security assessments conducted against controlled environments are defensible as the environmental variables can be maintained across assessment engagements. This is similar to the way other research has tested security properties using model generation instead of real world test beds (Masson, et al., 2007) . Systems administration conducted by experiment actors on the environment allows for defensible and equal representation of security change implementation.  The motivation and sophistication of the simulated attacker can be guaranteed to be equal across the different campaigns and therefore defensible. Given the control over the realistic network and simulation of realistic actors during the experiment this medium can provide measureable metrics that provide useable results for the validation of offensive security assessment paradigms.

## Experiment Design

With an evaluation medium determined for the experiment to be built upon it is important to pick a target for the offensive security assessment that allows the experiment to provide results that would translate to a real scenario. For this purpose, there is a further requirement for identifying a simulated target that would provide an opportunity to represent the type of environment that would provide have identifiable priority items for the CAPTR team model.

## Target Determination

The example of a law firm was chosen to be the basis for the lab network. A law firm contains data such as attorney client privileged information as well as information being used in on-going legal cases. If compromised, such objects would likely be so damaging to the organization it would cease to operate. This example also allows for separate segments of a network containing operational personnel in one area and legal personnel in another. Unlike other probable targets of motivated advanced malicious actors, the legal firm example allows for a relatively small network of forty to fifty machines to be used. This is in comparison to those of a large corporation or government institutions that would also likely be the target of such attacks. In a simulated law firm there is no need to emulate specialized equipment such as medical or SCADA devices which could prove difficult for experiment designers. The presence of such technology would also levy a need for specialized skills in the security assessment, systems administration and simulated attacker which would make finding experiment actors a challenge.

## Experiment Summary

CAPTR team methodology experimentation must defensibly answer two questions. Does CAPTR teaming identify findings that are unique to those found using offensive security assessors following traditional processes? Do the recommendations from such assessments stand up in the face of advanced adversaries? Answering these questions allows for a measured representation of the uniqueness of findings generated via the CAPTR team paradigm and the ability of such findings to mitigate risk in the face of advanced motivated actors such as APTs.

With the goal of answering both questions three identical copies of a network were created. The networks were built with only functionality in mind and were created to represent a small law firm of 42 Machines.  In this network, there were three functional LANs. There is a DMZ, a corporate LAN for devices supporting the operations of the organization such as a CEO and IT staff as well as a LAN segmented off for the lawyers, legal aids and customer information. Using the example of a law office allows for there to exist data and devices that if compromised could cripple or bring ruin to the organization. In this example, it would be confidential attorney client privileged information from cases that would be treated as lethal compromises. The three different networks had different IP addresses, host names, user names and domain names to appear unique to assessors and attackers but the networks were set up identically.

One network was left unchanged as a control. The second network was assessed by an experienced penetration tester and former red team member from a machine in the DMZ using typical offensive security assessment tools and processes. This test was conducted with a scope of assessing the entire organization if possible. The third network was assessed in the CAPTR team methodology, the assessor was made to understand the intent of such an assessment and was given tan initial scope of those items that would be lethal to the organization if compromised. This consisted of the case files and the servers they were stored on. These assessors then provided recommendations based on their findings. These recommendations allow for a comparison between what was identified and recommended from traditional security assessment and what was recommended by the CAPTR team resulting in a measure of uniqueness.

## Lab Design

With the type of organization decided, the lab network needs to be structured such that it provides for control and realism. The types of technologies involved in the lab network must be as close to representing a real-world organization as possible and the lab must be controlled in a way as to avoid any possible external contamination to the experiment.

### Lab Network Operating Systems

The most common operating system in use today is Microsoft Windows (Statistica, 2017) (Net Marketshare, 2017) and the version that is most common is Windows 7 (W3Counter, 2017) (Computer Hope, 2017) (Merriman, 2016). Therefore, the bulk of the lab network will consist of Windows 7 user devices in a domain with Windows 2008 domain controllers as that is the closest kernel version to Windows 7 for a Windows server operating system. As a note of accountability, at the time of experiment design as well as during the offensive security assessments and simulated attacks the remote code exploit for these kernel versions, MS17-010 (Microsoft, 2017) also referred to as ETERNALBLUE (Ullrich, 2017) had not been disclosed to the public or weaponized yet and did not impact the carrying out of this experiment.

The network required several Linux based operating systems as well. As Ubuntu was the most popular and common Linux operating system (Hoffman, 2014) it was chosen to represent Linux platforms in the network. Another Linux distribution Vyos (Vyos, 2018) was chosen as a routing and firewall platform for the experiment given its proven history, administration support community and reliability.

## Lab Network Layout

As discussed earlier, the network was intended to be set up representing a law firm network. This required having multiple functional areas for the network as well as allowing communication between them and to the simulated internet. The network would not connect to the actual internet to avoid experiment contamination.

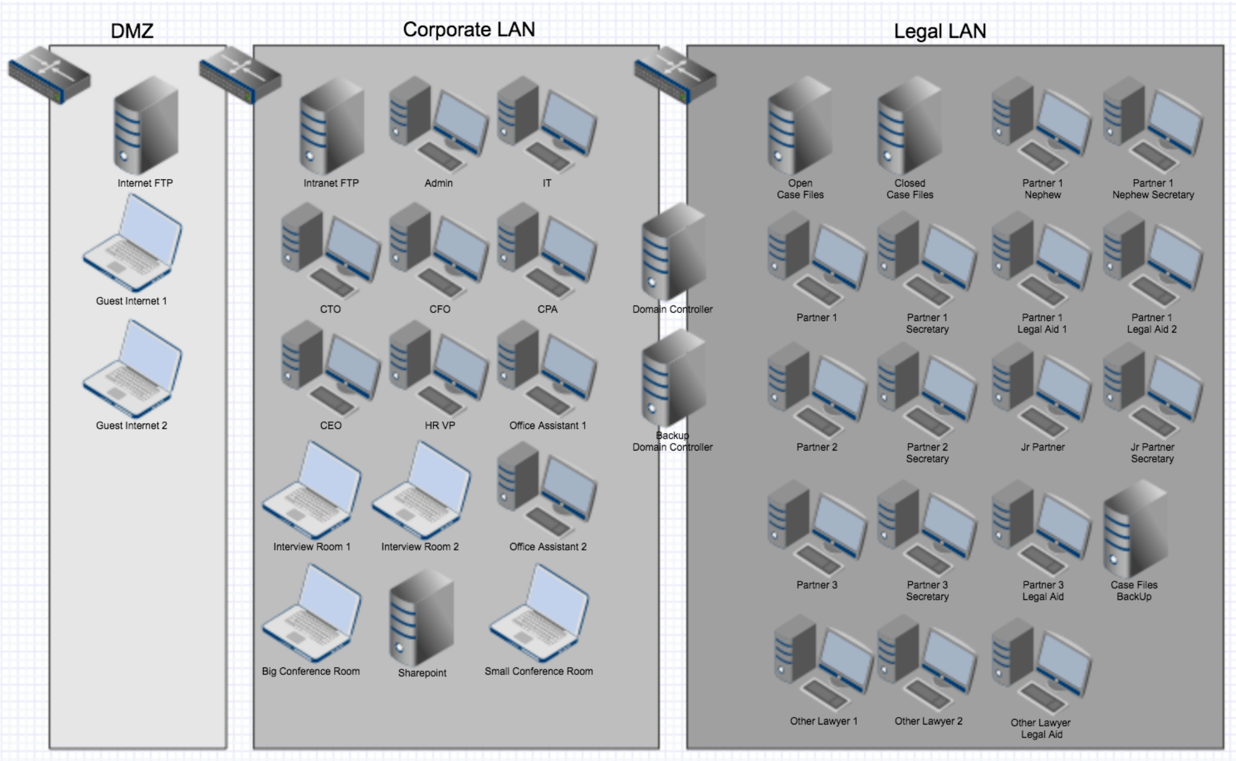


**Figure 29: Network Diagram**

In the above diagram the three routing devices were using the Vyos operating system, the internet and intranet FTP servers and Case Files Backup were using the Ubuntu operating system and the rest of the machines shown were using Microsoft Windows 7 or Server 2008 for desktop and servers respectively.

**Underlying Software & Hardware**

To allow for the installation and management of all of these devices and their software, virtualization was determined to be the most efficient solution. A server was built to host the entirety of the organizations devices with hardware adequate enough to provide the recommended amount of resources to each virtual machine. The Ubuntu operating system was installed on the physical server as it was more reliable than other operating systems with regards to running the VMWare Workstation software used to virtualize the lab network. VMWare workstation was chosen over open source virtualization software due to its stability and reliability as well as ease of virtual machine administration. Below is a table showing the individual machine requirements.

| Number of Devices | Device Type / Resources | CPUs | Memory | Storage |
|---|---|---|---|---|
| 3 | Ubuntu FTP Machines | 1 | 1GB | 5GB |
| 31 | Windows 7 Desktops | 1 | 2GB | 20GB |
| 5 | Windows Servers | 2 | 2GB | 20GB |
| 3 | Vyos Routers | 1 | 500MB | 1GB |
| 42 | Total | 47 | 76.5GB | 738GB |

**Table 7: Hardware Specifications**

To host this heavy resource requirement the physical server had the following specifications.

- 2 physical CPUs totaling 12 physical (24 logical) cores
- 2, 1TB solid-state hard drives to install virtual machines on
- 2, 2TB magnetic hard drives to back up to

- 1, 256GB solid-state hard drive to host the servers operating system and virtualization software
- 96GB of DDR3 server RAM

**Access Technology & Software**

The challenge of such an experiment being virtualized on a physical server instead of the cloud is the portability of access for the varied actors participating and requiring remote access while still maintaining a sealed environment.  To achieve this, an Ubuntu jump server was hosted in the Amazon cloud hosting service AWS. The lab internet from the position of the lab network, was limited to one listening post server installed with the Ubuntu operating system in a separate virtual LAN with a separate IP scheme from the emulated organization. Devices from within the organization were limited to communicate out to only the single IP of the listening post device and that device only received connections from the simulated lab IP ranges. The listening post server was also limited to being only able to communicate to the simulated lab or the single public IP address of the jump server hosted in AWS. It could not communicate to the physical server hosting the network. Communication was limited in this fashion from all points using both routing configurations and firewall policies.

The AWS hosted jump server itself allowed no outbound connections and only allowed inbound connections from the listening post server in the simulated lab internet. As actors in the experiment such as systems administration, security assessment or simulated attackers needed to gain access to the lab, their IP addresses would be permitted to communicate to the AWS machine for only the needed period. Communications to the AWS hosted jump server were limited at the operating system level via firewall policies as well as at the cloud hosting level using Amazons security policies to specific ports, source IPs and destination IPs.

To enable communication with the lab, the systems administrator would have to access the listening post machine via the VMWare workstation console on the physical server and utilize the SSH protocol to authenticate to the AWS hosted jump server and open up a reverse tunnel back into the lab network. Locally SSH would be utilized on the AWS jump server to forward traffic into this reverse tunnel. Lastly, the experiment actor who at the time was allowed to communicate with the AWS jump server would SSH into it. This results in opening up a forward tunnel the traffic of which would hit the local tunnel on the AWS jump server and be forwarded on into the lab network. This meant that only actors of the experiment and only during their specified window of performance for their specified roles could communicate back into the lab network. It also meant that even if the jump server and an actor machine were maliciously compromised they still could not communicate into the lab network if the administrator had not opened the reverse tunnel from within the simulated lab internet listening post server via physical access to the hosting server. Below is a diagram clarifying this setup.

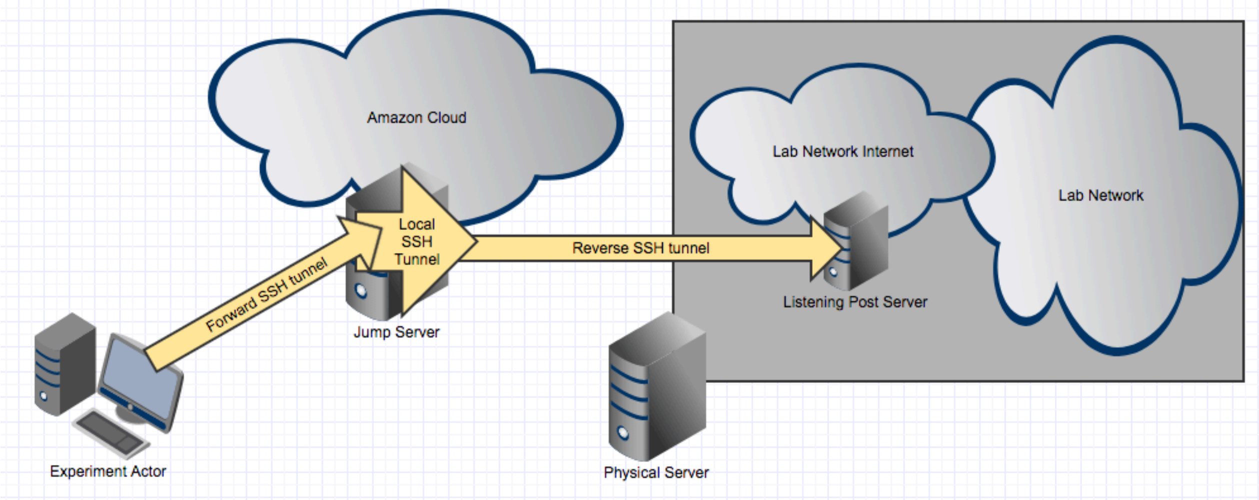


**Figure 30: Tunnel Set-Up**

### Assessment Software

To conduct the offensive security assessments and simulated attack against the lab networks a suite of offensive security tools would be needed. For this purpose, the Kali Linux distribution was chosen as well as the trial version of the computer exploitation framework Cobalt Strike. Cobalt strike was chosen as the client, server and implant technology for attacker and assessor access due to its extremely verbose activity tracking and logging capabilities as well as ease of use. The Cobalt Strike server was installed on the lab network internet listening post server. The Cobalt Strike client would be installed on experiment actor computers requiring interaction within the network and communicate with the server via the previously executed SSH tunnels. Then the Cobalt Strike implant would be executed with user context on a target machine within the lab network to give access to attacker or assessor as needed. This type of malware execution with unprivileged user context reflects the access gained via spear phishing techniques. As spear phishing is among the most common vector of compromise for APTs and other actors (TrendLabs APT Research Team, 2012) it was chosen as the access for the simulated attacks in the network.

Towards increasing the overall security and control over the lab network not only did the tunnels need to be set up correctly to allow communications into the network but the only ports allowed to communicate were SSH and the Cobalt Strike ports. As such, there was further authentication between the Cobalt Strike client and server via an ID string that if not matched would prevent connections to the implant control server and listening post installed on the server in the simulated lab network internet. The below diagram shows how the Cobalt Strike software allowed assessor and attacker to conduct activity from within the lab network.

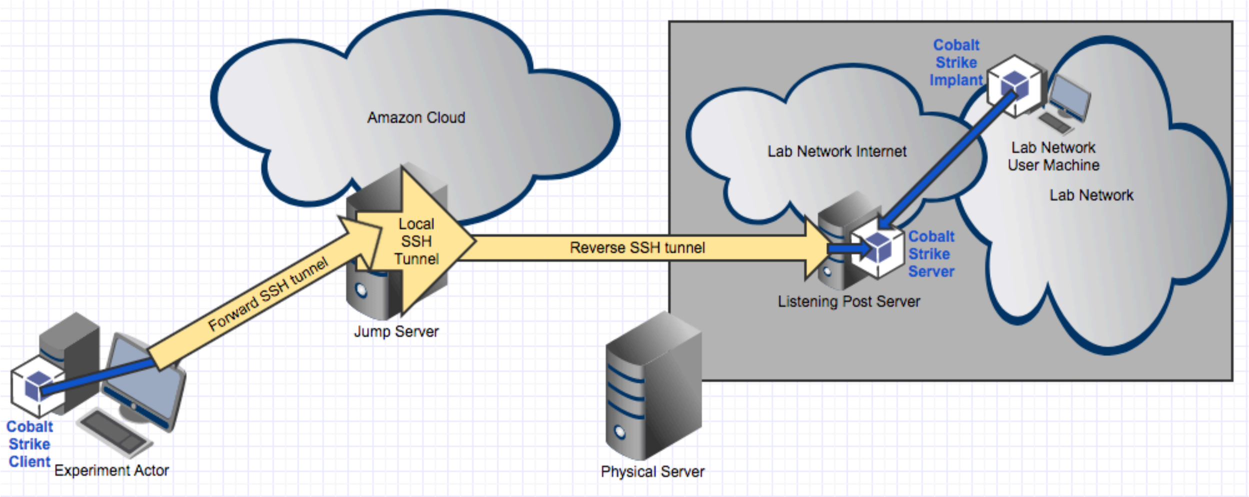


**Figure 31: Access Set-Up**

A list of the software utilized in this experiment can be found in Appendix A.

## Experiment Metrics

The purpose of this dissertation and experiment are to determine if the offensive security assessment paradigm of CAPTR teaming is a novel augment to traditional red teaming. Determining the novel nature of CAPTR teaming in comparison to traditional red teaming is impart shown via the categorical analysis of the assessment processes contained earlier in this dissertation. To lend a quantitative metric for novelty, this experiment will also allow for the two methods to provide findings which can be measured in their variance from one another to give a statistical idea of assessment uniqueness.

The experiment must also be able to determine the impact of recommendations to the security posture of the organization and its ability to mitigate advanced threats. To do this the National Institute of Standards and Technology's Common Vulnerability Scoring System Calculator (NIST, 2018) was used to generate a numerical representation of the associated risk a given compromised machine would have to the organization as a whole. Typically, this calculator is used to determine a numerical score of the impact a given vulnerability has to a single system. For use in the experiment the different machines are treated themselves as vulnerabilities and the organization is viewed as the system at risk. Therefore, the attributes that are input to create the overall score entered with this perspective. For example, if compromised by an attacker, a router within the organization would present the threat of traffic manipulation between two areas of the organization. The impact and difficulty of which are used in the CVSS calculator to give that device a score of 5.8. This value represents the device as a numerically measured vulnerability to the organization. Comparatively, a device such as machine set up for clients to use to browse the internet from the within the DMZ are less of a vulnerability to the organization if compromised and represent a lower risk value of 3.4. This is based on the impact and difficulty of turning a compromise of this machine against the organization. The lethal compromise devices within the organization are rated within the CVSS calculator to indicate the difficulty of turning the vulnerability of their compromise against the organization. This was done to include them within the overall risk value for the organization even though as lethal compromise items their compromise would be exponentially critical in comparison to other devices.

Below is a table containing the CVSS ratings for all of the in-scope devices of the lab network. The sum of these individual ratings represents the total amount of risk present in the organization. A detailed breakdown of the attributes that contributed to the score of each machine are contained in appendix B.

| Compromise Item | CVSS Rating |
|---|---|
| Internet / DMZ Router | 5.8 |
| DMZ / Corp Router | 5.8 |
| Corp / Law Router | 5.8 |
| Internet FTP Server | 4.3 |
| Client Internet Machine 1 | 3.4 |
| Client Internet Machine 2 | 3.4 |
| Intranet FTP Server | 4.3 |
| Domain Controller | 8.9 |
| Back-Up Domain Controller | 8.9 |
| Admin Server | 5.5 |
| Admin Machine | 6.6 |
| IT Machine | 6.6 |
| CEO (Chief Executive Officer) Machine | 4.7 |
| VP Human Resources Machine | 3.8 |
| CFO (Chief Financial Officer) Machine | 4.7 |
| CPA (Accountant) Machine | 3.8 |
| CTO (Chief Technology Officer) Machine | 4.7 |
| Office Assistant 2 Machine | 2.9 |
| Big Conference Room Machine | 2.9 |
| Small Conference Room Machine | 2.9 |
| Interview Room 1 Machine | 2.9 |
| Interview Room 2 Machine | 2.9 |
| Partner 1 Machine | 7.1 |
| Partner 1 Nephew Machine | 7.1 |
| Partner 1 Secretary Machine | 2.9 |
| Partner 1 Legal Aid 1 Machine | 7.1 |
| Partner 1 Legal Aid 2 Machine | 7.1 |
| Partner 2 Machine | 7.1 |
| Partner 2 Secretary Machine | 2.9 |
| Partner 2 Legal Aid Machine | 7.1 |
| Partner 3 Machine | 7.1 |
| Partner 3 Secretary Machine | 2.9 |
| Partner 3 Legal Aid Machine | 7.1 |
| Other Lawyer 1 Machine | 7.1 |
| Other Lawyer 2 Machine | 7.1 |
| Other Lawyers Legal Aid Machine | 7.1 |
| Jr. Partner Machine | 7.1 |
| Jr. Partner Secretary | 2.9 |
| Open Case Files Server | 8.8 & LETHAL COMPROMISE |
| Closed Case Files Server | 8.8 & LETHAL COMPROMISE |
| Case Files Back-Up | 9.8 & LETHAL COMPROMISE |
| Sum total amount of organizational risk | 228.7 |

**Table 8: CVSS Ratings**

## Personnel Requirements

To provide as defensible an experiment the performance of actions in the experiment needs to reflect expected behavior of such actors in the real world. To accomplish this, qualified personnel must be identified to perform the duties of the different actors within the experiment. Additionally, similarly qualified personnel will be identified to audit the actions of the individuals within the experiment to insure nothing is being done outside the bounds of normal activity. The following list indicates the personnel required to facilitate the experimental evaluation of the CAPTR team concept in comparison to that of traditional red teaming. The resumes of the individuals who performed these roles during the experiment are contained in Appendix C and are anonymized to protect the privacy of the actors.

- Systems Administrator
- Systems Administration Auditor
- Red Teamer
- Red Team Auditor
- CAPTR Teamer
- CAPTR Team Auditor
- Qualified & Sophisticated Attacker

## Experiment Schedule & Walkthrough

Below is a list indicating the chronological series of events that are required for successful completion of this experiment. Following this list is an in-depth walk-through featuring the details of each phase of the experiment.

1. **Control Network** and related documentation created by **Systems Administrator**
2. **Control Network** audited for realism and functionality by **Systems Administration Auditor**

3. **Control Network** cloned twice by **Systems Administrator** and clone documentation created
4. **Red Teamer** assesses **Network Clone 1**
5. **Red Team Auditor** verifies the **Red Teamer recommendations**
6. **Systems Administration Auditor** verifies **Red Teamer recommendations**
7. **Systems Administrator** implements changes to **Network Clone 1** based on **Red Teamer recommendations**
8. **Red Teamer** verifies changes were done in accordance with intent of **Red Teamer recommendations**
9. **CAPTR Teamer** assesses **Network Clone 2**
10. **CAPTR Team Auditor** verifies the **CAPTR Teamer recommendations**
11. **Systems Administration Auditor** verifies **CAPTR Teamer recommendations**
12. **Systems Administrator** implements changes to **Network Clone 2** based on **CAPTR Teamer recommendations**
13. **CAPTR Teamer** verifies changes were done in accordance with intent of **CAPTR Teamer recommendations**
14. **Red Teamer recommendations & CAPTR Teamer recommendations** analyzed to indicate novelty metric of CAPTR team process
15. **Simulated Attacker** wages campaigns against **Control Network**, **Network Clone 1**, **Network Clone 2**
16. Metrics compiled to indicate mitigation of risk to organization in each campaign

### Control Network and Related Documentation Created

The systems administrator creates a virtualized lab network in the image of one that could be utilized by a law firm. Devices within the network are configured and domains set up as well as user and administrative accounts. Documentation of the passwords, accounts and device addresses is compiled. This lab network and its documentation will act as the control network for the experiment as it will simply have a functional level of configuration and no further security measures or alterations of configuration besides that which allow for intended communication and activity.  The detailed network documentation for the control network can be found in Appendix D.

### Network Audited for Realism and Functionality

The Systems Administration Auditor will go over the network documentation as well as network diagrams of the control network to determine if it is realistic and indicative of a functional network configuration. The network will also be audited with regards to its potential to skew the results of the experiment.

### Control Network Cloned

The systems administrator will clone the now verified control network twice. This is to provide two separate swim lanes for the offensive security assessment paradigms to work within. The topology, types and number of devices will remain identical to the control network. The hostnames, users, accounts, passwords and IP addresses of the devices contained within the clones will be unique for each clone and separate as will the IP schemes themselves. This is to make them appear as unique as possible come the attack simulation portion of the experiment. Documentation for these control network clones can be found in Appendix E and Appendix F.

### Red Team Assessment

One of the clone networks will be assessed in the traditional red team method by the Red Teamer. The assessment of this network will be done in a time window of 10 hours to insure both assessments are concluded in equal timeframes. The Red teamer will then provide recommendations based on the assessment findings. The instructions sent to the Red Teamer at the beginning of the red team assessment can be found in Appendix G. The recommendations of the red teamer can be found in Appendix H.

### Audit of Red Team Recommendations by Read Team Auditor

The recommendations of the Red Teamer are subjected to audit by a Red Team Auditor who is a separate qualified red team practitioner. This is to insure the recommendations from the Red Teamer fall within scope of expected traditional red team assessment.

### Audit of Red Team Recommendations by Systems Administration Auditor

The recommendations of the Red Teamer are further subject to audit by the Systems Administration Auditor. This is done to ensure that the changes suggested by the Red Teamer fall within the scope of activity a typical systems administrator would conduct and not outside the realm of realism.

### Implementation of Red Team Recommendations

The Systems administrator takes the verified recommendations of the Red Teamer and begins implementing them into the Clone 1 network using up to 20 hours of administration time. The Red Teamer is instructed to provide recommendations in an order of importance for implementation and are informed that the Systems Administrator will only have 20 hours to complete the changes to the network. This is done to keep the offensive security assessors from recommending varying amounts of changes for the security of the network which could skew results. A copy of the recommendation guidelines provided to both the Red Teamer and CAPTR Teamer can be found in Appendix I. The Systems Administrator will then provide a log of changes implemented into the Clone 1 network to the Red Teamer.

### Verification of Red Teamer Recommended Changes

The Red Teamer is also responsible for auditing the implementation of changes conducted by the Systems Administrator based on recommendations of the offensive security assessment. The Red Teamer is to ensure that the changes were performed satisfactorily with regards to the intention of the Red Teamer. This prevents the Systems Administrator from poorly representing the assessment capabilities of the Red Teamer. A copy of the change log for the systems administration that implemented the changes to the Clone 1 network can be found in Appendix J.

### CAPTR Team Assessment

The CAPTR Teamer assesses Clone 2 of the control network. This is done in the same allotted time as the 10 hours given to the Red Teamer. The CAPTR Teamer is sent network documentation and a letter indicating the spirit of the CAPTR team to the CAPTR teamer as well as scope and rules for the engagement. Recommendation guidelines are sent to the CAPTR teamer as well. A copy of the CAPTR Team intent, scope and rules letter can be found in Appendix K. The CAPTR Teamer will provide recommendations based on findings of the offensive security assessment. A copy of the CAPTR Teamer recommendations can be found in Appendix L.

### Audit of CAPTR Team Recommendations by CAPTR Team Auditor

Similar to the recommendations of the red team, those of the CAPTR team are also audited by a separate party who is also qualified in offensive security and given the same intent of CAPTR teams information as the CAPTR Teamer. This will allow for third party verification that the changes suggested by this assessment method are in keeping within the spirit of CAPTR teaming.

### Audit of CAPTR Team Recommendations by Systems Administration Auditor

Also, like the Red Team recommendations those of the CAPTR team are subject to the same audit by the Systems Administration Auditor to determine that they fall within the scope of activity a typical systems administrator can be expected to perform.

### Implementation of CAPTR Team Changes

The Systems administrator takes the verified recommendations of the CAPTR Teamer and begins implementing them into the Clone 2 network also using up to 20 hours of administration time. The CAPTR Teamer is also instructed to provide recommendations in an order of importance for implementation and are informed that the Systems Administrator will only have 20 hours to complete the changes to the network. The Systems Administrator will provide a log of changes implemented into the Clone 2 network to the CAPTR Teamer.

### Verification of CAPTR Teamer Recommended Changes

The CAPTR Teamer is also responsible for auditing the implementation of changes conducted by the Systems Administrator based on recommendations of the offensive security assessment. The CAPTR Teamer is to ensure that the changes were performed satisfactorily with regards to the intention of the CAPTR Teamer. This prevents the Systems Administrator from poorly representing the assessment capabilities of the CAPTR Teamer. A copy of the change log for the systems administration that implemented the changes to the Clone 2 network can be found in Appendix M.

### Recommended Changes Analyzed

The changes suggested by the two teams are compared to indicate whether or not the two offensive security assessment paradigms provided the same or different results. This is part of the basis for making the case that the CAPTR team paradigm is a worthwhile augment to established techniques. If the changes recommended by either team were nearly identical it would make a weak statement for the novelty of CAPTR teaming. If the changes were largely different then there is a stronger case for the paradigm.

### Simulated Attacks

Cyber-attack campaigns are conducted against the control and clone networks. The Attacker is instructed to replicate motivated and sophisticated attacks against the organization in each of the three campaigns. The Attacker is informed that the organization for all three campaigns are legal firms and that the goal is to compromise as much of the network as possible with the specific goal of finding case files as they are the item of lethal compromise for these organizations. The attacker is given a maximum of 40 hours to conduct each of the cyber-attacks from the access provided, which is as earlier discussed, a user context implant running as if by successful spear phishing.  The order of the campaigns is unknown to the attacker however the Control was attacked first, the Red Team secured network second and the CAPTR team secured network third. This was to ensure that if the Attacker gained any proficiency as the attack campaigns were completed that the attacks would be most proficient against the CAPTR team secured network and any bias this created would make attacks against the CAPTR Team network most likely to be successful and if anything, skew results against the CAPTR team model.

### Metrics Compiled

Once the campaigns are completed the compromised devices are tallied and a percentage of the overall risk present in the network secured is identified for each. This is done to provide a quantitative measure of the amount of risk mitigated by the changes recommended by the offensive security assessments.

## Addressing Defensibility Requirements

Briefly this section summarizes ways in which the aforementioned experiment is able to address the requisite characteristics for defensibility.

### Addressing Controlled & Realistic Environment Requirement

The virtualized lab simulation of a network serving as a replica of potential real network servicing a law firm means that it is both controlled and a realistic situation to conduct both offensive security assessment and attack simulation. Further the great lengths taken to guarantee remote communication of actors while maintaining a contaminant free experiment mean that no outside actor or incident will affect the lab network.

### Addressing Defensible Security Assessments

Using a lab network not connected to the internet means that security assessment is conducted in a vacuum, free of user and administrator created events that may unfairly help or hinder one assessment methodology over the other. The use of industry qualified offensive security experts in the carrying out of the assessments provides both defensibility to their assessment as well as furthering realism. Additionally, having the assessments audited by similarly qualified separate third party offensive security experts means there is an extra level of validation for the legitimacy of the assessments and the generated recommendations provided from them. The equal limit of time and like recommendation guidelines means that both assessment paradigms have fair assessment engagement windows and know the time restrictions on the administrator ahead of time.

### Addressing Defensible Systems Administration

Insuring the networks were created and administered across the separate assessment platforms by the same administrator insured that one network did not receive more or less qualified systems administration than the other. The audit of the networks themselves by a separate third party qualified systems administrator prevented the lab network from failing to represent a realistic operating environment. The audit of the assessment recommendations from both teams by a third-party systems administrator insured that the implementations needed were within the scope of typical systems administration and would not skew the outcome of the test in favor of one assessment paradigm over the other. The equal limit of time for change implementation across both assessed networks kept the implementation of security fair between both assessed networks. Lastly, the presentation of change logs regarding the assessor recommendations back to the assessor insured that the changes done to the networks were in keeping with the intention of the assessors.

### Addressing Motivated & Sophisticated Attacker

The use of an extremely qualified cyber operations expert and senior red team member with experience performing APT emulation allowed for an equal level of sophistication to be applied to all three attack campaigns. The level of skill maintained by the attacker meant that the networks were more likely to see deeper assessment penetration and therefore changes recommended by the assessors were more likely to face attacker scrutiny. Having a simulated attacker mean that no outside attackers could influence the emulation campaigns and therefore it would be similarly capable of targeting each of the three networks. The brief to the attacker on specific motivation for the legal firm's case files in addition to wanting the whole network compromised meant that the actor had a distinct purpose that was the same for all three networks which achieved a fair level of motivation in all three campaigns.

### Addressing Measureable Results

The comparison of number of recommendations and their uniqueness between the two evaluated assessment paradigms allowed for a measure of novelty between the suggested CAPTR Team paradigm and established red team practices. Utilization of the NIST provided CVSS calculator to calculate the risk each compromise machine allowed for a comparable quantitative evaluation metric. This allowed the experiment to grade the success of the paradigms in protecting overall risk as well as the ability to directly compare the paradigms to each other.

## Results: Recommendation Phase

The red team assessor of the network had six recommendations as a result of the findings of the red team assessment that were implemented in the administration time window. The CAPTR team assessor of the network had eleven changes that were recommended as a result of the CAPTR team assessment and similarly implemented. One of the recommendations both teams had in common was securing use of the RDP service. The rest of the changes recommended by the offensive security assessments were unique to each other. This clearly delineates the CAPTR and red team methodologies are varied enough to lead to the discovery of different findings resulting in recommendations. The divergence of CAPTR team recommendations from those of the red team show that the CAPTR team paradigm is a novel offensive security assessment method. Below is a table listing summarized recommended changes from both assessments

| Red Team Recommendations | CAPTR Team Recommendations |
|---|---|
| Secure RDP Service | Secure RDP Service |
| Secure FTP Service against brute force | Split one domain into two |
| Secure SSH Service against brute force | Change network topology |
| Disable Anonymous SMB | Separate Admin accounts |
| Firewall Settings to prevent DMZ to internal communication | Disable task creation and WMI |
| Address CVE-2009-3103 | Remove FTP servers, utilize SCP |
|  | Utilize SCP for file transfer using special SCP only account |
|  | Secure and Encrypt Case Files |
|  | Lock down local firewall for File Servers |
|  | Allow only local administration for File Servers |
|  | Silo off the two Non-DMZ LANs from each other with firewall rules |

**Table 9: Recommendations Summary**

An administrator then implemented the changes recommended by either team to the respective networks. The six changes recommended by the red team required system administration to modify seventy-seven configurations or settings on devices where those recommended by the CAPTR team required seventy-three modifications of systems. The recommendation that the two teams had in common only required changing two machines. These changes were to the domain controllers to lock down the RDP service using group policy.

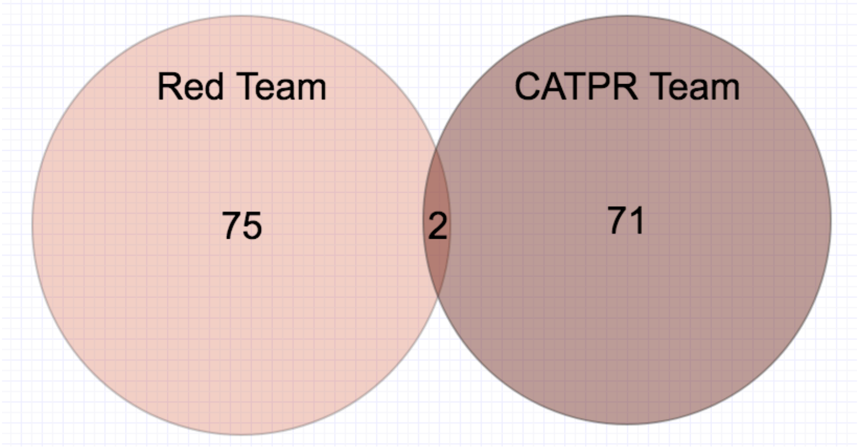


**Figure 32: Changes to devices Implemented by administrator based on recommendations**

## Results: Campaign Phase

After the changes were implemented, the experienced offensive security subject matter expert was used to represent an APT intent on compromising the target legal firms as completely as possible with the specific motivation of gaining access to privileged attorney client information. This allowed for an evaluation of the effectiveness of the changes implemented on the network compared to the control and with regards to each other. To provide measureable results on the ability of each offensive security assessment to mitigate risk to the assessed organization a metric was defined. For this purpose, the National Institute of Standards and Technology (NIST) calculator for the Common Vulnerability Scoring System (CVSS) was used (National Institute of Standards and Technology, 2017). Input was given to the CVSS calculator for each device in the network treating it as if it was a vulnerability to the organization. This allowed for a defensible scoring on the value to the organizations overall risk that each device had as a compromise item. The total CVSS score for the organization was 228.7 which is the result of totaling the CVSS score for all devices. The devices that were and were not compromised by the APT during the campaigns against red team and CAPTR team assessed networks serve as a defensible and measureable metric for effectiveness. The total CVSS score of the devices not compromised by the APT in each network represents the percentage of risk mitigated. Below is a figure illustrating the machines compromised during the APT campaigns against respective networks. A diagram of the control campaign is not necessary as all hosts were compromised. The red overlay indicates the machine was compromised and the blue overlay indicates the machine was protected throughout the attacker campaign.

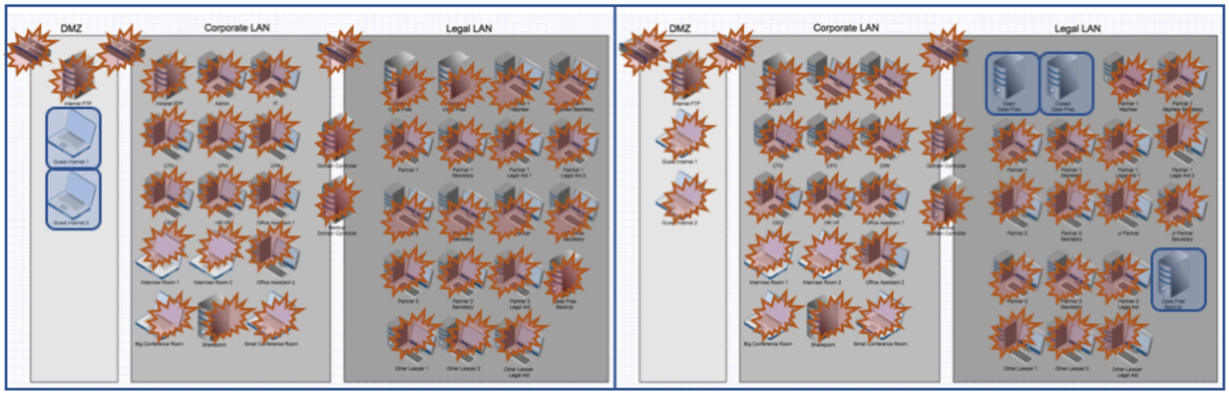


**Figure 33: Red Team Vs. CAPTR Team Campaign Results**

On the left is the red team campaign where all hosts besides the DMZ hosted customer internet access machines. On the right is the CAPTR team campaign where all hosts were compromised besides the open case files, closed case files and case files back up servers. These were the three machines identified as lethal compromise items for the target organization. Below is a table representing the overall risk values preserved by using the offensive security methods and their recommendations. The grey line represents the total value of risk associated with all of the machines in the network combined. The red bar represents the amount of that total risk that was compromised by the hacker and the blue represents the amount of the risk that was prevented by the assessing team.

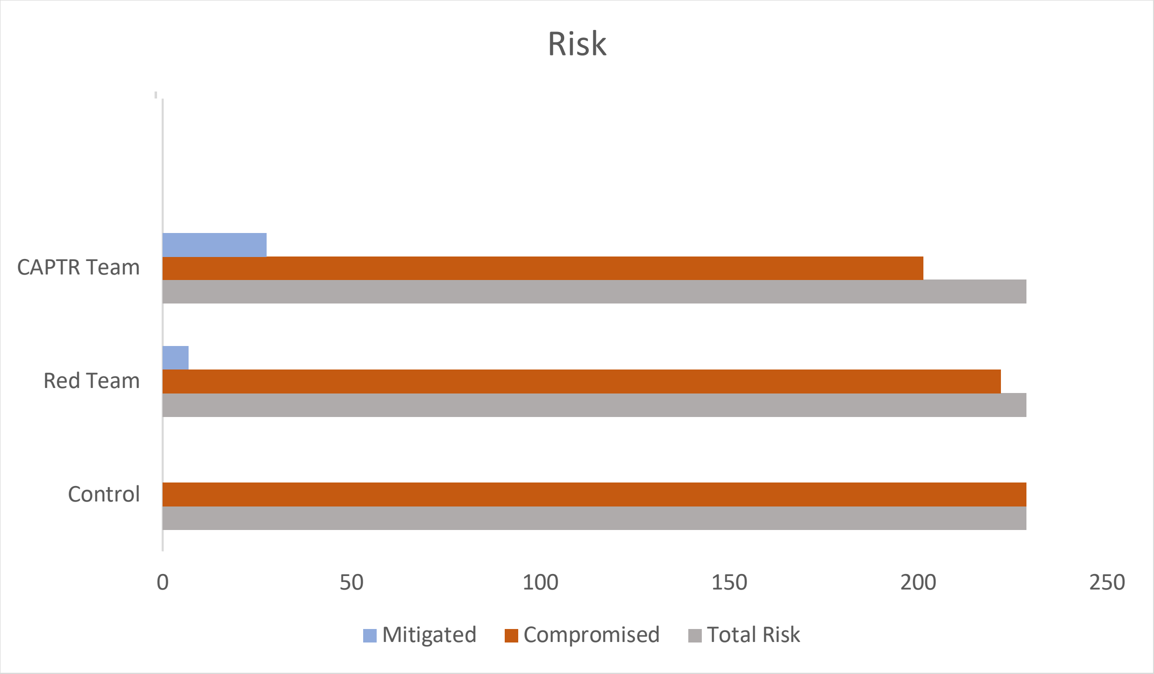


**Figure 34: Representation of risk measured by CVSS scores**

The red team assessment recommendations provided mitigating changes that prevented two devices from being compromised by the APT which together had a total CVSS score of 6.8. Therefore, the red team was able to protect 4.7% of the organization devices which mitigated 3% of the total risk faced. The CAPTR team assessment recommendations provided mitigating changes that prevented three devices from being compromised by the APT which had a total combined CVSS score of 27.4. These changes protected 7% of the organization devices mitigating 12% of the total risk. This also included all 3 devices identified as potentially lethal to the organization if compromised. In the control network 100% of the devices were compromised by the APT.

Experimentation showed that of the 16 recommendations from the offensive security assessments, only 1 or 6% were the same. This means that the assessments provided recommendations that were 94% unique. The recommendations of the CAPTR team paradigm protected 33% more machines than those provided by the red team. Additionally, the devices protected by the CAPTR team assessment represented 12% of the overall risk faced by the organization which is 400% greater than the risk mitigated via devices protected by red team recommendations. The CAPTR team process provided unique recommendations and the changes were proven to be effective in mitigating risk to the organization when compared to the control and red team assessed networks.

## Case Studies

To further provide evidence indicating a clear need for the type of offensive security assessment that CAPTR teaming provides case study was also conducted. This was accomplished using the new methodology to provide improved offensive security assessment in a scenario where traditional red teaming had not resulted in a complete assessment. These case studies were conducted as part of red team engagements for a fortune 500 (Forbes, 2017) technology company which will not be named due to non-disclosure agreements.

### Case Studies Scenario 1

In this case study scenario, a specific product owned by the host company was being evaluated. The red team scope consisted of external assessment of the product public IP addresses from the internet as well as lateral assessment from adjacent net blocks of the company owned internal datacenter hosting the product. The CAPTR team scope consisted initially of a lethal compromise item. Both tests were conducted by the same three senior penetration testers.

#### Scenario 1 Red Team Assessment Walkthrough

In the red team conducted assessment several weeks were spent externally enumerating the internet facing product IP space. The only port open was a web port tied back to an API with no website or any ability for the team to interact with it. Once this attack surface was fully evaluated the team moved to an internal point of presence inside the company datacenter and began evaluating potential vulnerabilities exposed laterally to other LANs in the datacenter. After surveying the IP space internally, the red team had identified several file indexes being hosted on port 80 via HTTP accessible without authentication. Inside these file stores the team found several API keys and spent over a week trying to interact with the APIs using those keys which were ultimately usable but extremely limited in scope and not a significant finding. Further the red team identified a local file inclusion on a different web server that allowed the red team to compromise a SSH key for a low-level user. This key was used to move laterally and interactively into the product LAN unfortunately in the time left for the assessment the team was not able to escalate privilege despite moving around to several hosts inside the product LAN.

### Scenario 1 CAPTR Team Assessment Walkthrough

The product IT and security staff remediated the red team identified issues in the networks and asked for a re-assessment of their LANs. This time however the team was utilized in the CAPTR team method. The team was given unprivileged user access to the machine that administrated all internal devices using SaltStack software (SALTSTACK, 2017). Compromise of this salt master server with super user privileges would allow a hacker to destroy the product infrastructure entirely. Performing the local portion of the CAPTR team assessment the team was able to elevate privileges by identifying a world writeable job being executed with super user context. Once elevated on the system the team verified it could compromise the SaltStack software which represented the lethal threat to the product. After ensuring there were no other ways of elevating privilege on the machine the team moved on to identifying ways in which the salt master could be pivoted to by using passive intelligence gathered from the machines operating system regarding communications data, authentication and command history as well as running services. From here the team identified that administrators of the salt master machine were pulling configurations from a remote repository which ended up also being unauthenticated. Lastly the CAPTR team identified a pivot point was the monitoring server for the LAN which was accessible with an admin user SSH key found on salt master. Once on the machine the team was able to change to super user without supplying additional credentials due to poor security configurations and was able to identify, via configuration files on the machine, that the web application it hosted for LAN service monitoring was configured with default credentials. There were many other findings as well however those discussed above were found within several days of the assessment beginning.

### Scenario 1 Conclusions

The two assessments identified completely different findings from each other even with the same personnel conducting both. The value of the findings from the CAPTR team assessment and the time wasted on at least one of the red team findings also speaks to the diversity and successfulness of the CAPTR team paradigm.  There is the possibility that the team would have eventually compromised the salt master in the initial assessment if given enough time however it is clear that in a very efficient and divergent manner the CAPTR team brought new potential to offensive security assessment almost immediately identifying extremely dangerous findings regarding lethal compromise and a likely pivot point.

## Case Studies Scenario 2

In this case study the target of the offensive security assessment was the DMZ and also a therein contained jump LAN. The DMZ was positioned in between the general datacenter networks of the company and the corporate user segments with a specific LAN in the DMZ responsible for hosting jump hosts where users were directed to pivot on to get between the corporate networks and into the datacenter. The assessment was to test the security of the DMZ and of more concern the jump LAN. The initial scope for the red team was to leverage several accesses within the datacenters and to attempt to exploit and pivot upstream into the DMZ and jump LAN to identify vulnerabilities that may allow for an attacker to get from the datacenters into the corporate LAN. The scope of the CAPTR assessment was run with this same intent but from the initial access of one unprivileged user on a jump box within the jump LAN and from there to determine what the critical threats were to that pivot point.

### Scenario 2 Red Team Assessment Walkthrough

The red team leveraged its datacenter accesses to perform initial scanning of the DMZ to find potential vulnerabilities to gain access inside the DMZ and then approach the jump LAN. After two weeks scanning the thousands of DMZ hosts several were identified as being vulnerable to attack due to poor Nagios configurations and one machine had an unauthenticated web vulnerability that allowed for remote execution of code. The red team spent another week attempting to gain remote code execution which was possible on several of the Nagios machines a well as the vulnerable website. However, after much effort there was an inability to escalate privilege as well as an inability to from a DMZ context identify the LAN which contained the jump hosts.

### Scenario 2 CAPTR Team Assessment Walkthrough

From the unprivileged access of a user account on a jump box the CAPTR team first looked to locally elevate privileges and were able to do so via an operating system specific privilege escalation exploit. From this local administrator context, the CAPTR team obtained the local admin credentials but were unable to pivot off the machine due to security software that was installed. Next, the team was able to use the local administrator context to obtain a copy of another user's authentication token. The new token was from a low-level domain administrator who had more permissions than the original user and was able to authenticate to other machines in the jump LAN using the token to authenticate over the remote desktop protocol.

After a quick scan of the LAN determined the location of several servers, the CAPTR team was able to identify an antivirus management server. The newly obtained token let the team pivot to this server. On this server the previously used local privilege escalation exploit was unusable. However, the machine did let the team elevate privileges using unsecured job scheduling to execute their tools with system context. Now the team was able to read registry key and installation information for the antivirus software and was able to gain administrative control of the antivirus management portal. Using this portal, the team was capable of executing code on machines which had antivirus clients managed by this server which were both within the jump LAN but also in several other corporate locations.

**Scenario 2 Conclusions**

The red team was able to assess a large attack surface of the overall DMZ from the datacenter as asked, however it did take several weeks. Additionally, once the red team was able to exploit machines within the DMZ there was not enough time or information to lead them to discovery of a method that would gain access to the jump LAN located within the DMZ.

In several days the CAPTR team was able to identify several local privilege escalation techniques that could enable an attacker, once within the jump LAN, to pivot to unanticipated machines. This was despite security software installed to protect pivoting from one machine to another. Further, centralized management software for antivirus was discovered to have no additional security permissions or separate accounts associated with it which was a key vulnerability that when paired with the local privileged escalations let unprivileged users become administrators of the antivirus management server and have the ability to pivot to other LANS. Within a much shorter time period the CAPTR team was able to determine more critical vulnerabilities with direct impact to the overall security of the organization.

# Discussion

## CAPTR Team Disadvantages

To present the CAPTR team paradigm in as complete an analysis as possible it is important to outline where the new approach would not be appropriate. Weaknesses in the CAPTR team model should also be presented as part of this dissection of security assessments. Impediments to the successful initiation of CAPTR teams includes weaknesses in the approach as well as those issues any new idea must overcome in the face of the established and incumbent.

CAPTR team process is designed and based around the idea of perceiving those vulnerabilities most likely to be utilized by APTs to breach lethal compromise items. Thus, the CAPTR team approach is limited with regards to its effectiveness concerning other types of threats and their varied points of presence. This model is unlikely to identify all internet facing vulnerabilities in a network due to its initial point of presence and assessment process. This also leaves open potential low hanging fruit that may be attacked by less sophisticated actors such as automated attacks and script kiddies (SECPOINT, 2017). These less sophisticated actors are likely intent on attacking the internet presence of an organization and with no inclination or motivation towards specific data deep within a network.

The greatest challenge regarding this new paradigm is in the beginning portions of the assessment process. The need to have both skilled security personnel as well as those familiar with risk management is unique to this new method of security assessment. Also, failure to accurately mesh risk and security while distilling critical and lethal compromise items impacts the entirety of the test. The introduction of a process new to security assessment and the reliance on the data produced by the scope creation of a CAPTR team assessment creates a potential Achilles heel for the success of an evaluation.

The initial point of presence from which a CAPTR assessment must begin also introduces difficult and new obstacles. In a non-tabletop assessment, the CAPTR team process requires the test begin with access to some of the most valuable data and devices in an organization. This requires a large amount of trust and liability between an organization and those testing it with the CAPTR team model. Access to the crown jewels of an organization is a touchy and difficult subject in traditional security assessment rules of engagements and testing agreements. In CAPTR teaming, the risk is possibly higher, and trust required more complete. When taken into account along with the novel nature of CAPTR teams, organizations willingness to undergo such testing and security companies' efforts to offer such a service could be impacted.

Additionally, the initial point of presence being deeper in a network means more required coordination during the test with IT and security staff. It is possible this added strain will affect the cost benefit analysis an organization places on whether to move forward with this type of assessment. Lastly, as highlighted earlier there are certainly organizations where this type of assessment is not appropriate given a risk evaluation of the types of information and data contained within potential client networks. If there cannot be identified data or machines that would pose lethal or critical compromise to an organization, it is not likely they would want to undergo a CAPTR team assessment. Also, with such a focus on APTs and internally held extremely valuable data, CAPTR teams are not a complete solution to security assessment needs by any organization. Where CAPTR team assessments fit in priority amongst existing security products and services already utilized by an organization will also impact the successful implementation of the new paradigm in the existing construct.

## CAPTR Team Implementation

For the CAPTR team paradigm to successfully augment standing security constructs it must be accepted into the group of security services organizations utilize. To accomplish this the CAPTR team must satisfy several requirements. The security environment that exists today must contain within it the skills and tools necessary for CAPTR team capabilities to be immediately viable. In the totality of security service customers there must exist a large enough subset where CAPTR team assessments are appropriate. Lastly there must be indications that trends in cyber security will continue shepherding more organizations towards adopting the paradigm.

### Feasibility

There are obstacles to adoption of any new security practice and to be brought into the fold of accepted security practices it must be readily feasible for CAPTR teams to be created. Help Net Security lists five major impediments to cybersecurity framework implementation as (Help Net Security, 2017);

- Lack of trained staff
- Lack of necessary automation tools
- Lack of budget
- Lack of audit tools

- Lack of tool integration

Essentially, the major obstacles to acceptance of security frameworks is the need to accommodate and acquire new tools and skills, which costs organizations time and money. There is no need to train staff towards new offensive security skills to accomplish CAPTR team assessment if there already exists a capability to execute traditional red team penetration tests. Since, as Dandurand mentions, “any red team has to comprise a wide range of cyber security experts who can provide an adversarial or ‘outside-the-box’ view when conducting red team assessments” (Dandurand, 2011) and CAPTR teaming would leverage the same security assessment related skillsets. A red team is also expected to already maintain skills such as finding vulnerabilities, delivering exploits and conducting network operations (Brangetto, et al., 2015) which lends to facilitating a CAPTR team. This same crossover exists with tools and techniques. A CAPTR team scans targets and enumerates for vulnerabilities just as a traditional red team does. If an organization maintains a red team capability it will have no need to purchase or develop new tools to accomplish CAPTR team assessments. Since there is no onus on learning different skills and acquiring new tools there is no burden of integration placed on an organization wanting to facilitate the new paradigm. Not having to introduce new skill or tool requirements also relieves the need for additional budget constraints in the stand up of a CAPTR team capability. There is a need to encompass operational risk management analysis into the team since this is needed to work with the customer organization to adequately identify scope. Though these skills are potentially new to the security assessors they are skills that can be learned from business personnel likely already handling operations of the security company itself. This means that the only new additional skills the security assessors must ascertain to conduct CAPTR test are ones that can likely be learned organically from non-offensive security staff of an organization.

The operational difference between red teams and CAPTR teams is the process. With such a high amount of shared resources any red team capability can be adapted to perform CAPTR team assessments by integration of the process outlined in this dissertation.

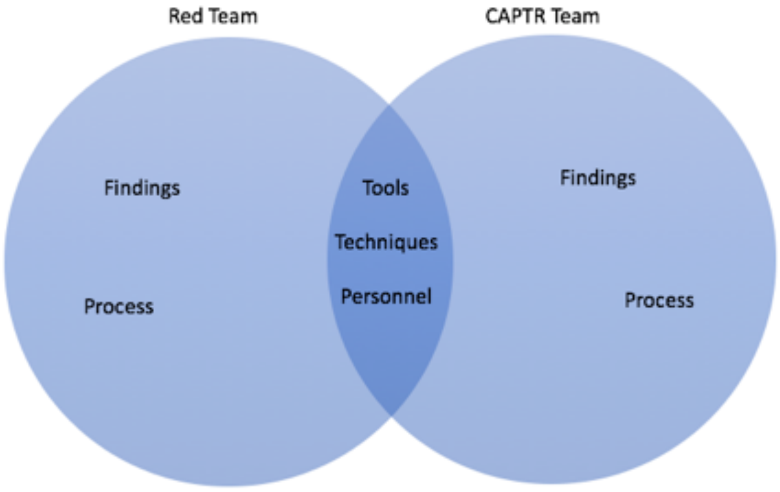


*Figure 35: Red Team / CAPTR Team Crossover*

For any new idea to take hold there must be an obvious need that it immediately fulfills. The CAPTR team concept has been proposed such that as a security service it fills a niche not adequately focused on by the traditional red team penetration test. That niche being prioritized critical compromise security assessment. This alone does not mean such a focus translates directly to an obvious interest by security customers.

The scope of CAPTR team assessments starts with those items that if compromised would prove highly impactful or fatal to that organization. Not every type of organization will have these sorts of compromise items and some may benefit less or little at all from having a CAPTR team evaluation of their networks. As an example, a small business in the product industry like a bakery or coffee shop. No amount of information data breach and disclosure is likely to shut down that business.

The same cannot be said for institutions such as the medical industry where HIPAA fines for information breaches and breach disclosure can reach millions of dollars (Services, 2017). There is the banking industry where in addition to any financial losses there is also the fining of institutions that can be in the tens of millions of dollars if information systems and controls contribute to data breach incidents (Martin & Titcomb, 2016).

The need for addressing critical compromise items and the ways APTs may access them is not limited to financial and health institutions. Any organization that relies heavily on its ability to keep some amount of information from public purview, be it intellectual property or personnel information, is at risk of being a target for APTs. As such any organization that is a potential target for APTs is a good candidate for CAPTR team assessments.

**Future Growth**

It is imperative that once implemented any paradigm continues to remain relevant. CAPTR teams are a solution for current problems that translates well into the future of security practices and as such it is worth adopting. The prevalence of APTs continues to grow and recognition of their threat to organizations is becoming a more accepted notion especially with data breaches in general as well are on the uptick (Liu, et al., 2015).

Although APT campaigns were historically associated with nation states, the amount of APT attacks by cybercriminals is increasing (Barth, 2016). Other institutions such as Arbor Networks note the rise of APTs stating "The proportion of respondents seeing APTs on their networks has increased from 22 percent to 30 percent year over year" (Arbor Networks, n.d.). The gamut of industry is now a target for a spreading contingent of APTs.

Aside from the general increase in APT like activity the two sectors already known to be in the crosshairs of cybercriminals are seeing increases over past trends as well. Kaspersky Labs reported "a cyber-criminal gang that used custom malware and APT techniques to steal millions of dollars while infecting hundreds of financial institutions in at least 30 countries." (Computer Incidents Investigation Department, GReAT, 2016). Healthcare continues to see more APT activity as well as such attacks like the Anthem hack where "hackers broke into a database containing the personal information of nearly 80 million records related to consumers, that one incident more than doubled the number of people affected by breaches in the health industry since the agency started publicly reporting on the issue in 2009." (Peterson, 2015). The growth of APT capabilities is on the rise and the need for security assessments like those of a CAPTR team to affect APT incursions will continue to increase in kind.

## Conclusions

This dissertation has presented the paradigm of counter APT red teaming as a solution towards improved mitigation of prioritized assets from threats such as APT actors. The need for ethical hacker conducted offensive security assessment in general has been established by taxonomy of automated hacking technologies and their disadvantages. Common and accepted red team practices have been dissected and insufficiencies categorized with regards to specifically mitigating the threat of APTs. The tradecraft of CAPTR teams has been established with the intent of addressing the shortcomings of current red team methods. This has been done utilizing high impact item centric assessment processes involving novel initialization perspectives, risk evaluation and attack surface analysis. Experimentation has shown CAPTR teaming to be unique in both comparison to red teaming in the carrying out of assessment and in the resultant findings. Changes based on these recommendations have also shown the CAPTR team to provide improved mitigation of impact from emulated APT actor campaigns. Additionally, Case study has supported such security improvements via CAPTR team utilization in real world scenarios with regards to severity of findings and efficiency of their identification. The CAPTR team model has set the precedent for academic improvement upon the tradecraft and processes of ethical hacker conducted offensive security assessment. Further, this dissertation has also provided a standardized experimental framework for measuring both novelty and success of future offensive security assessment variations.

# Appendices

## Appendix A – Experiment Software

Operating Systems:

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Ubuntu Linux distribution version 16
- Vyos Linux based routing and firewall platform version 1.1.8

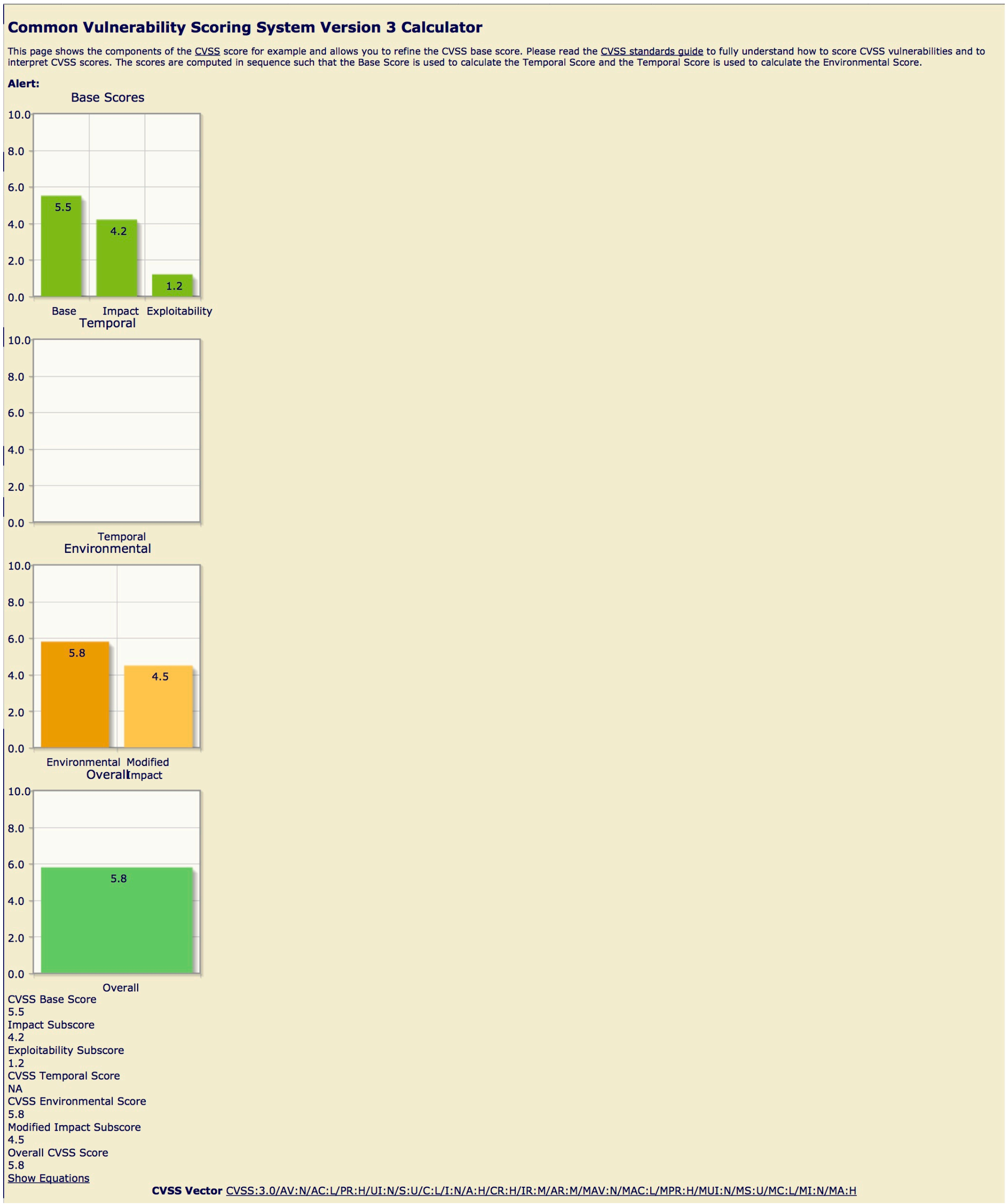
Applications:

- VMWare workstation version 12
- Cobalt Strike Trial Version
- Kali Linux 2017.2
- Amazon AWS EC2

## Appendix B – CVSS Score of Compromise Items

## Compromise Item: Internet / DMZ Router

**Threat to Organization:** Ability to manipulate traffic flow between the internet and DMZ
**Indicator of Compromise:** Attacker demonstrates ability to authenticate to device over SSH and enter configure prompt



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

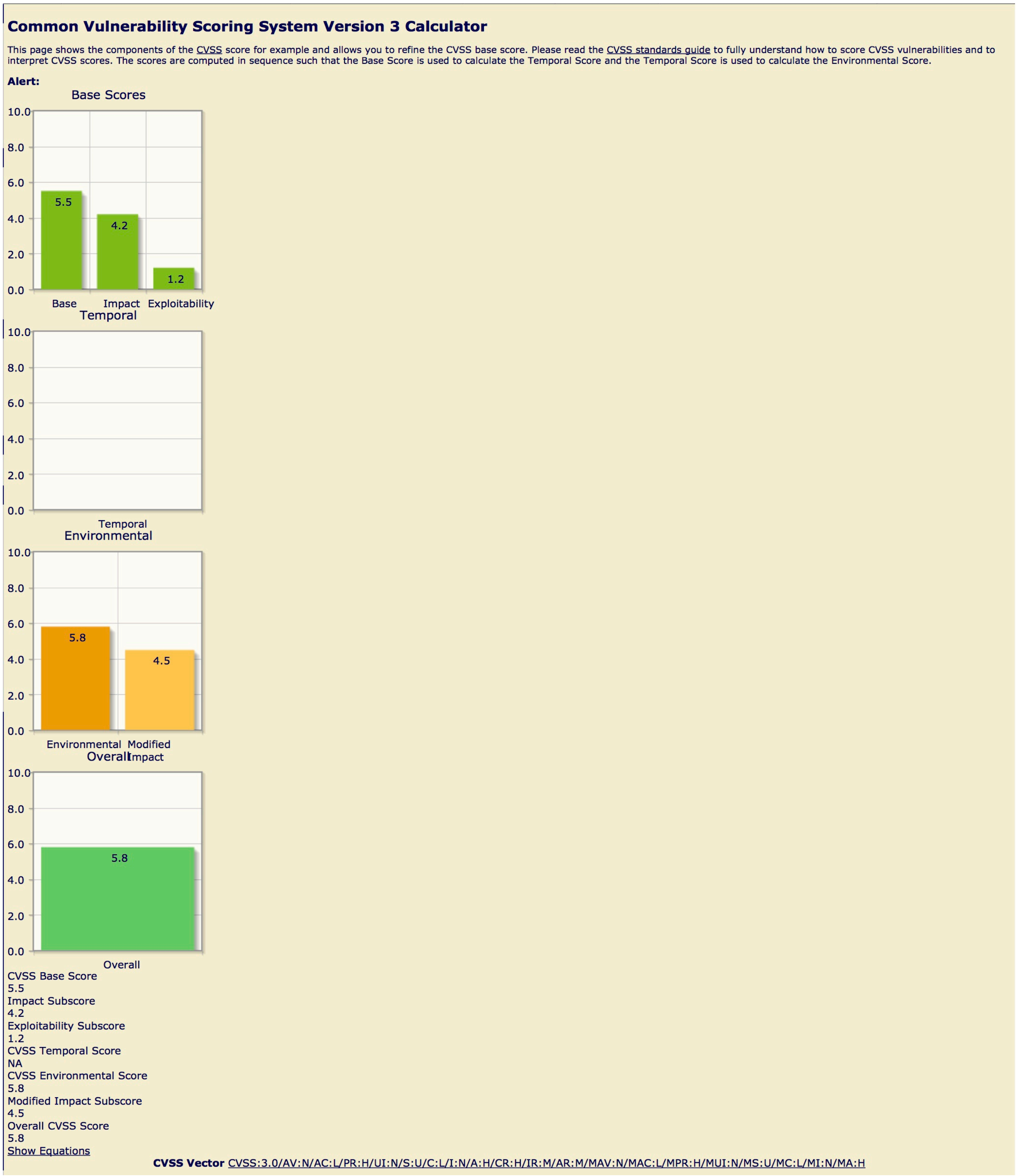
**Alert:**

CVSS Base Score
5.5
Impact Subscore
4.2
Exploitability Subscore
1.2
CVSS Temporal Score
NA
CVSS Environmental Score
5.8
Modified Impact Subscore
4.5
Overall CVSS Score
5.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:H

**Compromise Item: DMZ / Corp Router**

**Threat to Organization:** Ability to manipulate traffic flow between DMZ and Corp Subnets of organization
**Indicator of Compromise:** Attacker demonstrates ability to authenticate to device over SSH and enter configure prompt



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

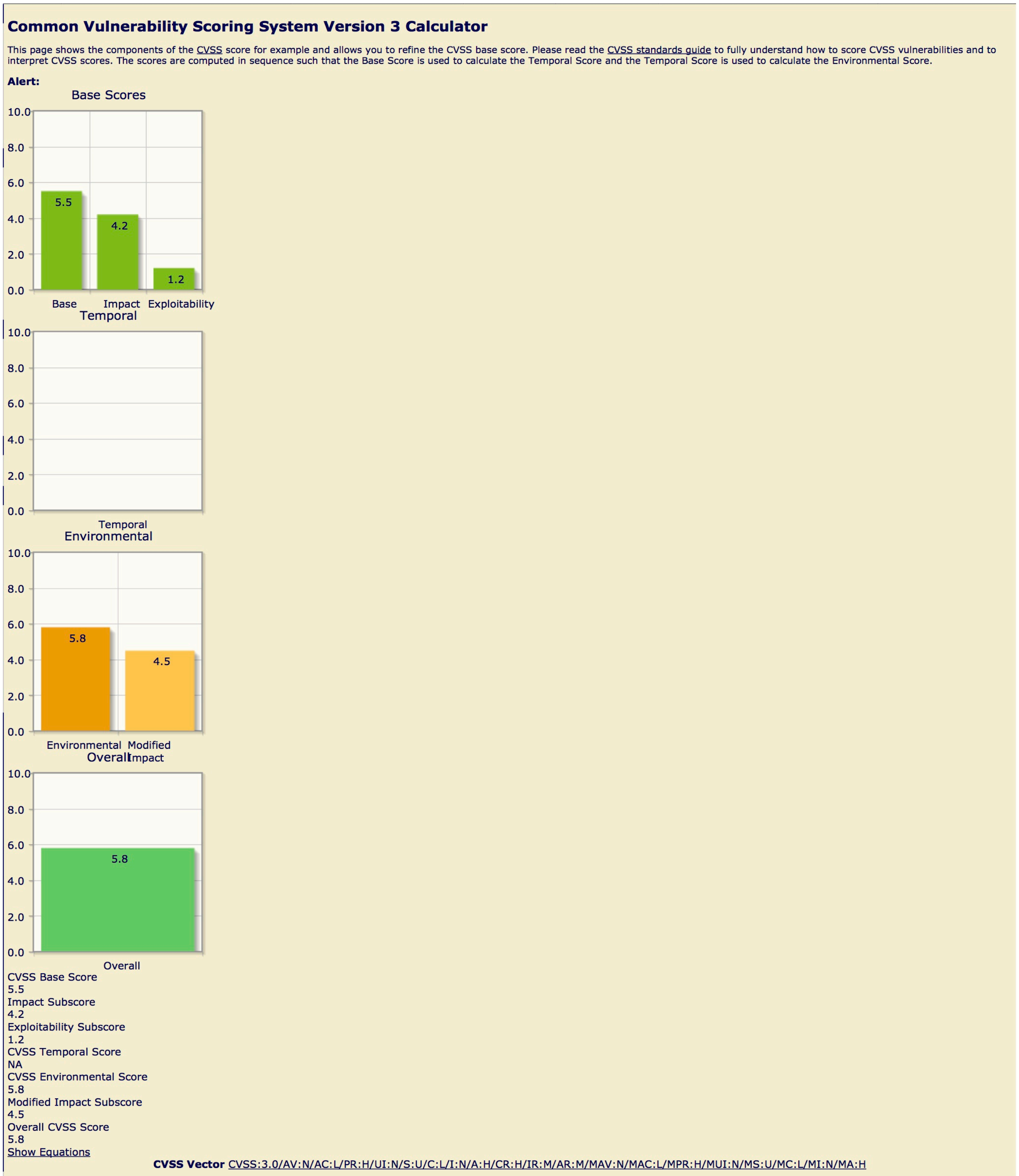
**Alert:**

CVSS Base Score
5.5
Impact Subscore
4.2
Exploitability Subscore
1.2
CVSS Temporal Score
NA
CVSS Environmental Score
5.8
Modified Impact Subscore
4.5
Overall CVSS Score
5.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:H

**Compromise Item: Corp / Law Router**

**Threat to Organization:** Ability to manipulate traffic between Corp and Law subnets of organization
**Indicator of Compromise:** Attacker demonstrates ability to authenticate to device over SSH and enter configure prompt



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

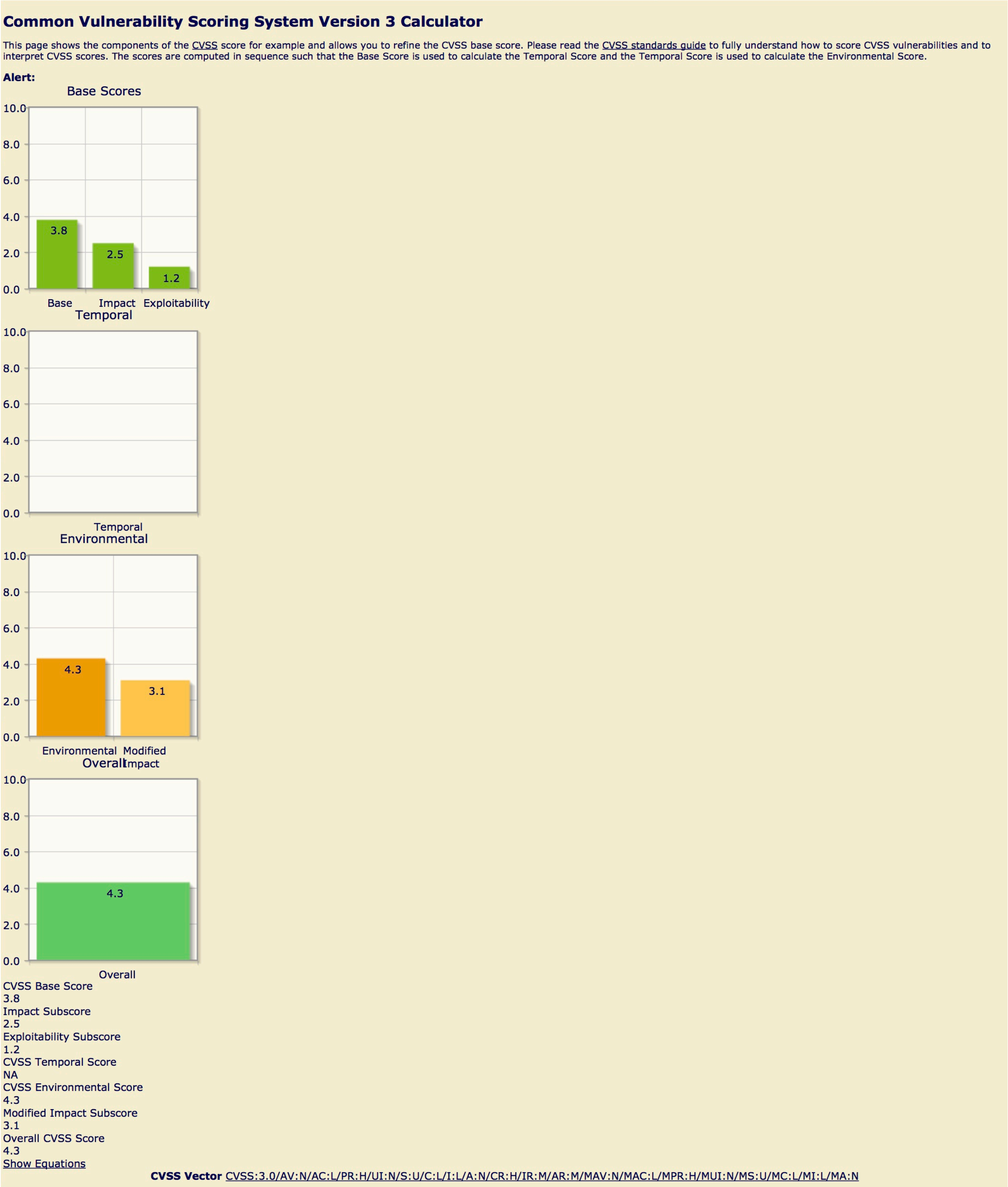
**Alert:**

CVSS Base Score
5.5
Impact Subscore
4.2
Exploitability Subscore
1.2
CVSS Temporal Score
NA
CVSS Environmental Score
5.8
Modified Impact Subscore
4.5
Overall CVSS Score
5.8

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:H

## Compromise Item: Internet FTP Server

**Threat to Organization:** Initial access into organization and ability to observe case files related to currently in court cases as they are placed on this server to be utilized
**Indicator of Compromise:** Ability to authenticate to the server and execute shell code



## Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

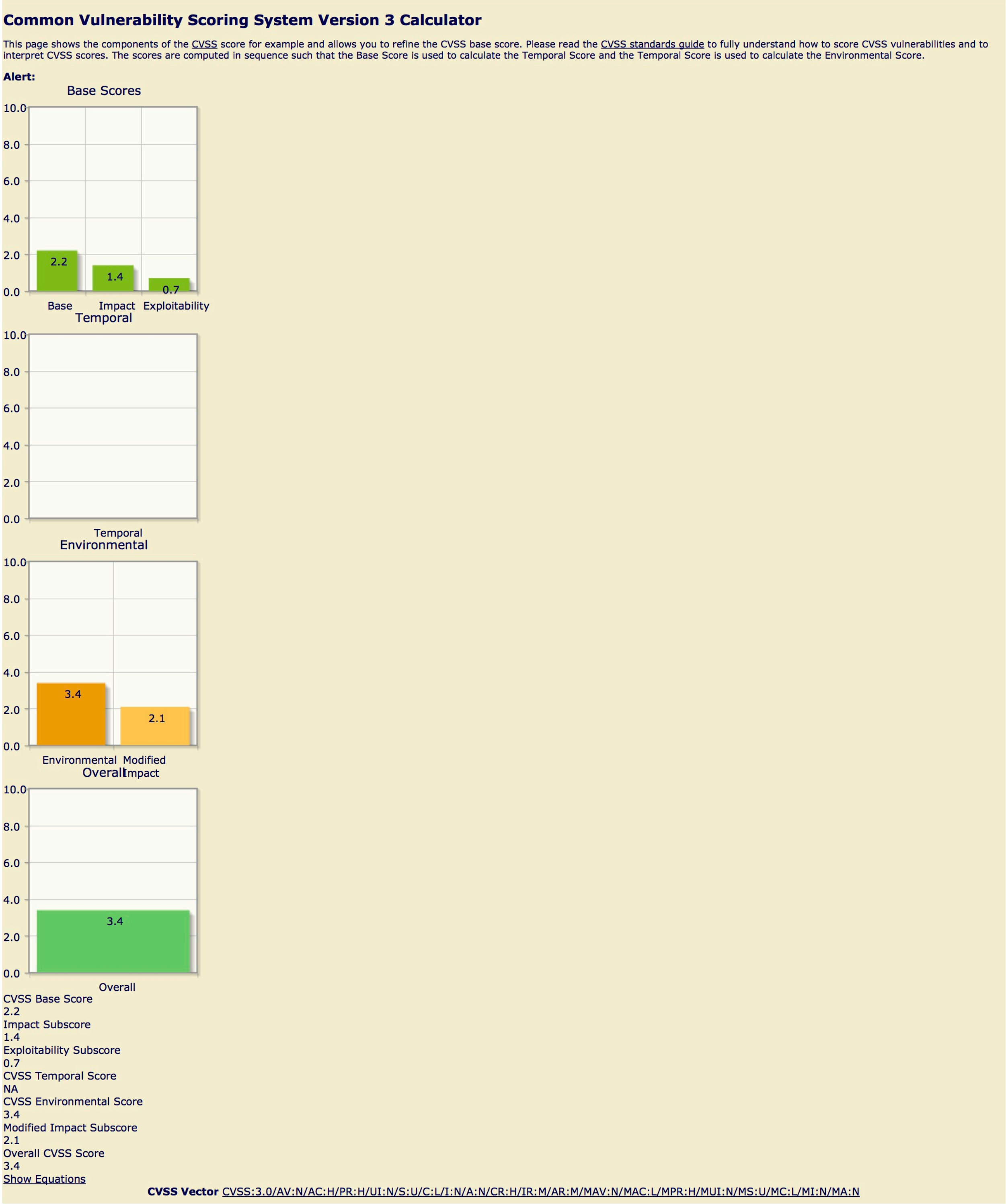
**Alert:**

CVSS Base Score
3.8
Impact Subscore
2.5
Exploitability Subscore
1.2
CVSS Temporal Score
NA
CVSS Environmental Score
4.3
Modified Impact Subscore
3.1
Overall CVSS Score
4.3
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:L/MA:N

## Compromise Item: Client Internet Machine 1

**Threat to Organization:** Ability to steal client specific information of clients who use the machine
**Indicator of Compromise:** Ability to execute code on the machine



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

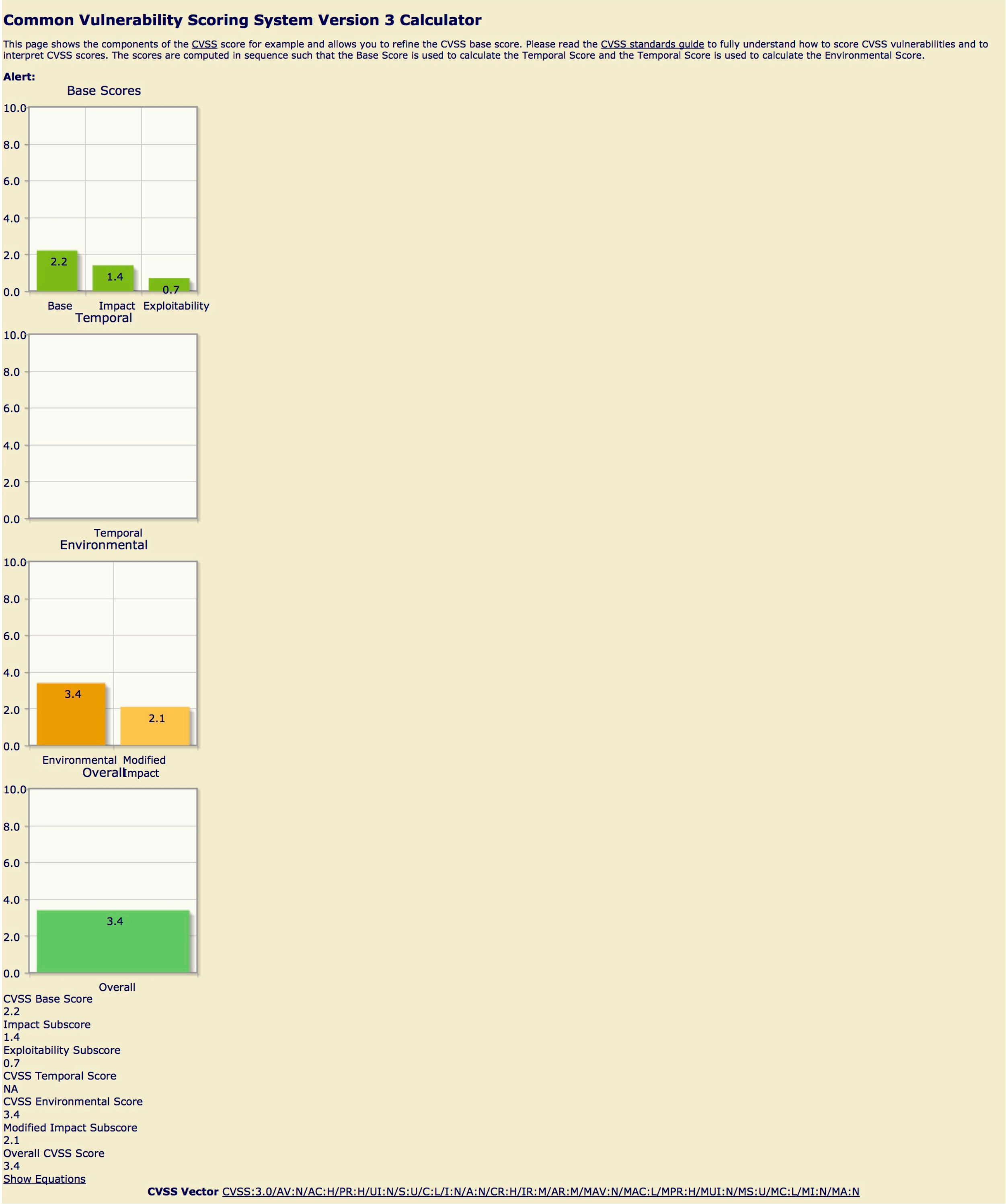
**Alert:**

CVSS Base Score
2.2
Impact Subscore
1.4
Exploitability Subscore
0.7
CVSS Temporal Score
NA
CVSS Environmental Score
3.4
Modified Impact Subscore
2.1
Overall CVSS Score
3.4
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:N

## Compromise Item: Client Internet Machine 2

**Threat to Organization:** Ability to steal client specific information of clients who use the machine
**Indicator of Compromise:** Ability to execute code on the machine



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

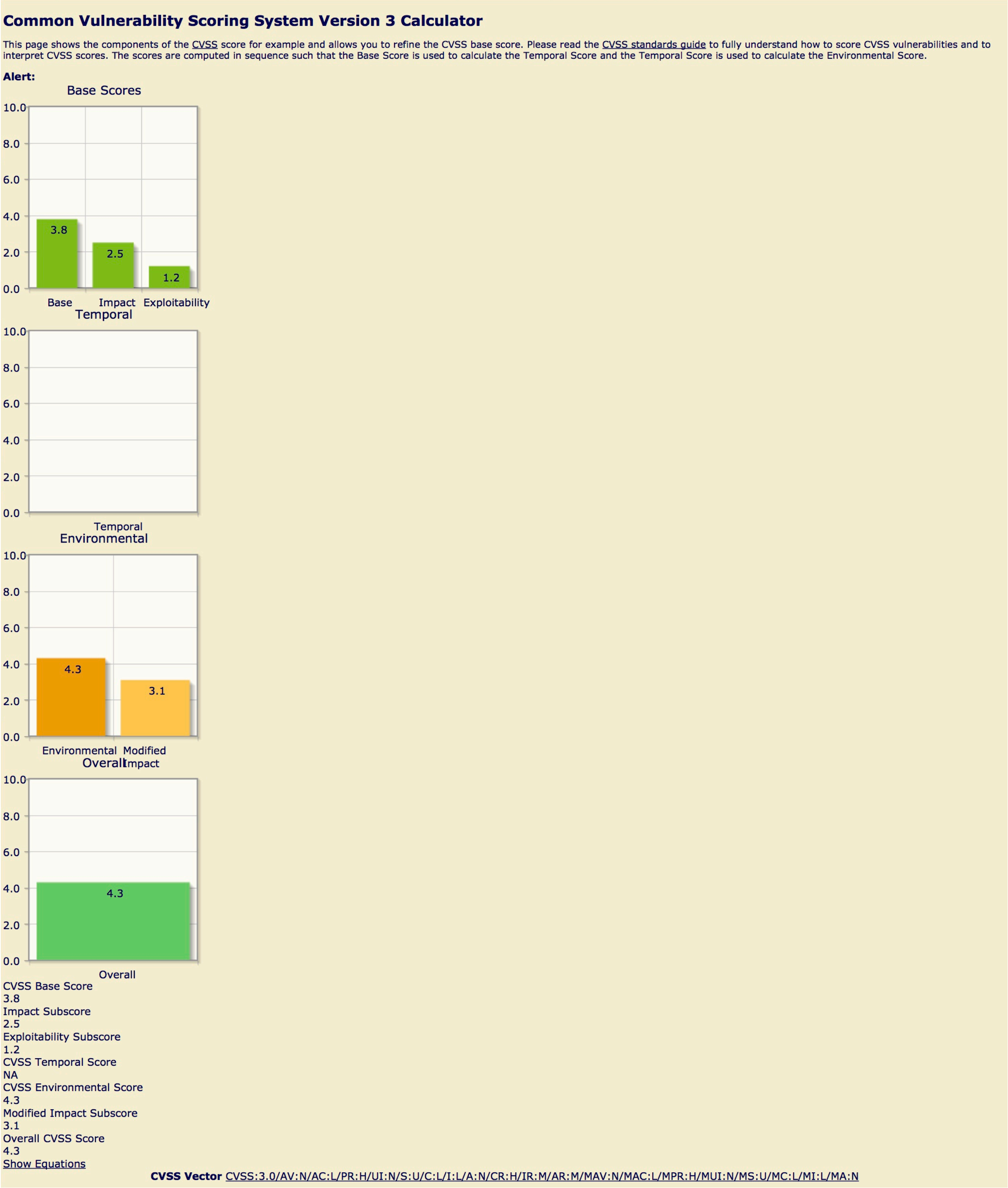
**Alert:**

CVSS Base Score
2.2
Impact Subscore
1.4
Exploitability Subscore
0.7
CVSS Temporal Score
NA
CVSS Environmental Score
3.4
Modified Impact Subscore
2.1
Overall CVSS Score
3.4
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:N

## Compromise Item: Intranet FTP Server

**Threat to Organization:** Ability to observe case files being moved between intranet and internet FTP server
**Indicator of Compromise:** Ability to authenticate to the server and execute shell code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

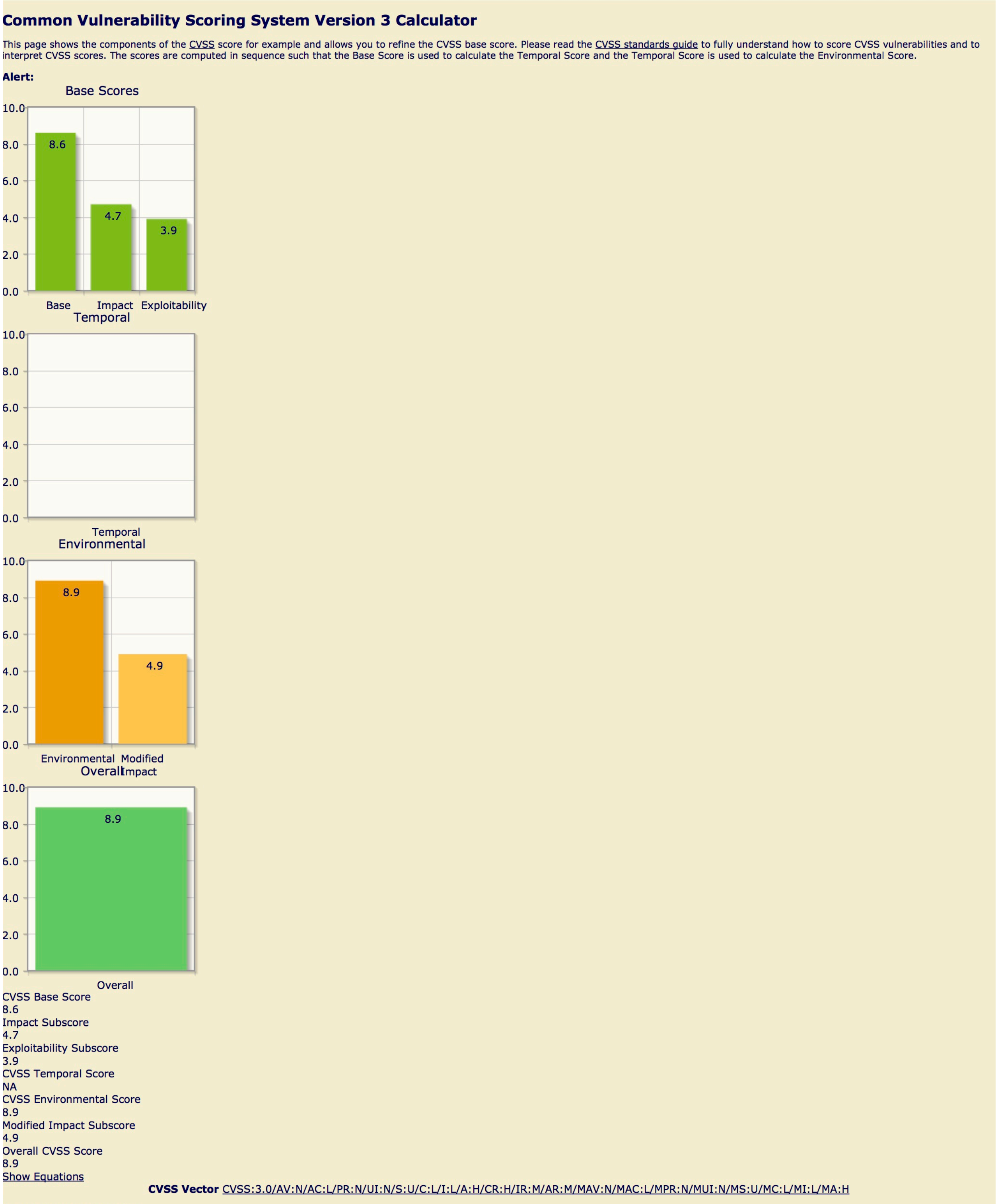
**Alert:**

CVSS Base Score
3.8
Impact Subscore
2.5
Exploitability Subscore
1.2
CVSS Temporal Score
NA
CVSS Environmental Score
4.3
Modified Impact Subscore
3.1
Overall CVSS Score
4.3
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:L/MA:N

## Compromise Item: Domain Controller

**Threat to Organization:** Ability to compromise all the Domain with Administrator privileges
**Indicator of Compromise:** Ability to execute code as System or Domain Administrator



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

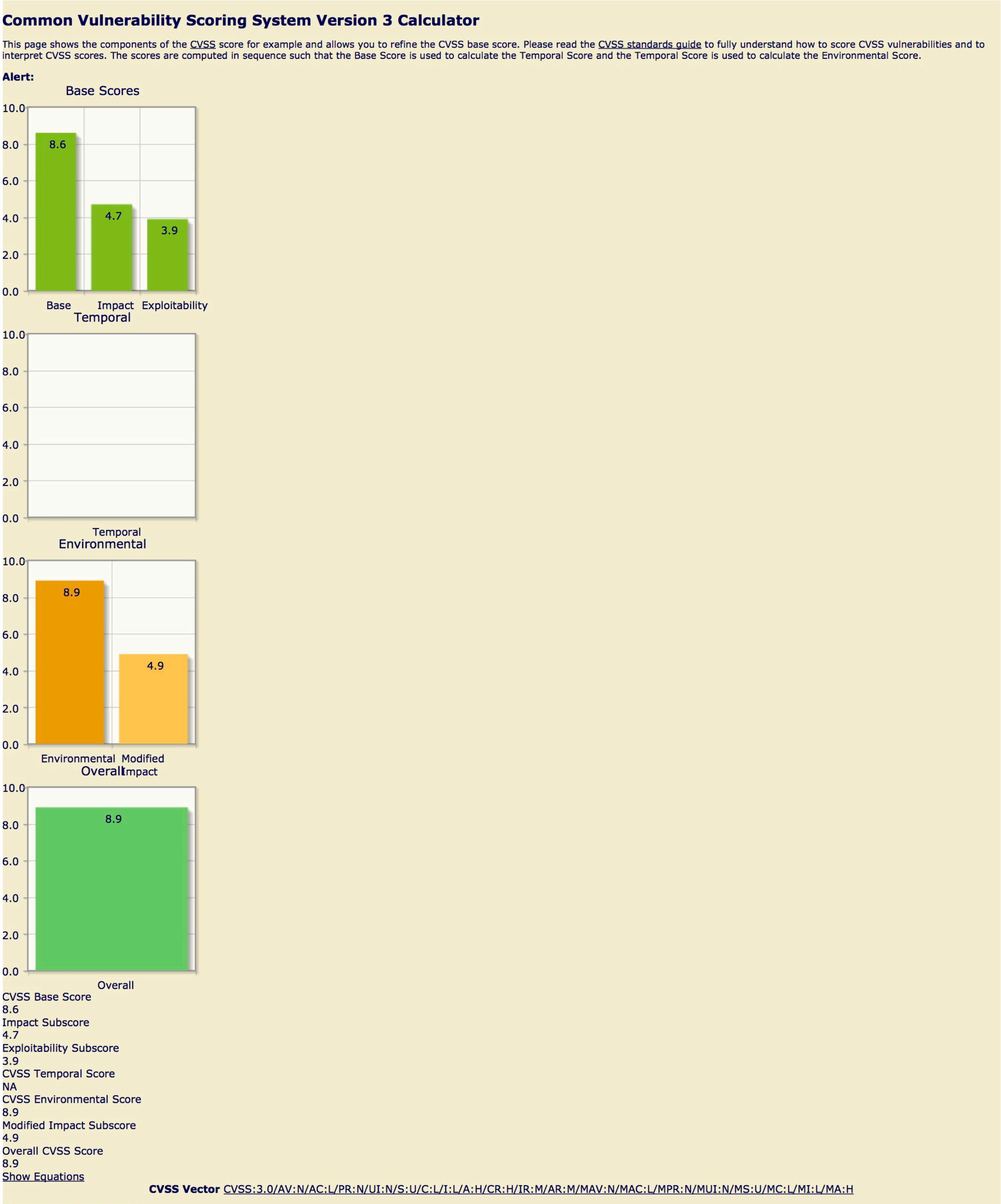
**Alert:**

CVSS Base Score
8.6
Impact Subscore
4.7
Exploitability Subscore
3.9
CVSS Temporal Score
NA
CVSS Environmental Score
8.9
Modified Impact Subscore
4.9
Overall CVSS Score
8.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:L/MA:H

## Compromise Item: Back-UP Domain Controller

**Threat to Organization:** Ability to compromise all the Domain with Administrator privileges
**Indicator of Compromise:** Ability to execute code as System or Domain Administrator



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

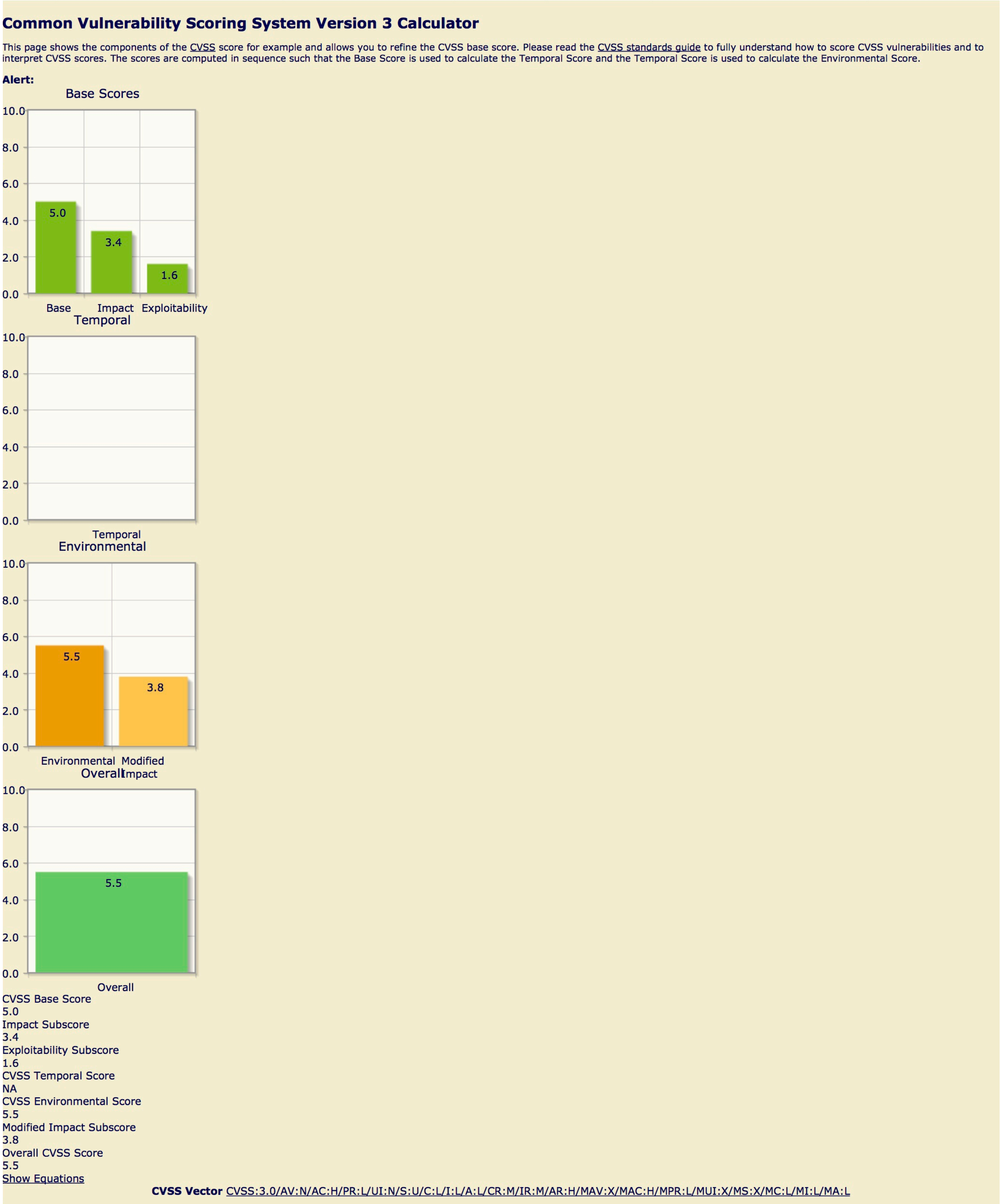
**Alert:**

CVSS Base Score
8.6
Impact Subscore
4.7
Exploitability Subscore
3.9
CVSS Temporal Score
NA
CVSS Environmental Score
8.9
Modified Impact Subscore
4.9
Overall CVSS Score
8.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:L/MA:H

## Compromise Item: Admin Server

**Threat to Organization:** Ability to see information regarding administration of the IT systems
**Indicator of Compromise:** ability to execute code on the machine



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

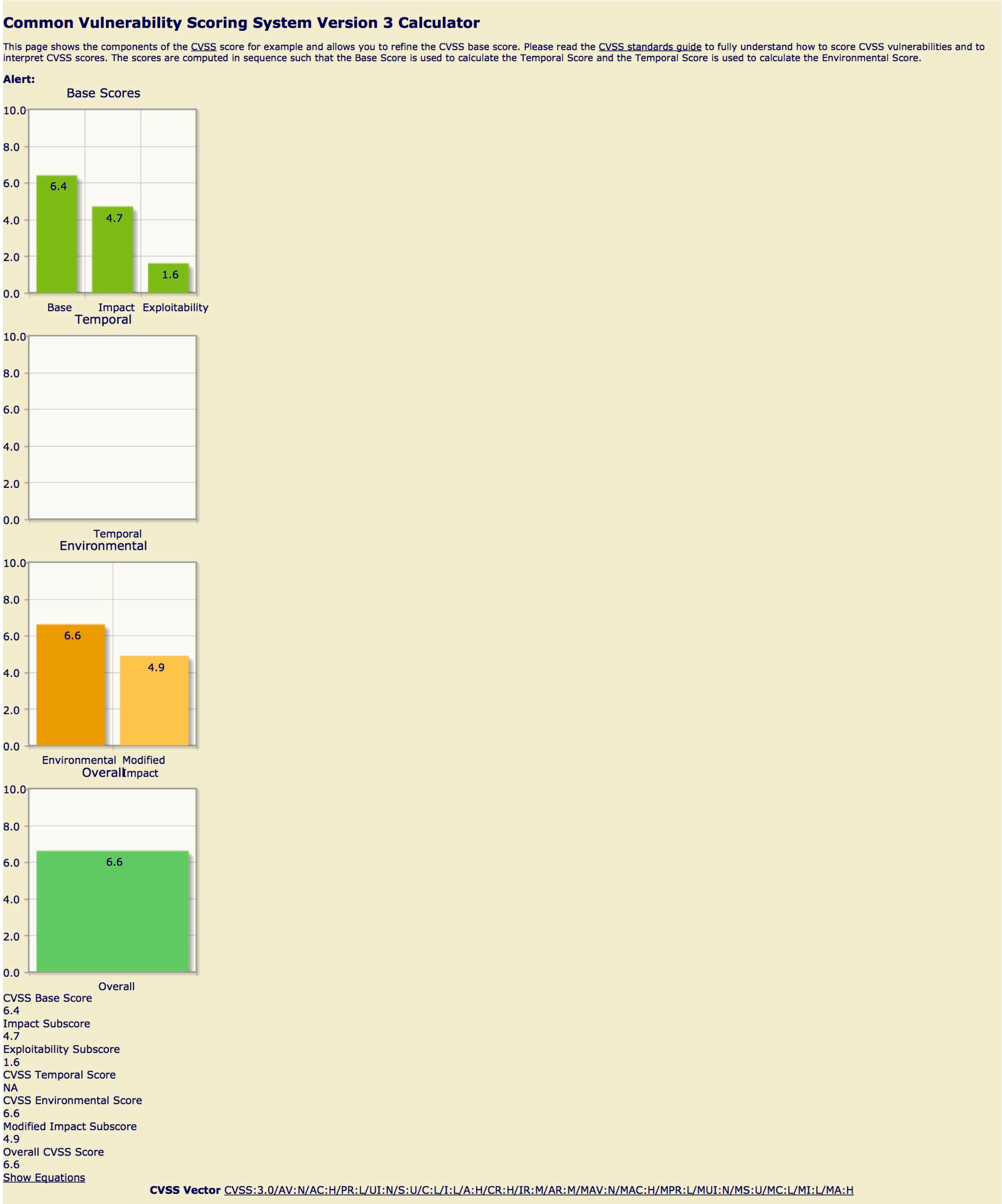
**Alert:**

CVSS Base Score
5.0
Impact Subscore
3.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
5.5
Modified Impact Subscore
3.8
Overall CVSS Score
5.5
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/CR:M/IR:M/AR:H/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:L/MI:L/MA:L

**Compromise Item: Admin Machine**

**Threat to Organization:** Ability to have access to the admin for the domain with the potential of domain compromise
**Indicator of Compromise:** ability to execute code on the machine



## Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

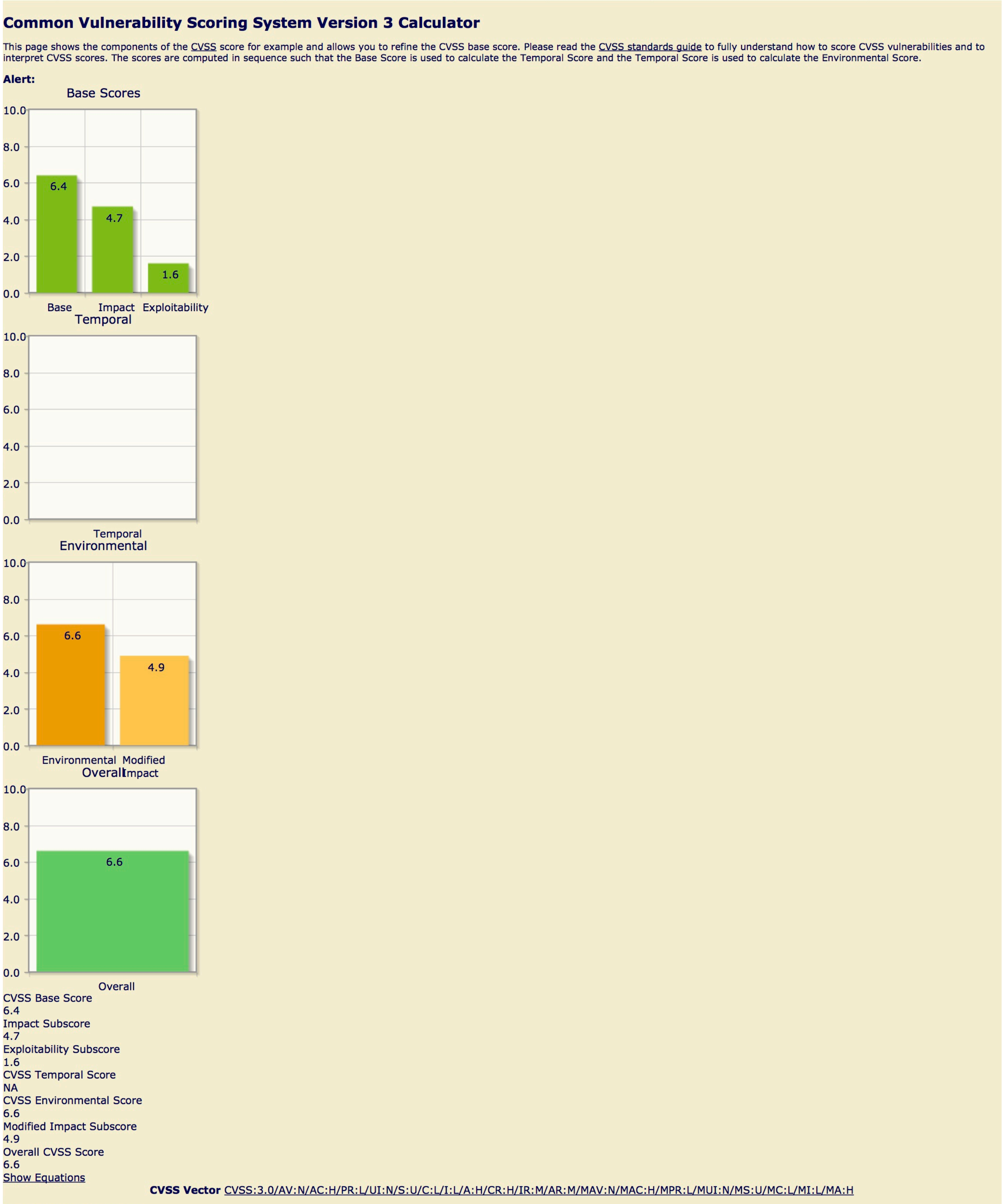
**Alert:**

CVSS Base Score
6.4
Impact Subscore
4.7
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
6.6
Modified Impact Subscore
4.9
Overall CVSS Score
6.6
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:U/MC:L/MI:L/MA:H

## Compromise Item: IT Machine

**Threat to Organization:** Ability to access what the IT administrator for the organization does
**Indicator of Compromise:** ability to execute code on the machine



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

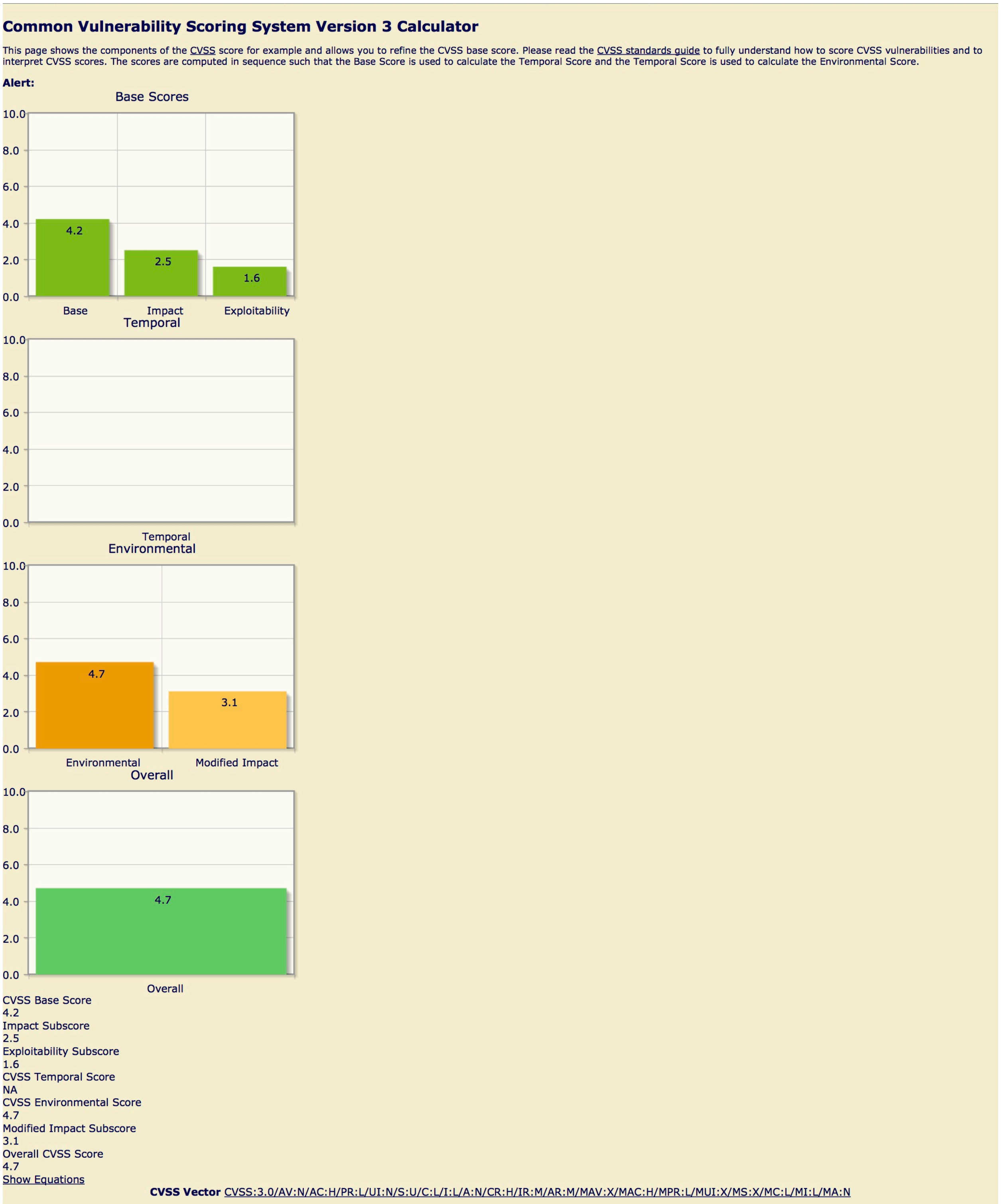
**Alert:**

CVSS Base Score
6.4
Impact Subscore
4.7
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
6.6
Modified Impact Subscore
4.9
Overall CVSS Score
6.6
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:U/MC:L/MI:L/MA:H

## Compromise Item: Chief Executive Officer Machine

**Threat to Organization:** Ability to see the same information as the CEO of firm
**Indicator of Compromise:** Ability to execute code on the machine



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

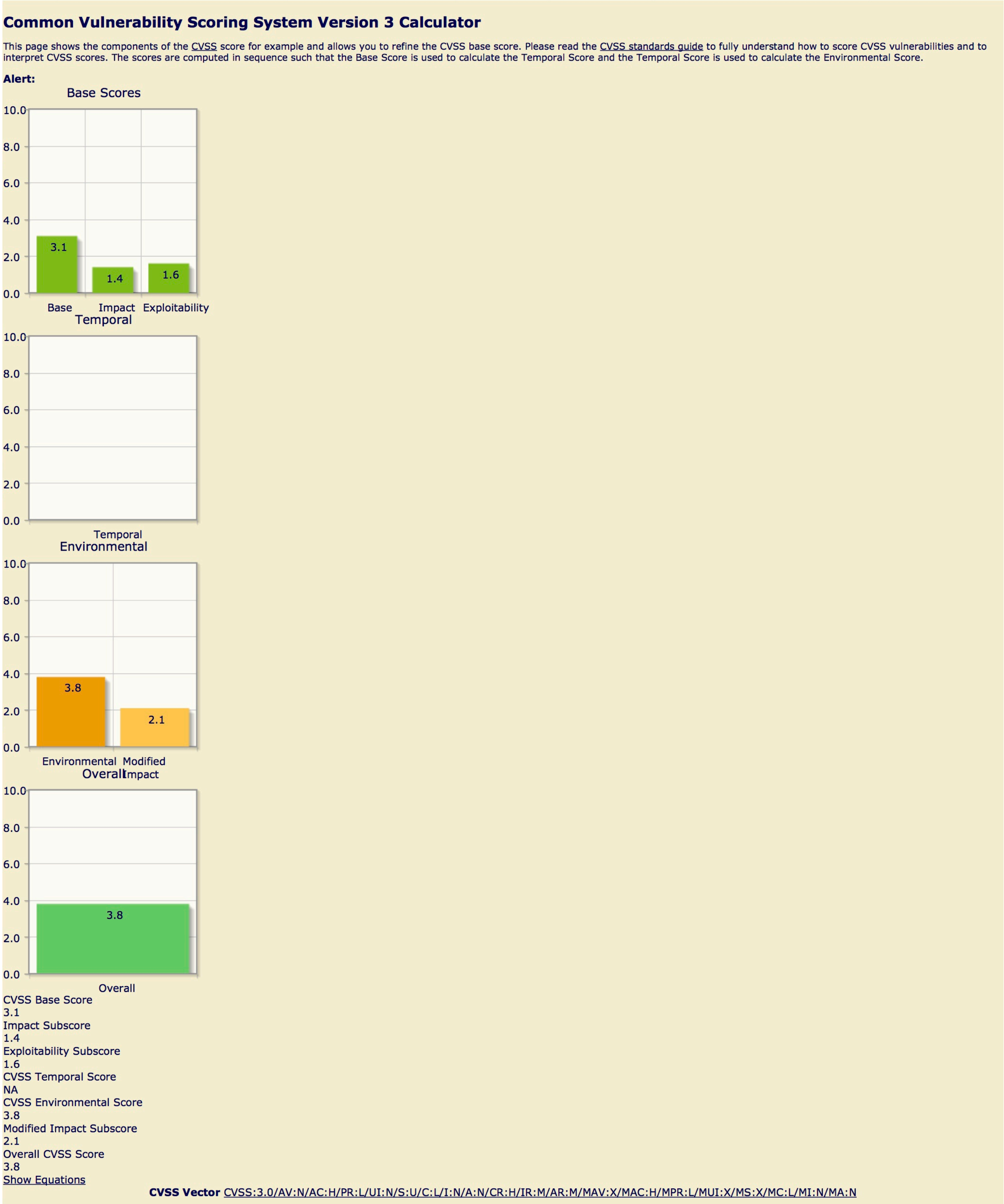
**Alert:**

CVSS Base Score
4.2
Impact Subscore
2.5
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
4.7
Modified Impact Subscore
3.1
Overall CVSS Score
4.7
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:L/MI:L/MA:N

## Compromise Item: VP of Human Resources Machine

**Threat to Organization:** Access to personal information of employees
**Indicator of Compromise:** Ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

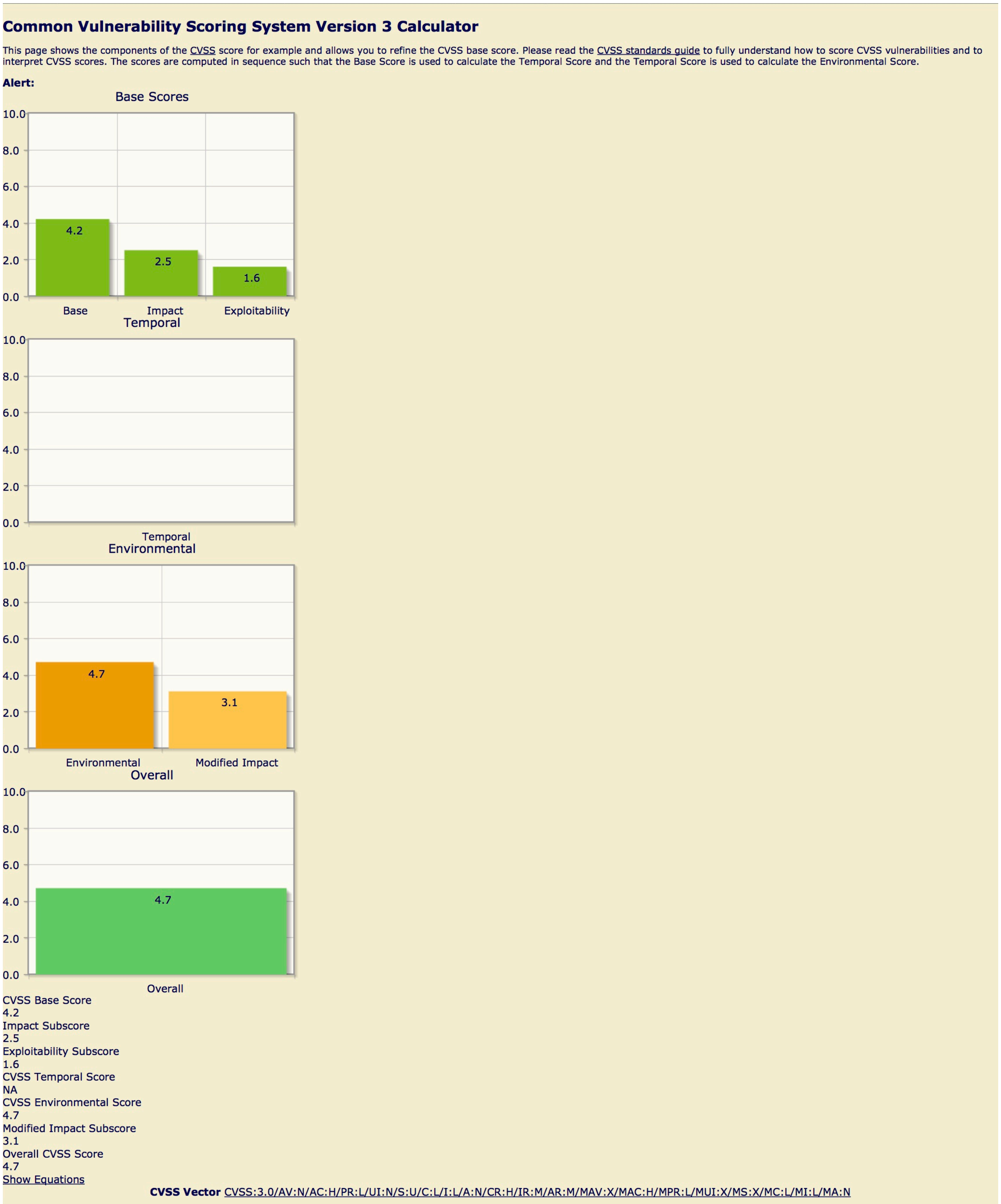
**Alert:**

CVSS Base Score
3.1
Impact Subscore
1.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
3.8
Modified Impact Subscore
2.1
Overall CVSS Score
3.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:L/MI:N/MA:N

**Compromise Item: Chief Financial Officer Machine**

**Threat to Organization:** Ability to view and manipulate budget and financial information of firm
**Indicator of Compromise:** ability to execute code



## Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

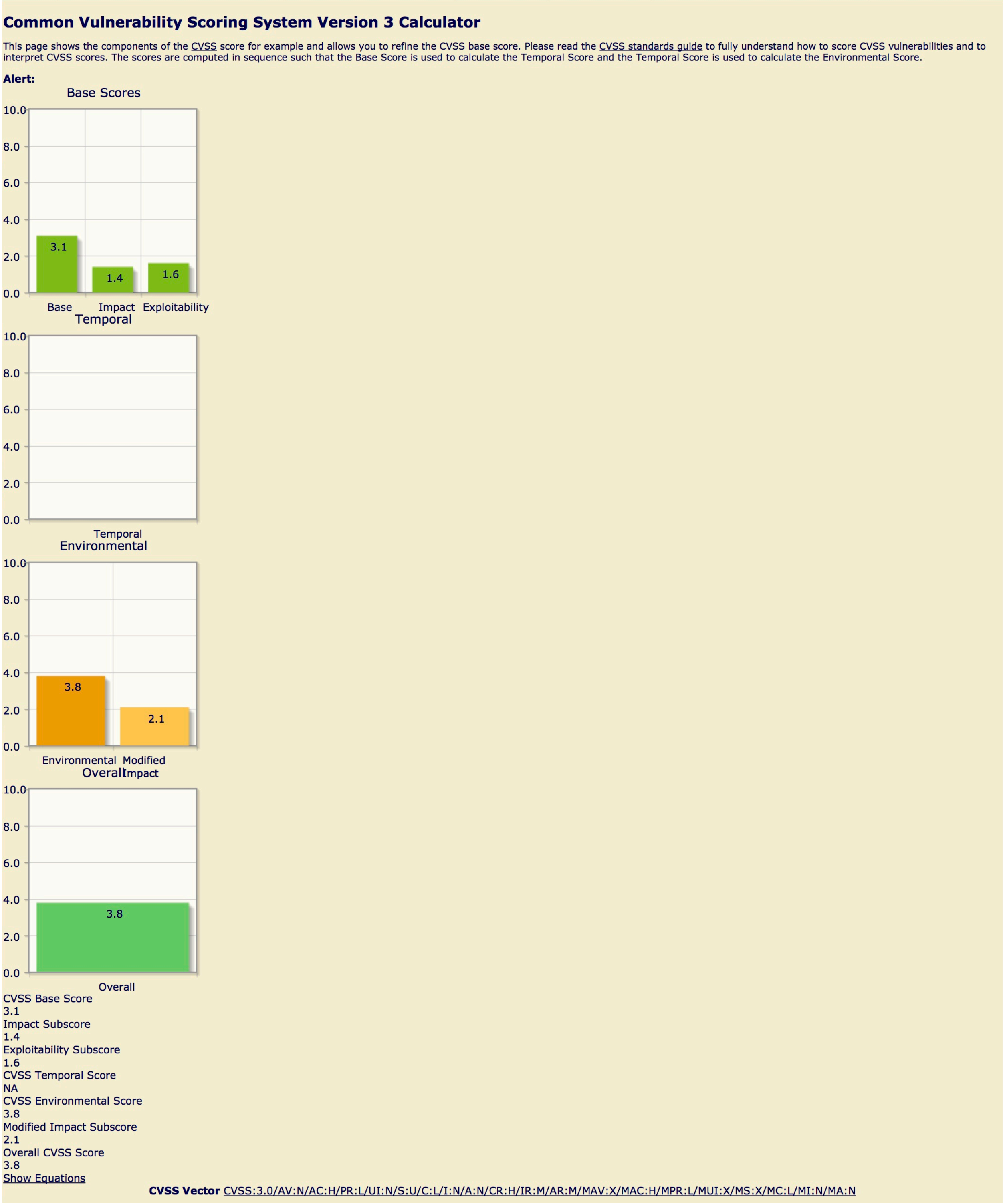
**Alert:**

CVSS Base Score
4.2
Impact Subscore
2.5
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
4.7
Modified Impact Subscore
3.1
Overall CVSS Score
4.7
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:L/MI:L/MA:N

## Compromise Item: Accountant

**Threat to Organization:** Ability to view and manipulate pay roll and accounts of the firm
**Indicator of Compromise:** Ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

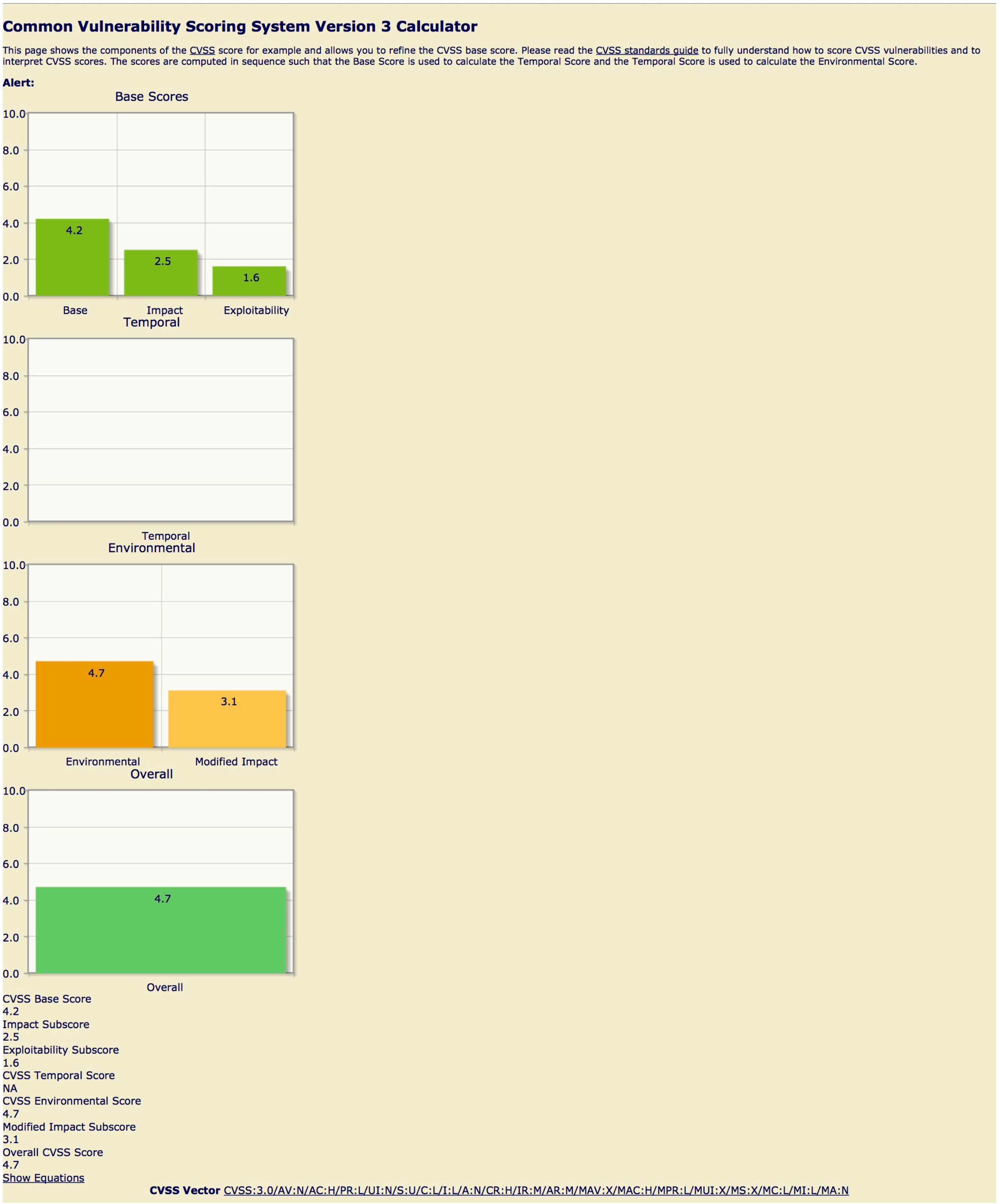
**Alert:**

CVSS Base Score
3.1
Impact Subscore
1.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
3.8
Modified Impact Subscore
2.1
Overall CVSS Score
3.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:L/MI:N/MA:N

**Compromise Item: Chief Technology Officer**

**Threat to Organization:** Ability to view and manipulate information regarding technology choices of the firm
**Indicator of Compromise:** Ability to execute code



## Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

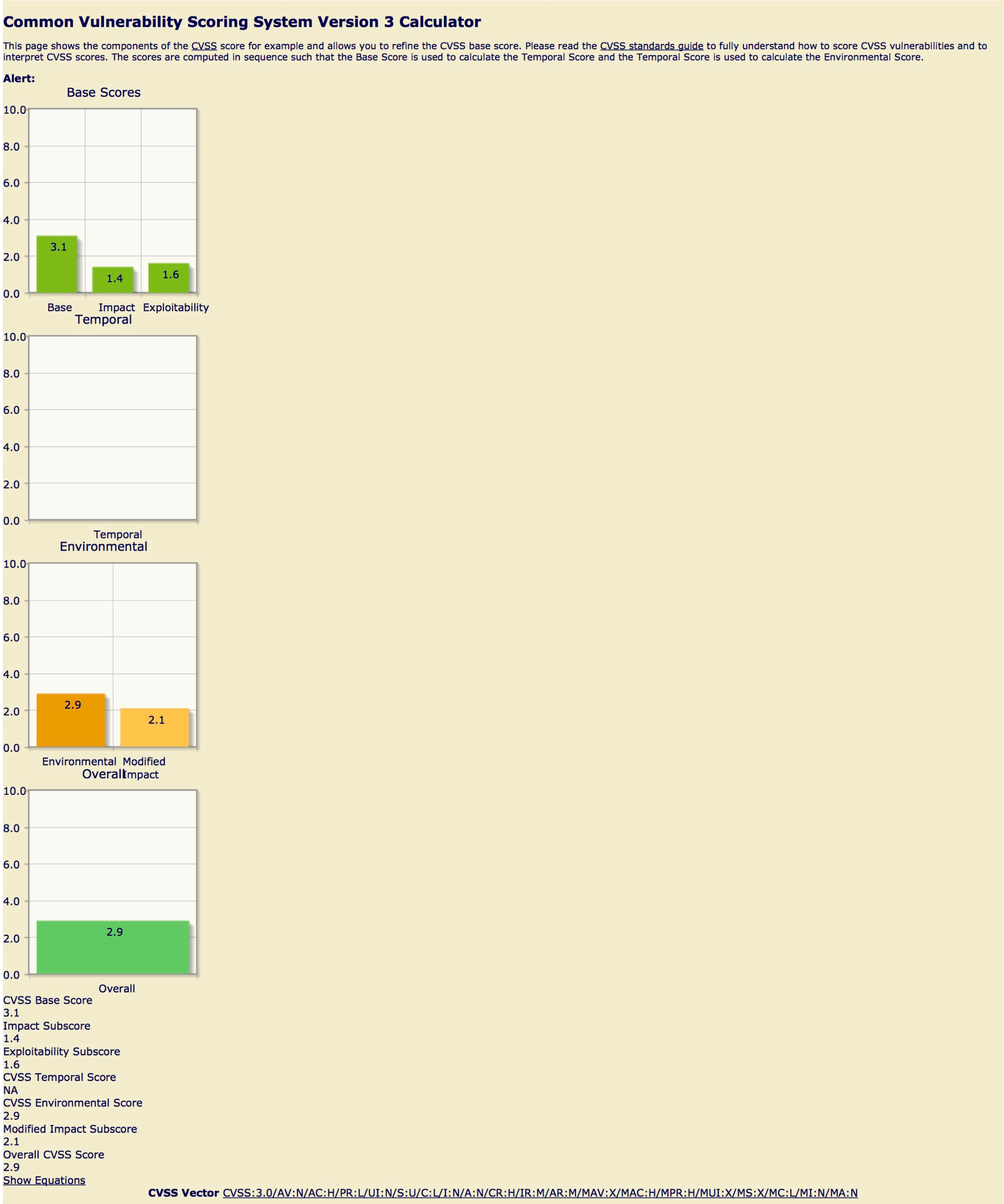
**Alert:**

CVSS Base Score
4.2
Impact Subscore
2.5
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
4.7
Modified Impact Subscore
3.1
Overall CVSS Score
4.7
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:L/MI:L/MA:N

## Compromise Item: Office Assistant 2 Machine

**Threat to Organization:** Ability to access files and schedules the office assistant maintains
**Indicator of Compromise:** Ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

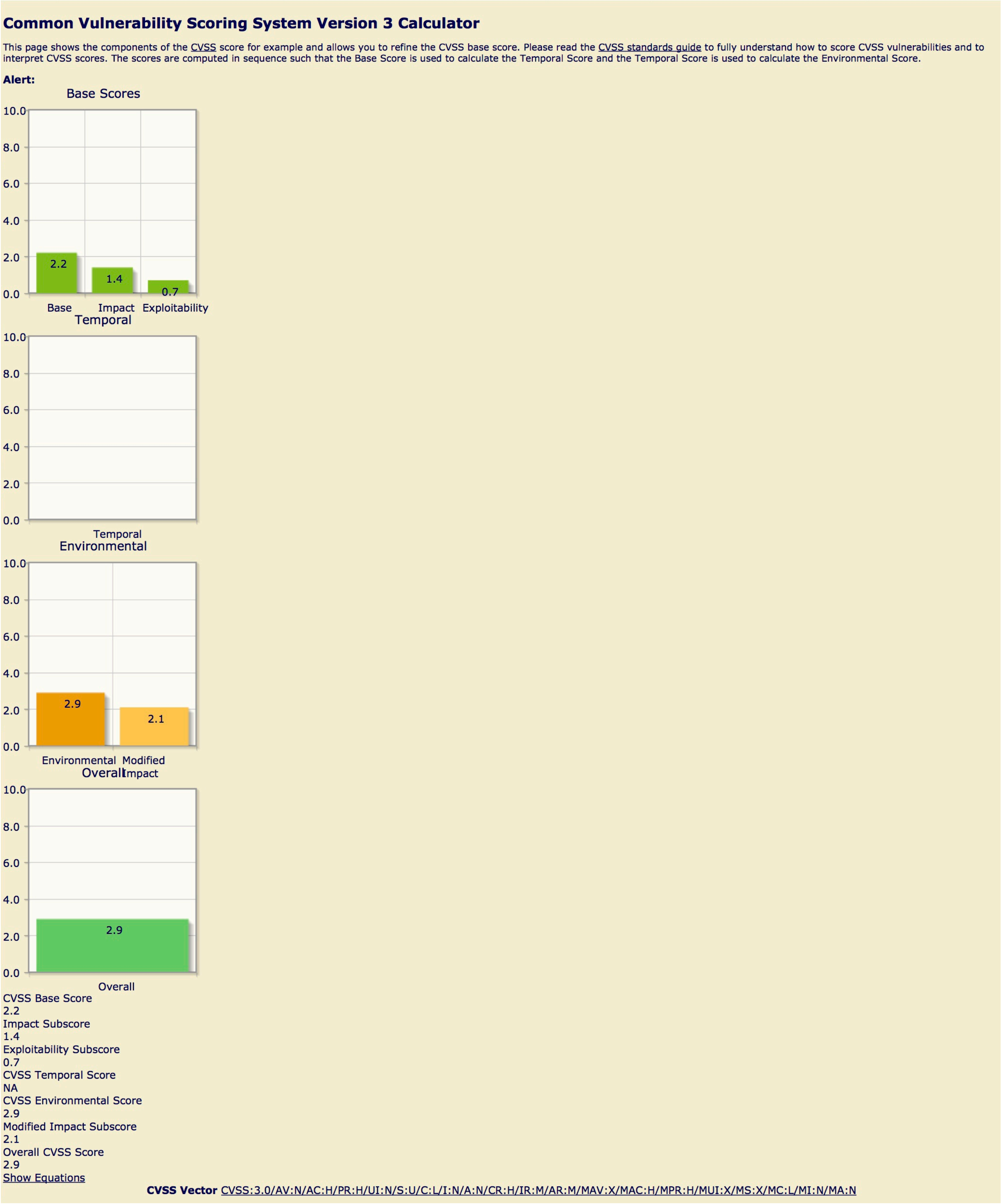
**Alert:**

CVSS Base Score
3.1
Impact Subscore
1.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
2.9
Modified Impact Subscore
2.1
Overall CVSS Score
2.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:H/MUI:X/MS:X/MC:L/MI:N/MA:N

## Compromise Item: Big Conference Room Machine

**Threat to Organization:** Ability to know what information is being addressed at meetings
**Indicator of Compromise:** Ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

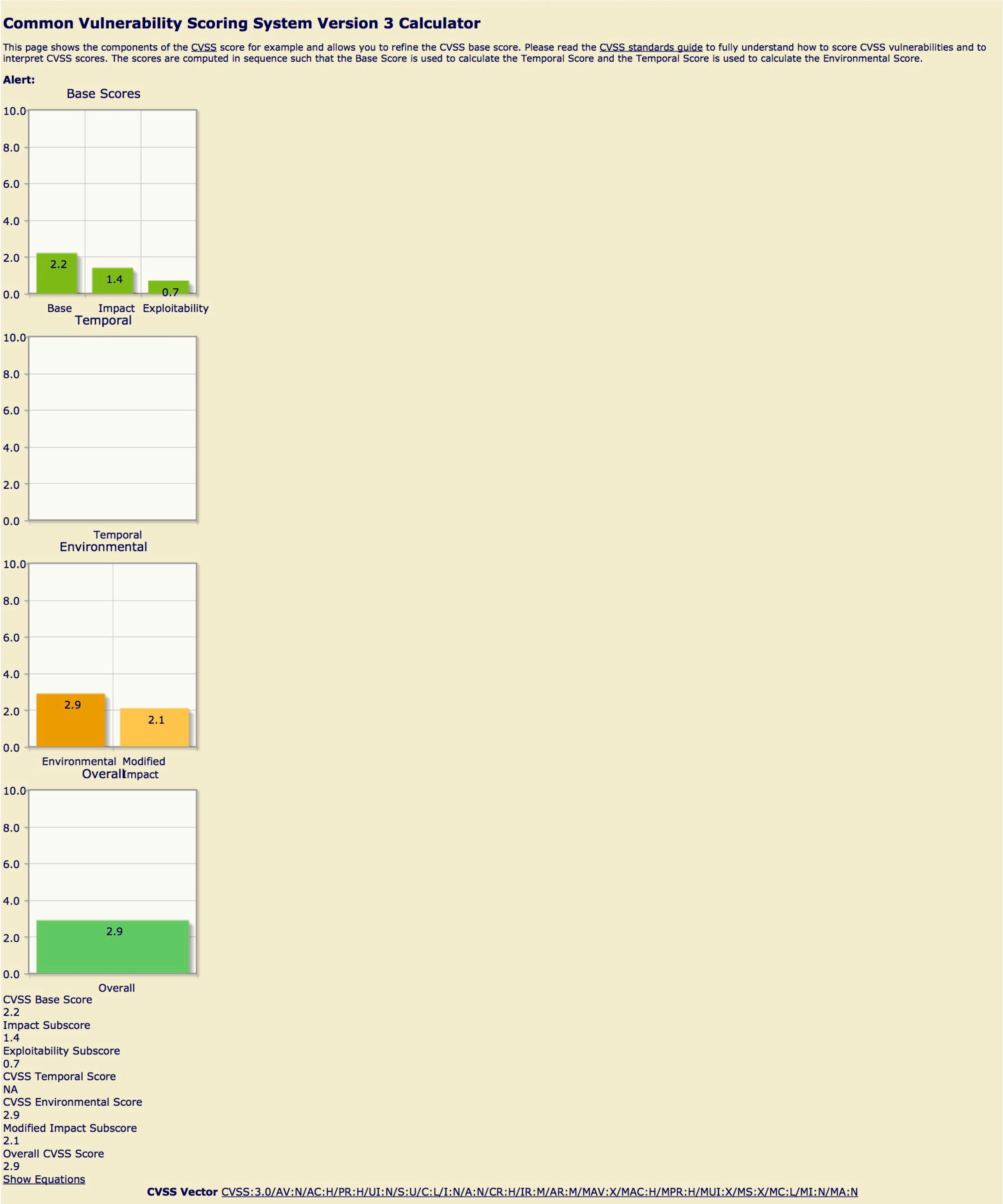
**Alert:**

CVSS Base Score
2.2
Impact Subscore
1.4
Exploitability Subscore
0.7
CVSS Temporal Score
NA
CVSS Environmental Score
2.9
Modified Impact Subscore
2.1
Overall CVSS Score
2.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:H/MUI:X/MS:X/MC:L/MI:N/MA:N

## Compromise Item: Small Conference Room Machine

**Threat to Organization:** Ability to know what information is being addressed in this room
**Indicator of Compromise:** Ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

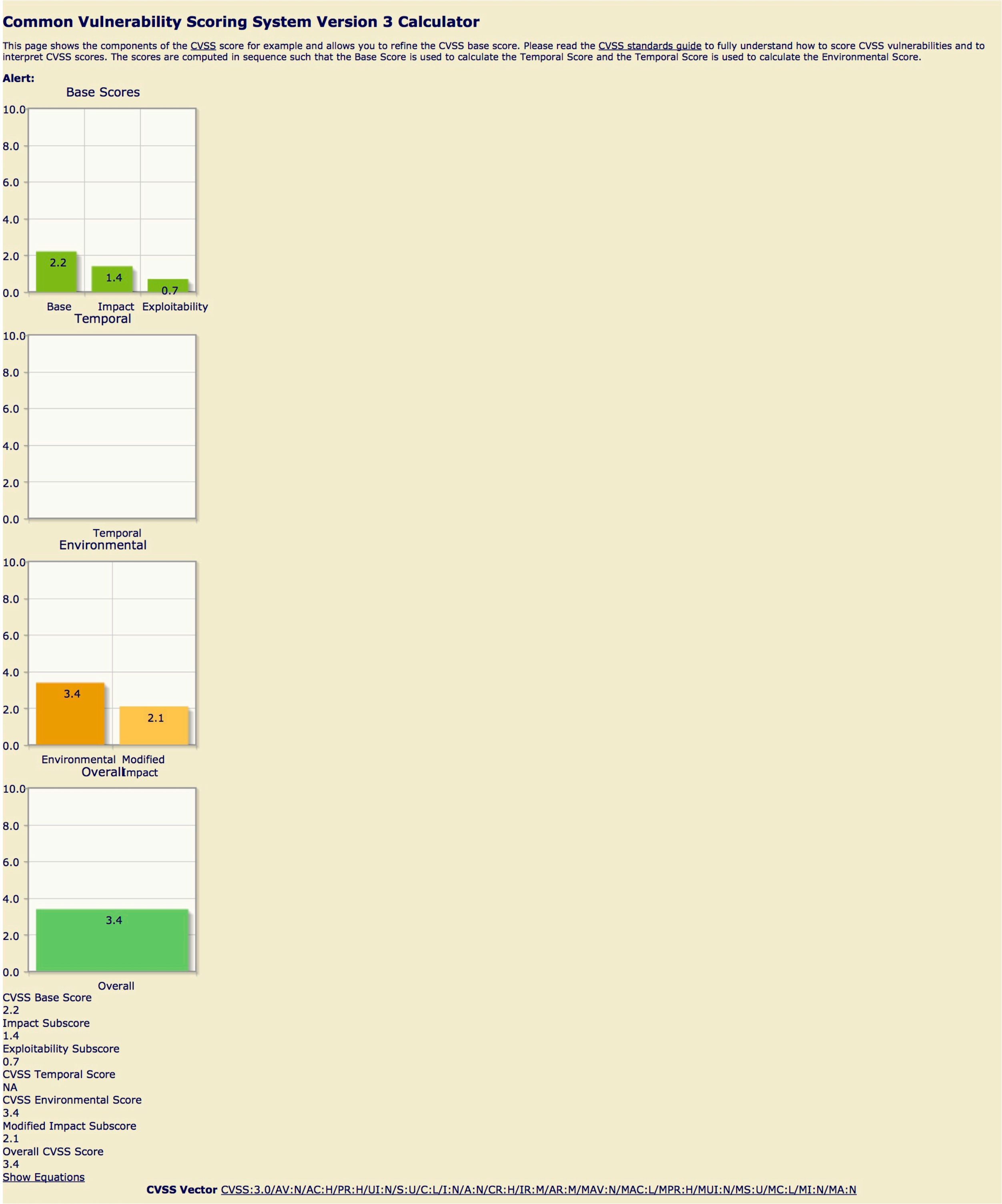
**Alert:**

CVSS Base Score
2.2
Impact Subscore
1.4
Exploitability Subscore
0.7
CVSS Temporal Score
NA
CVSS Environmental Score
2.9
Modified Impact Subscore
2.1
Overall CVSS Score
2.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:H/MUI:X/MS:X/MC:L/MI:N/MA:N

## Compromise Item: Interview Room 1 Machine

**Threat to Organization:** Ability to see information used by interviewers / interviewees
**Indicator of Compromise:** Ability to execute Code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

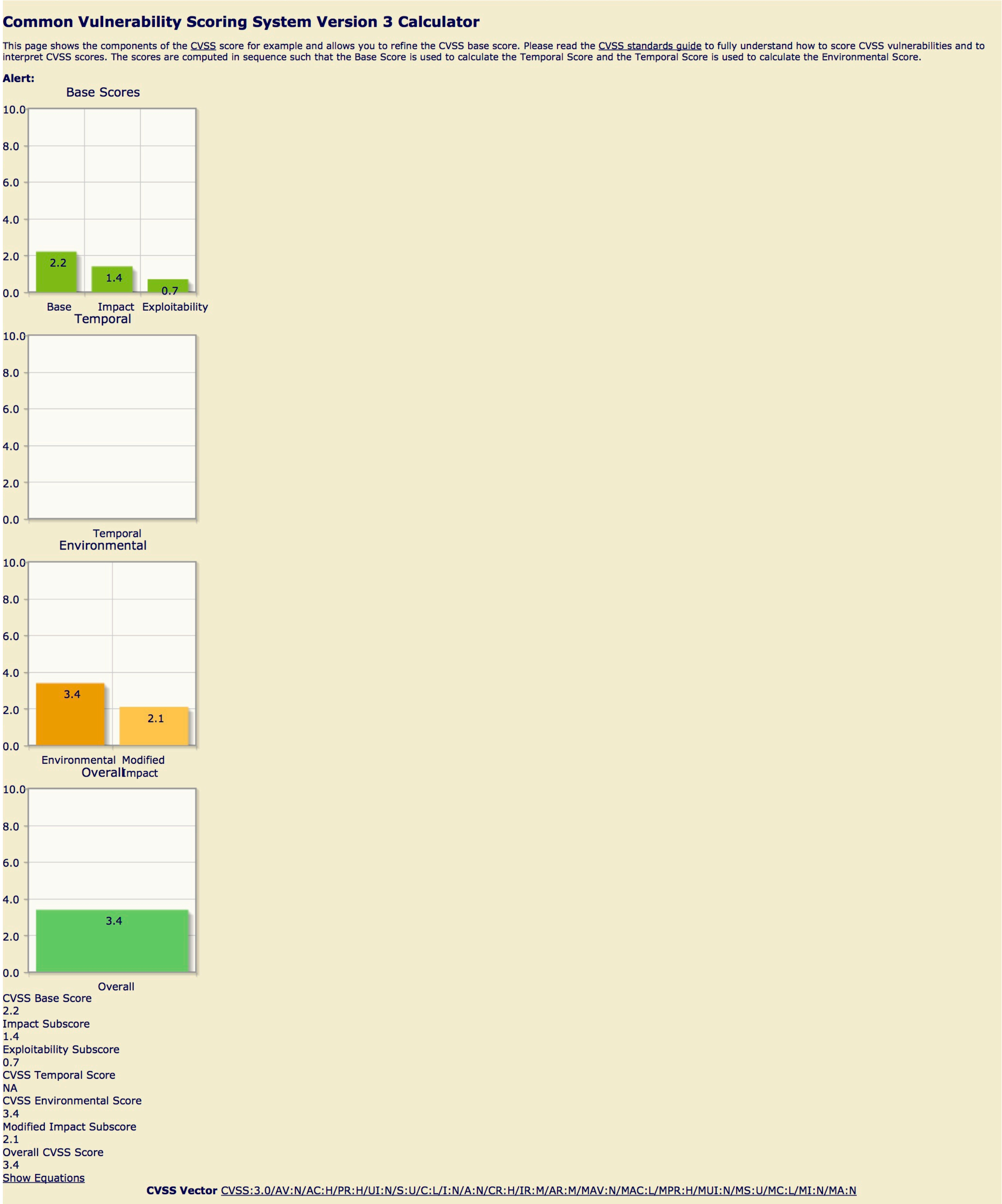
**Alert:**

CVSS Base Score
2.2
Impact Subscore
1.4
Exploitability Subscore
0.7
CVSS Temporal Score
NA
CVSS Environmental Score
3.4
Modified Impact Subscore
2.1
Overall CVSS Score
3.4
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:N

### Compromise Item: Interview Room 2 Machine

**Threat to Organization:** Ability to see information used by interviewers / interviewees
**Indicator of Compromise:** Ability to execute Code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

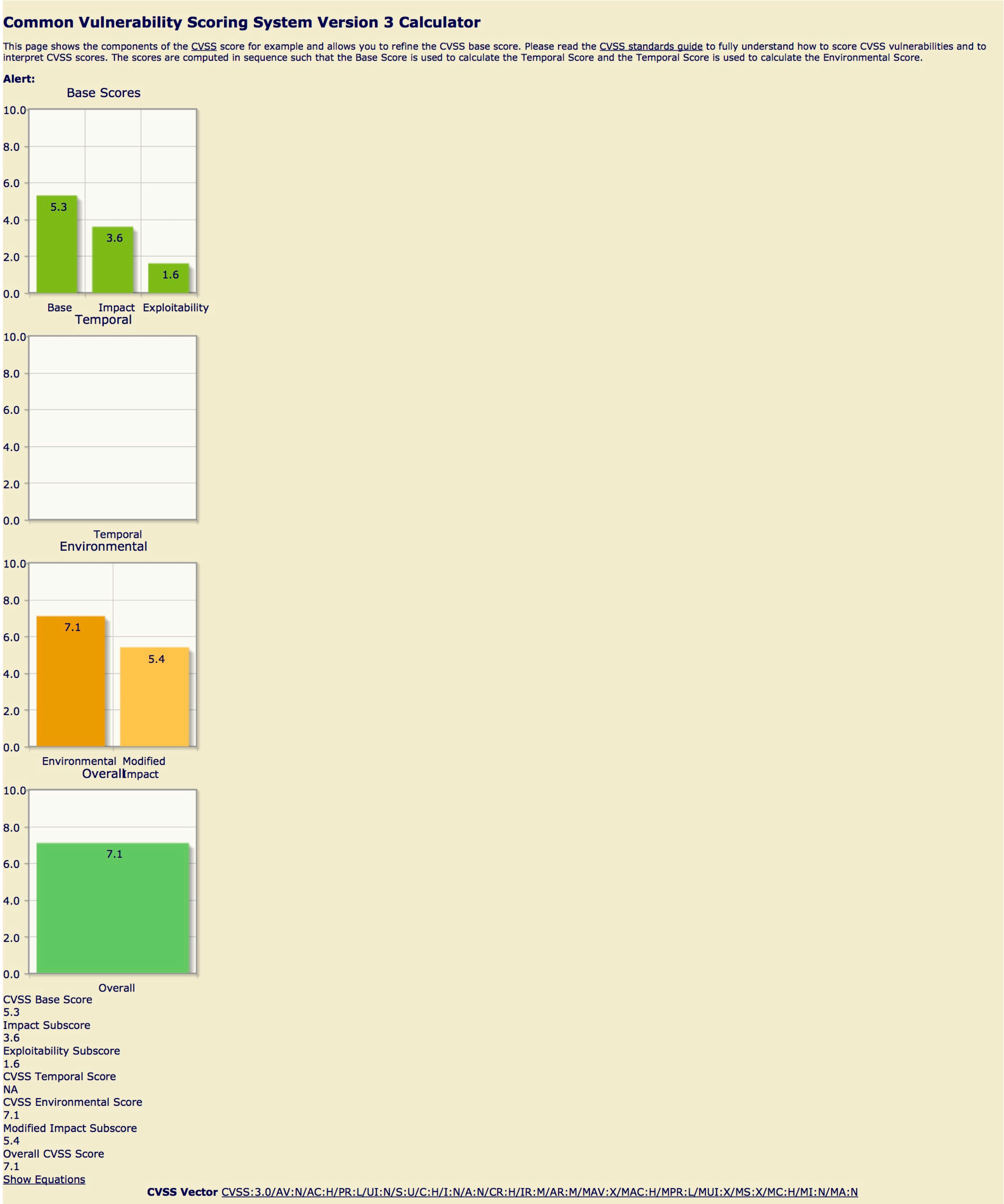
**Alert:**

CVSS Base Score
2.2
Impact Subscore
1.4
Exploitability Subscore
0.7
CVSS Temporal Score
NA
CVSS Environmental Score
3.4
Modified Impact Subscore
2.1
Overall CVSS Score
3.4
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:N/MA:N

## Compromise Item: Partner 1 Machine

**Threat to Organization:** Ability to see all legal materials for Partner 1 Team cases
**Indicator of Compromise:** ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

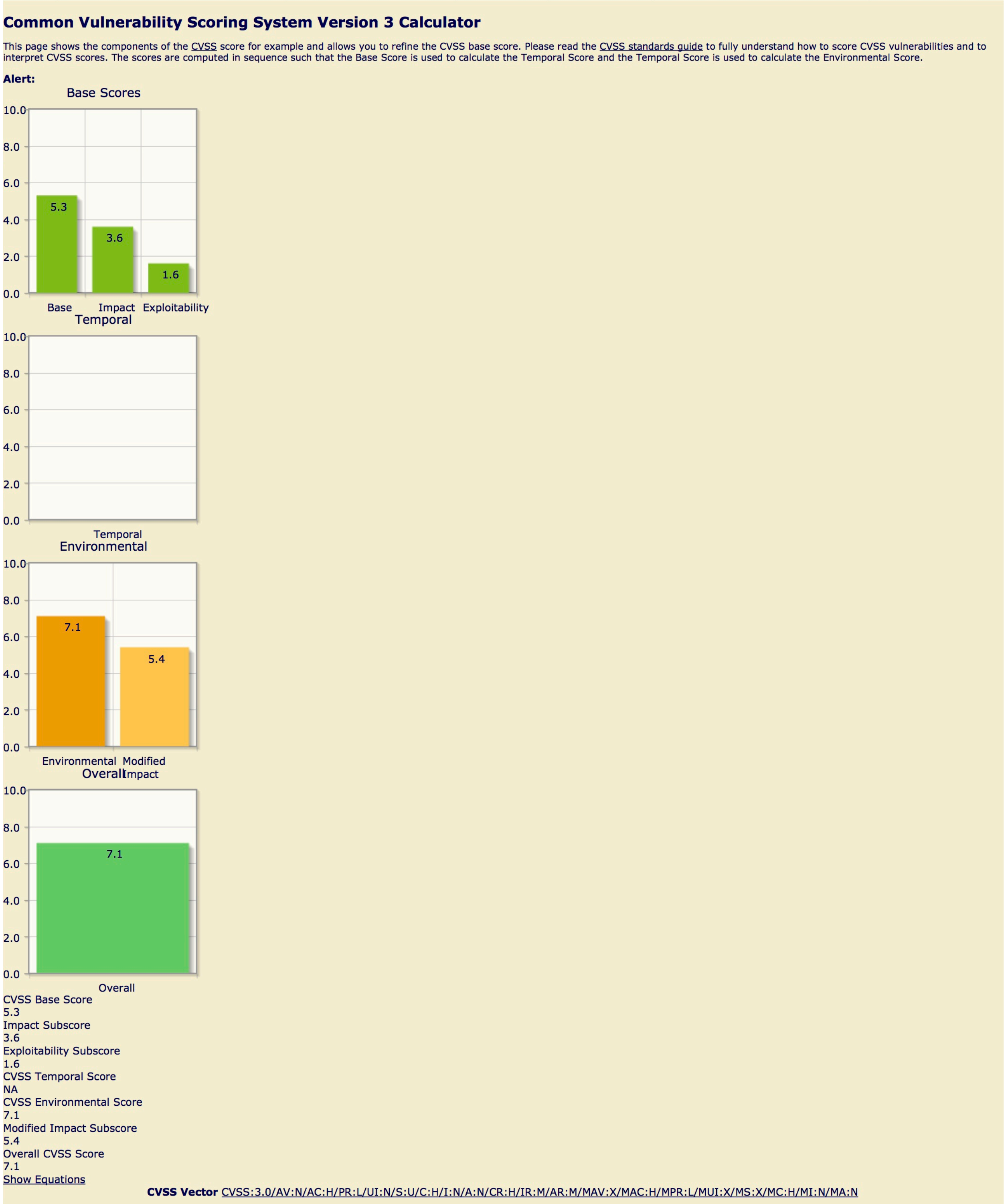
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 1 Nephew Machine

**Threat to Organization:** Ability to see all legal materials for Partner 1 Team cases
**Indicator of Compromise:** ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

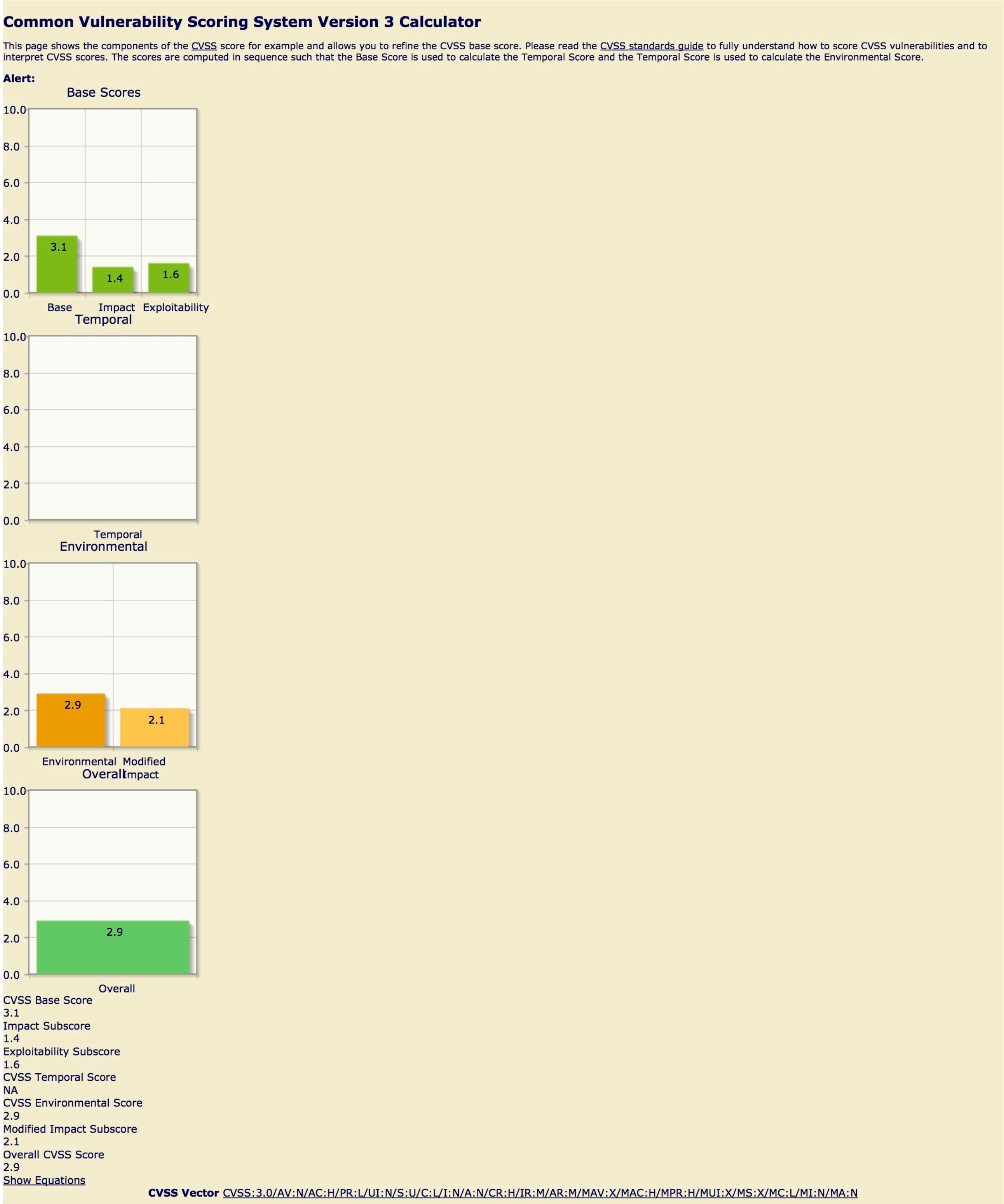
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 1 Secretary Machine

**Threat to Organization:** Ability to see all legal materials for Partner 1 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

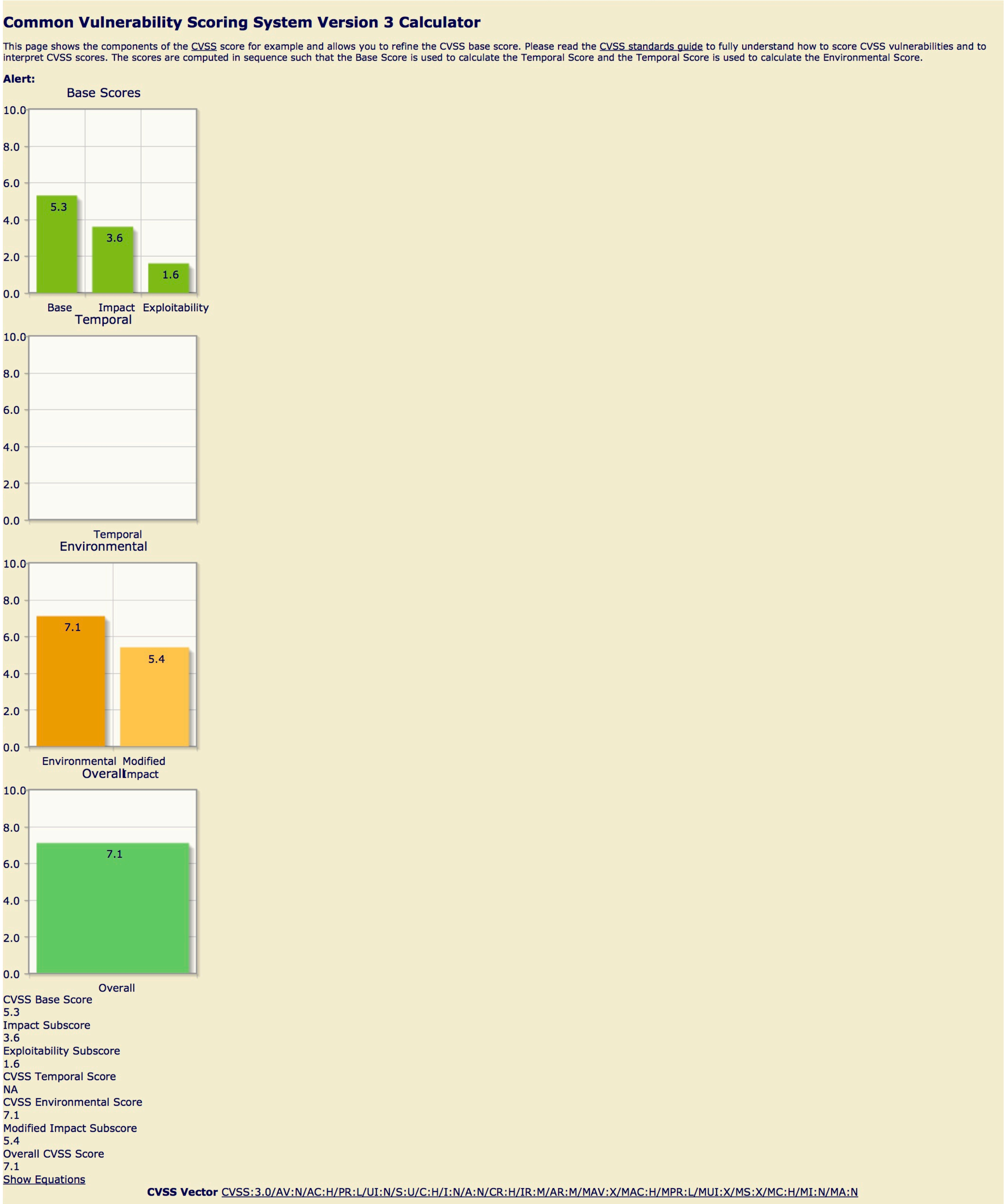
**Alert:**

CVSS Base Score
3.1
Impact Subscore
1.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
2.9
Modified Impact Subscore
2.1
Overall CVSS Score
2.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:H/MUI:X/MS:X/MC:L/MI:N/MA:N

## Compromise Item: Partner 1 Legal Aid 1 Machine

**Threat to Organization:** Ability to see all legal materials for Partner 1 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

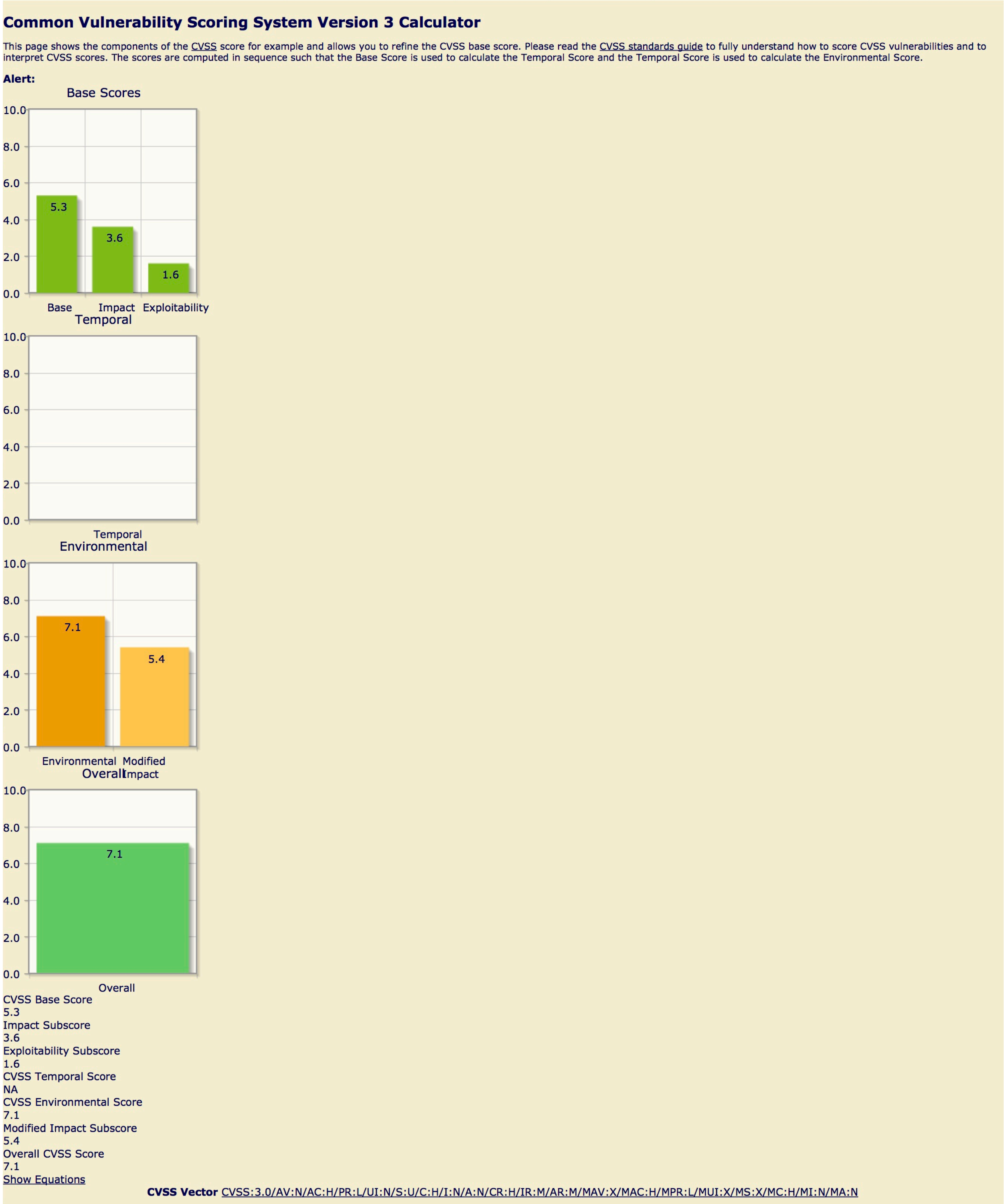
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 1 Legal Aid 2 Machine

**Threat to Organization:** Ability to see all legal materials for Partner 1 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

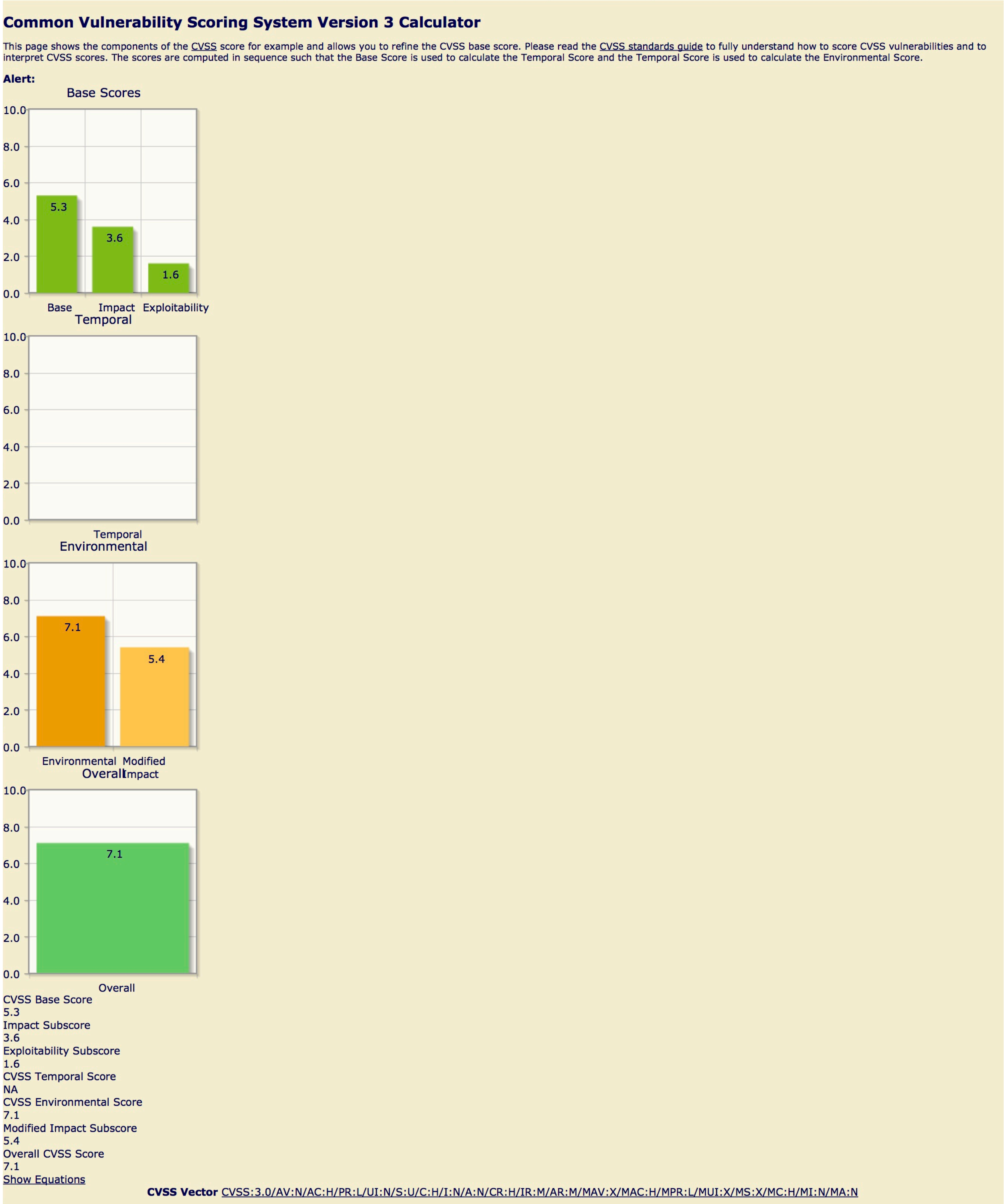
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 2 Machine

**Threat to Organization:** Ability to see all legal materials for Partner 2 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

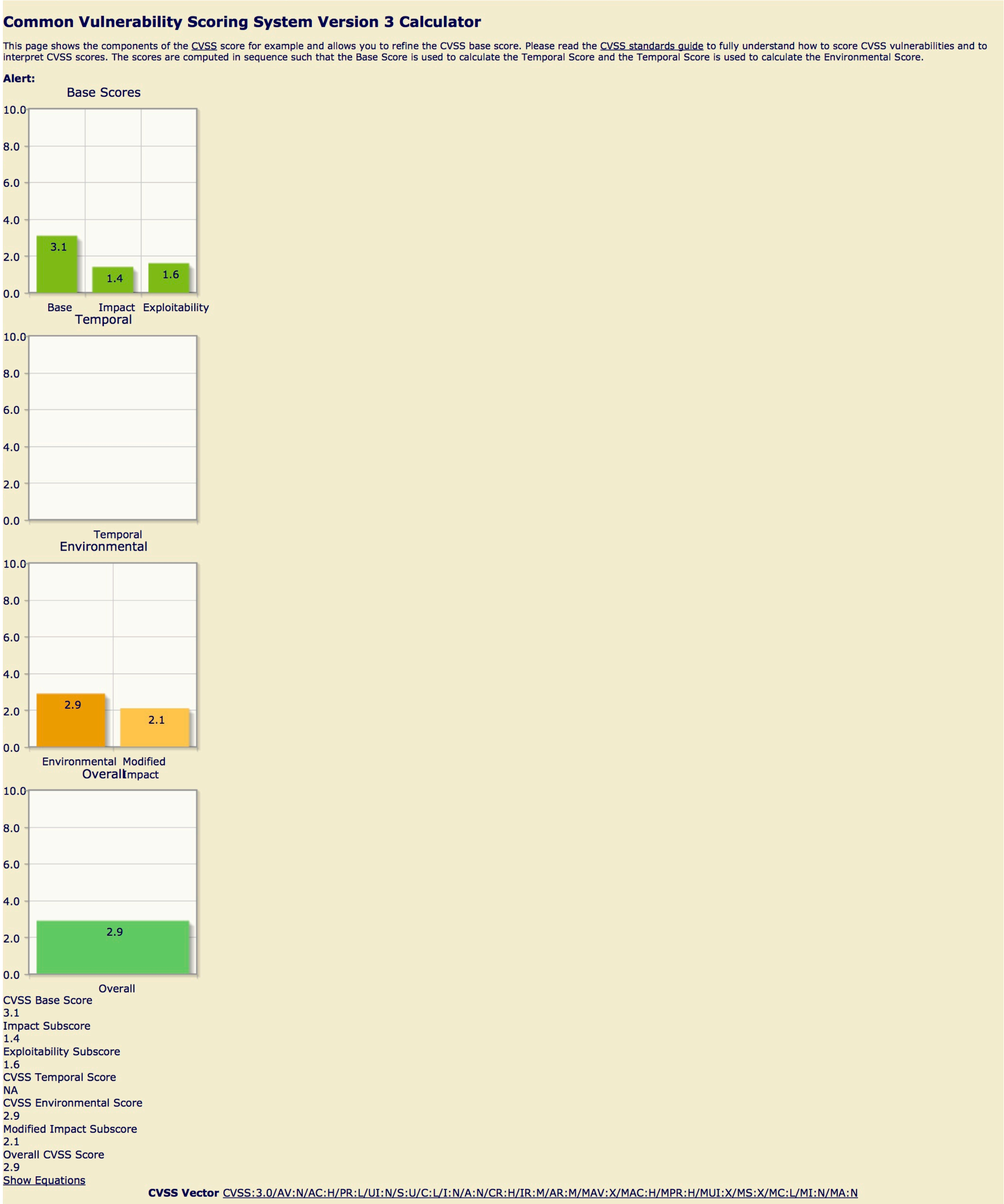
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 2 Secretary Machine

**Threat to Organization:** Ability to see all legal materials for Partner 2 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

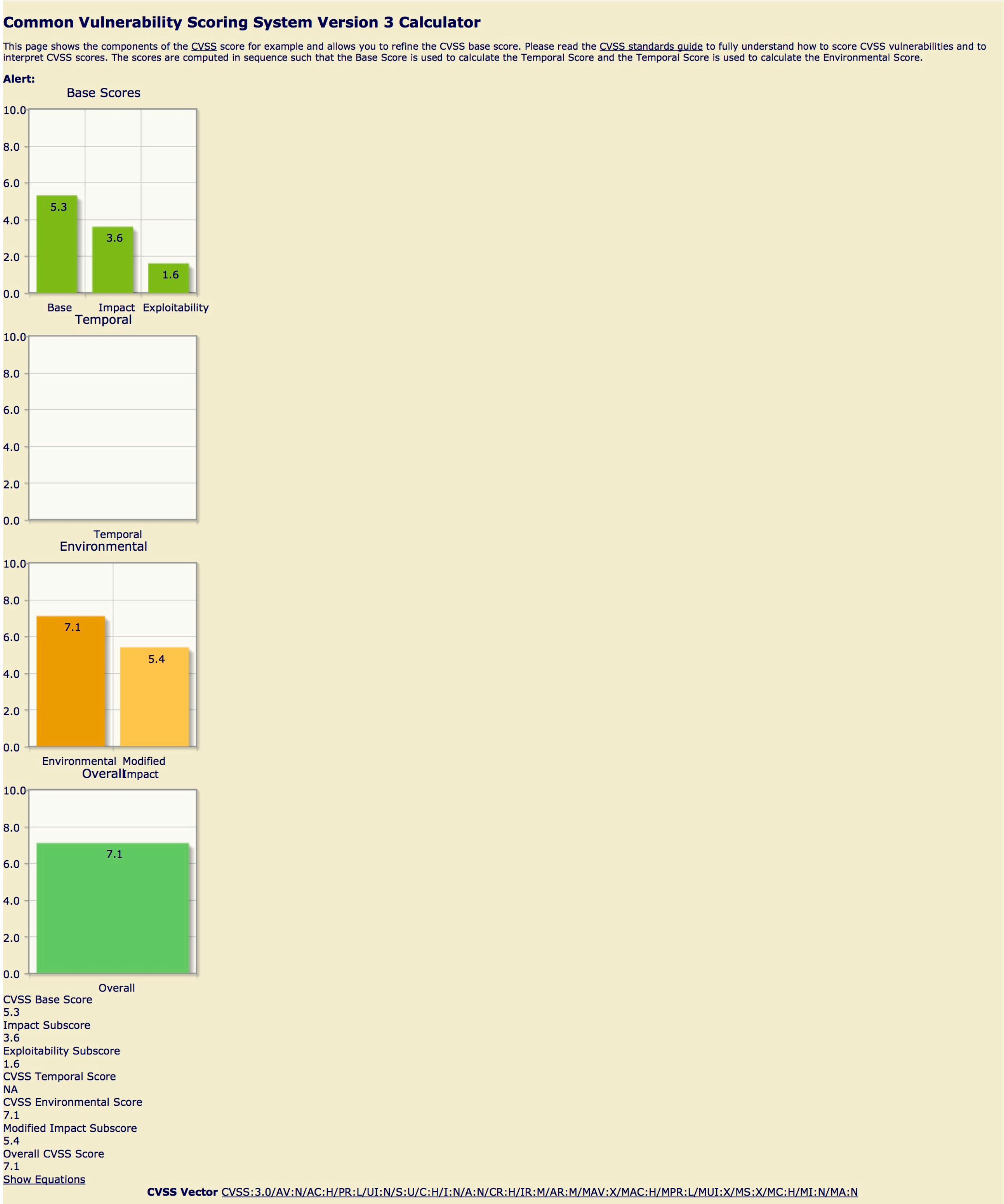
**Alert:**

CVSS Base Score
3.1
Impact Subscore
1.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
2.9
Modified Impact Subscore
2.1
Overall CVSS Score
2.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:H/MUI:X/MS:X/MC:L/MI:N/MA:N

## Compromise Item: Partner 2 Legal Aid Machine

**Threat to Organization:** Ability to see all legal materials for Partner 2 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

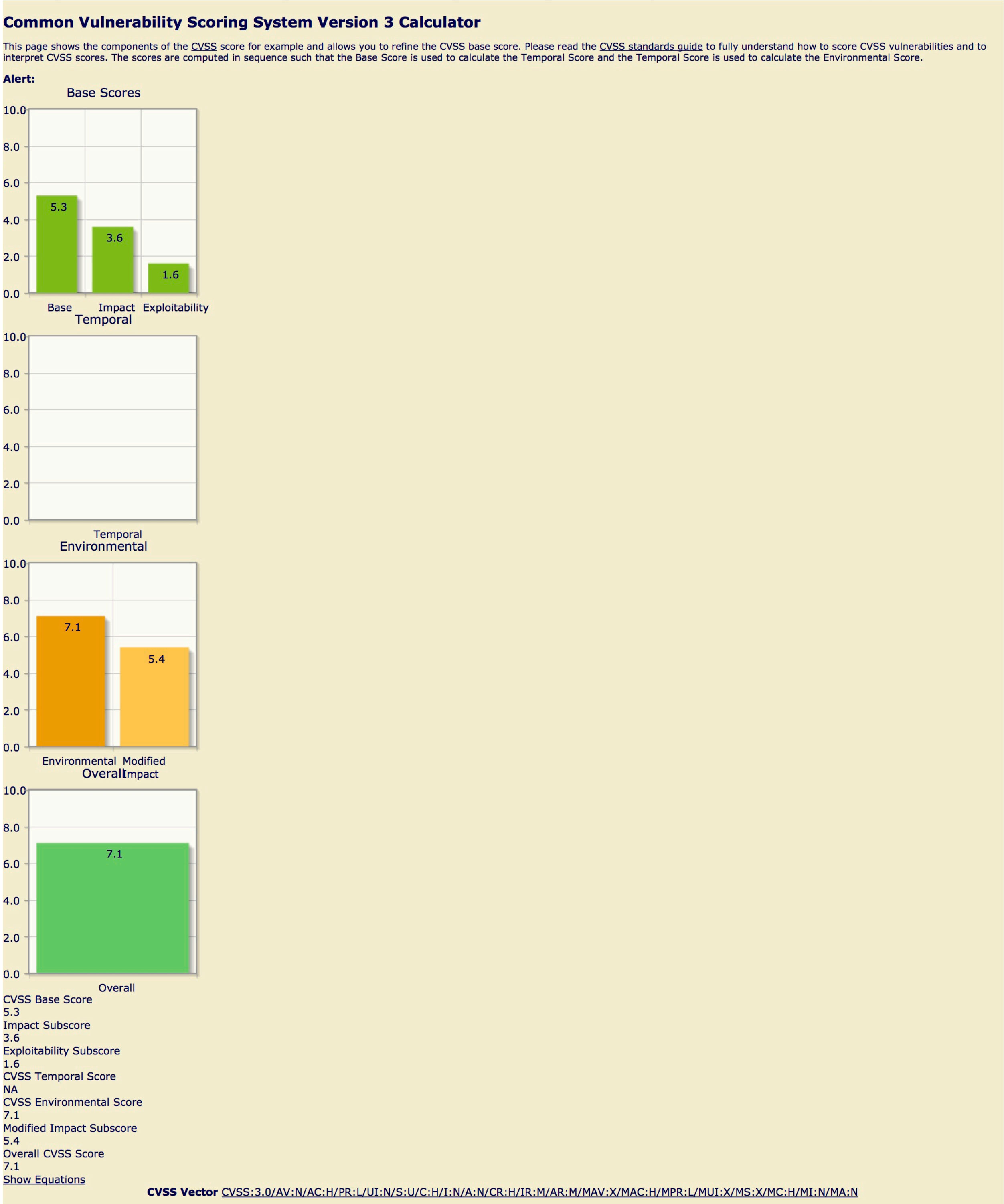
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 3 Machine

**Threat to Organization:** Ability to see all legal materials for Partner 3 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

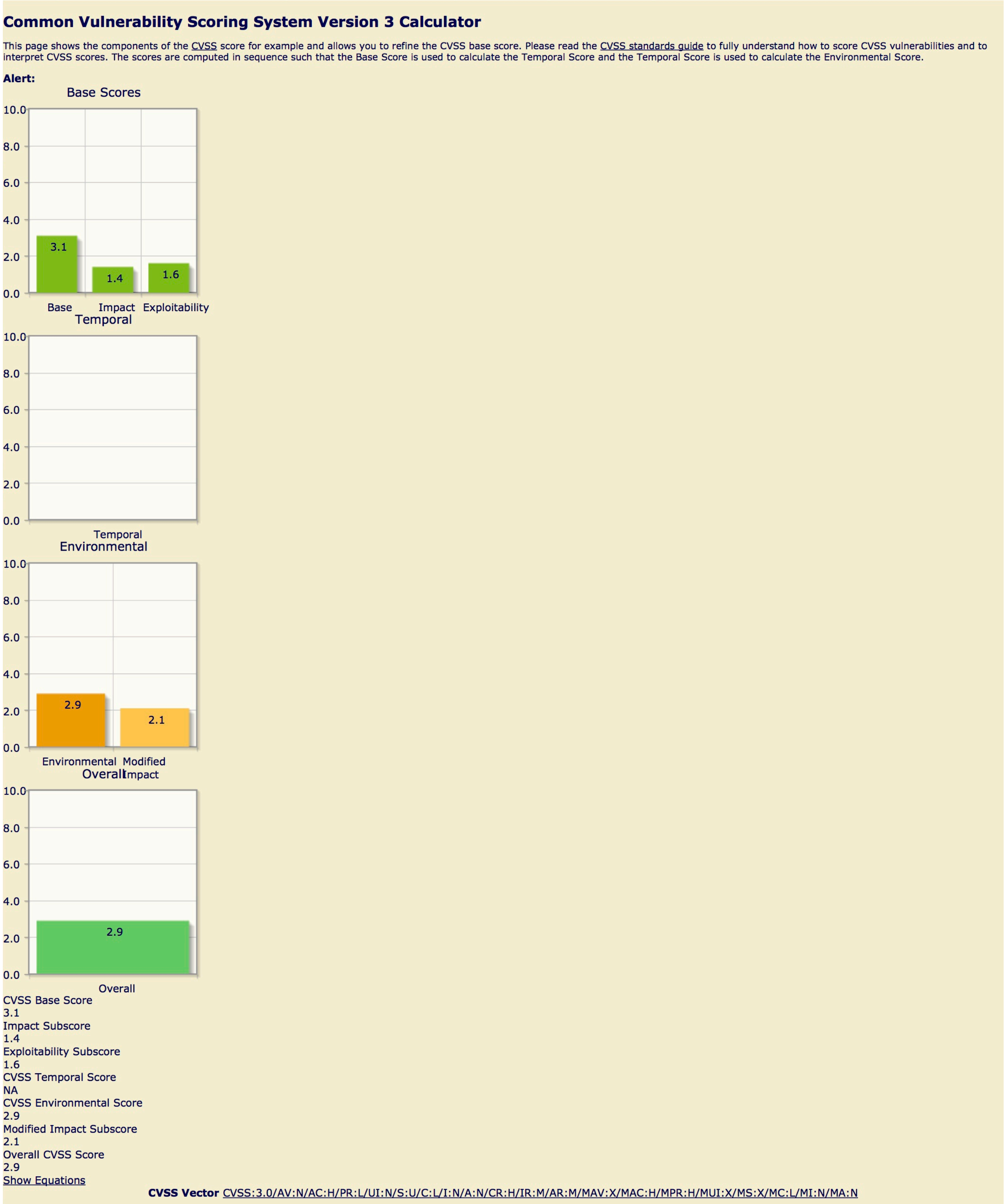
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Partner 3 Secretary Machine

**Threat to Organization:** Ability to see all legal materials for Partner 3 Team cases
**Indicator of Compromise:** ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

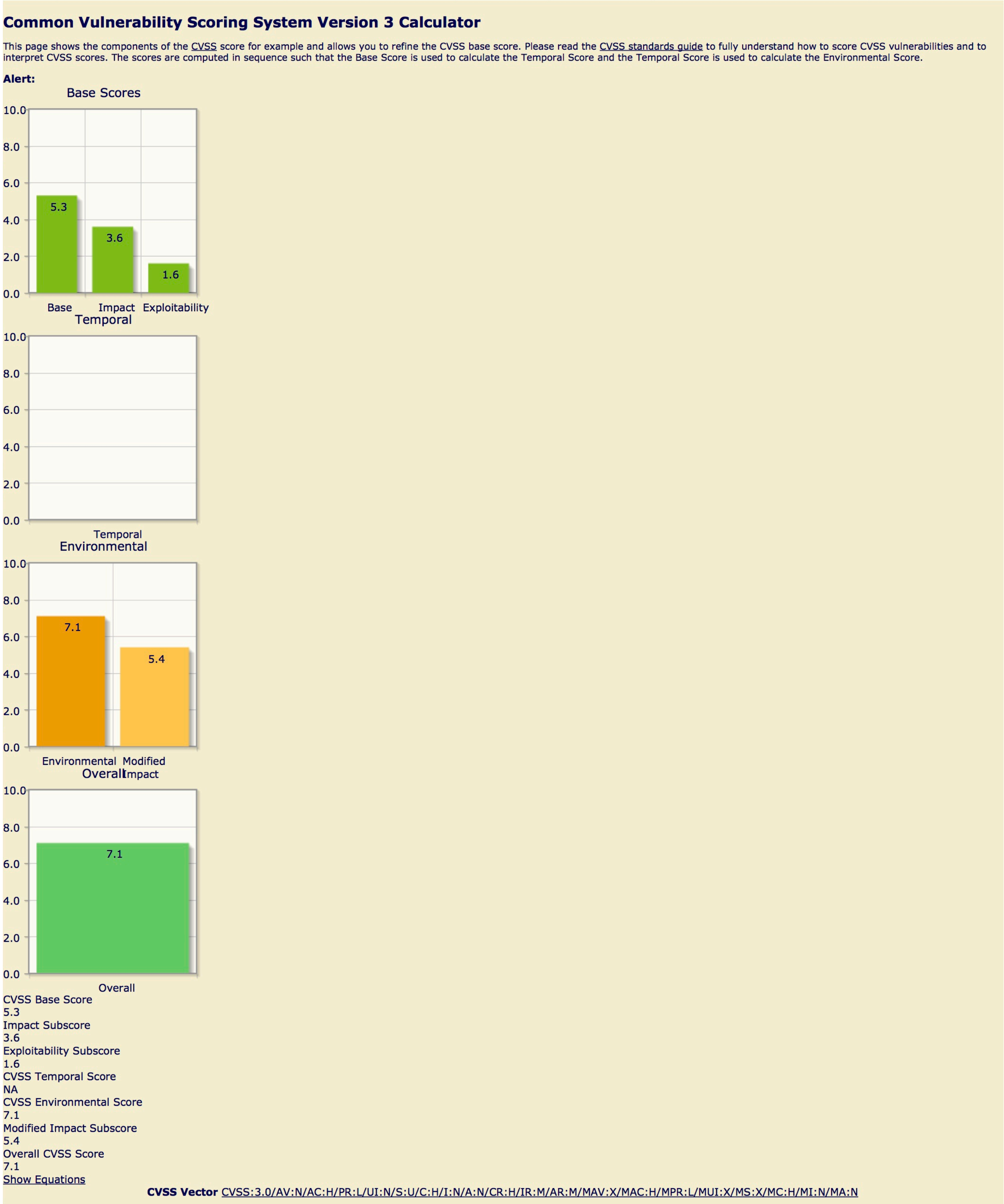
**Alert:**

CVSS Base Score
3.1
Impact Subscore
1.4
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
2.9
Modified Impact Subscore
2.1
Overall CVSS Score
2.9
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:H/MUI:X/MS:X/MC:L/MI:N/MA:N

## Compromise Item: Partner 3 Legal Aid Machine

**Threat to Organization:** Ability to see all legal materials for Partner 3 Team cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

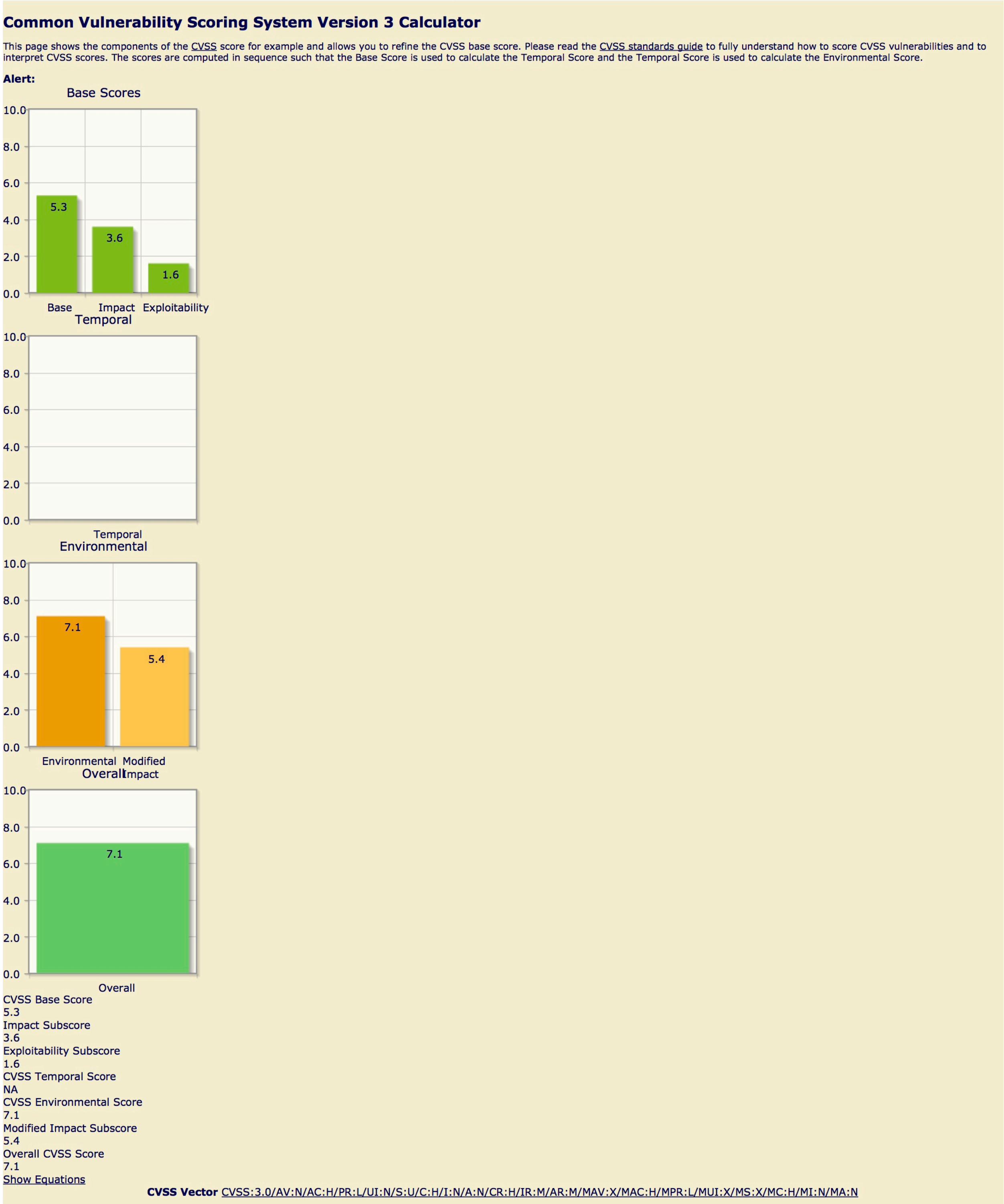
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Other Lawyer 1 Machine

**Threat to Organization:** Ability to see all legal materials for Other Lawyer 1 cases
**Indicator of Compromise:** ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

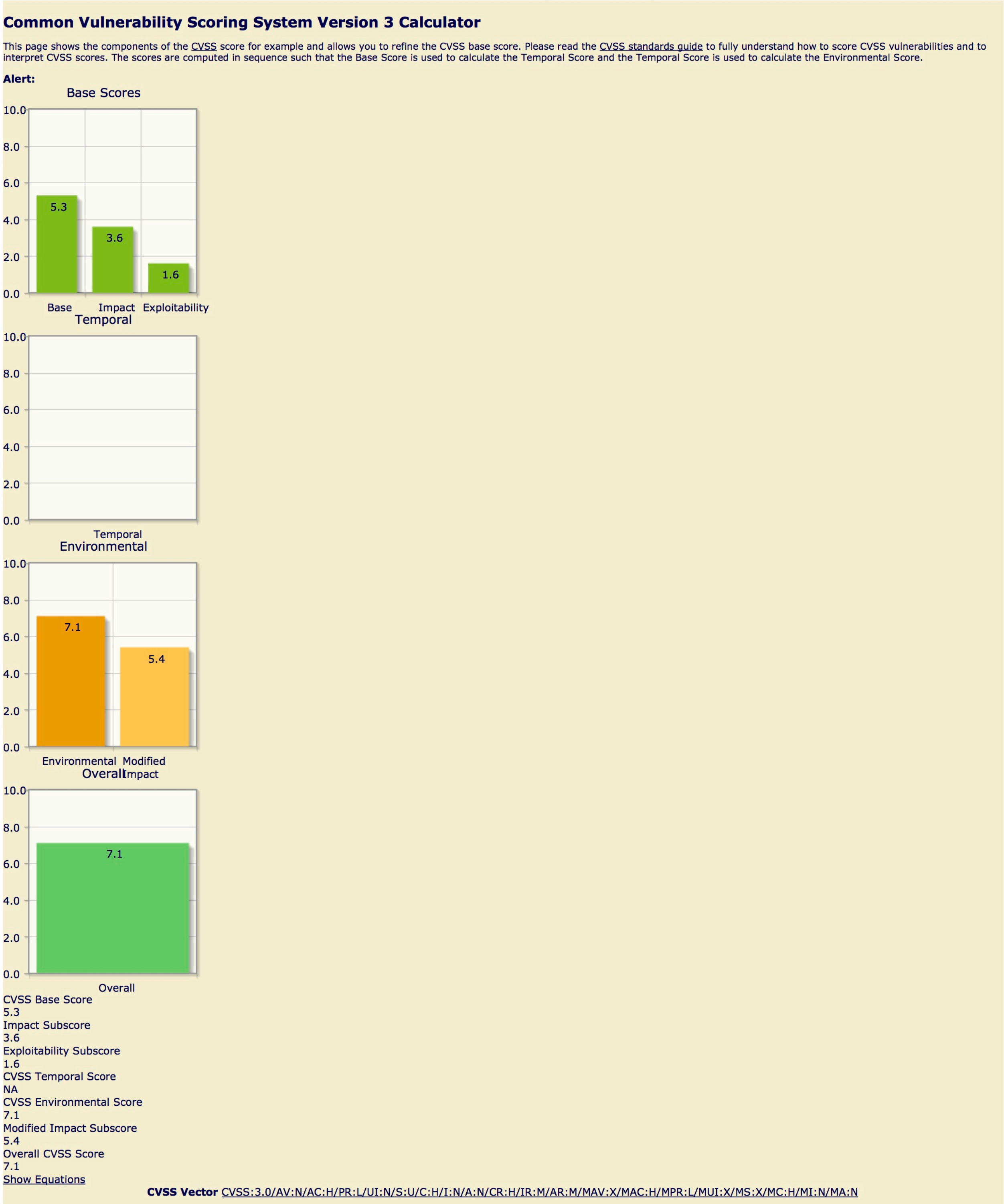
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Other Lawyer 2 Machine

**Threat to Organization:** Ability to see all legal materials for Other Lawyer 2 cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

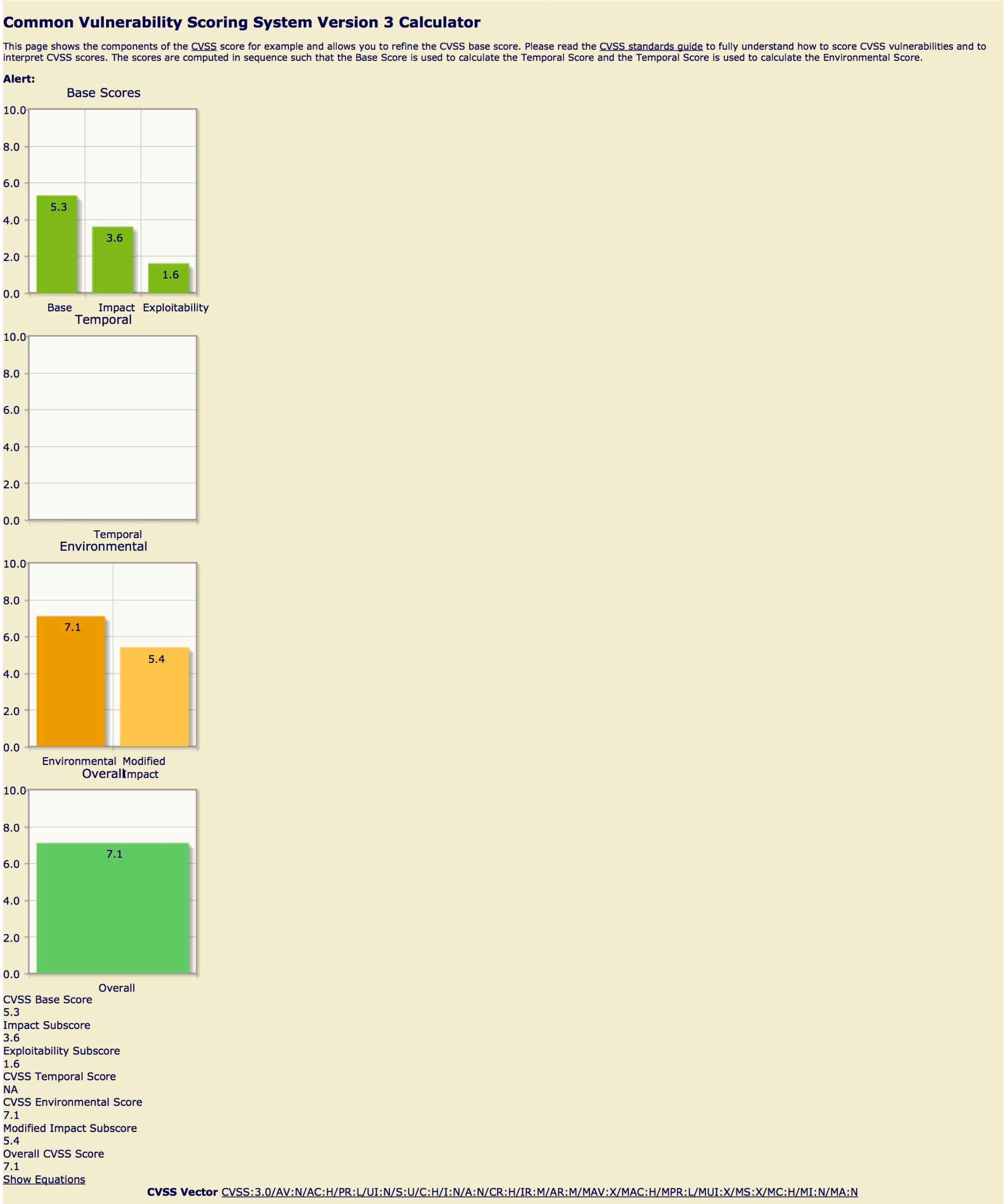
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Other Lawyer’s Legal Aid Machine

**Threat to Organization:** Ability to see all legal materials for Other Lawyer 1 &2 cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

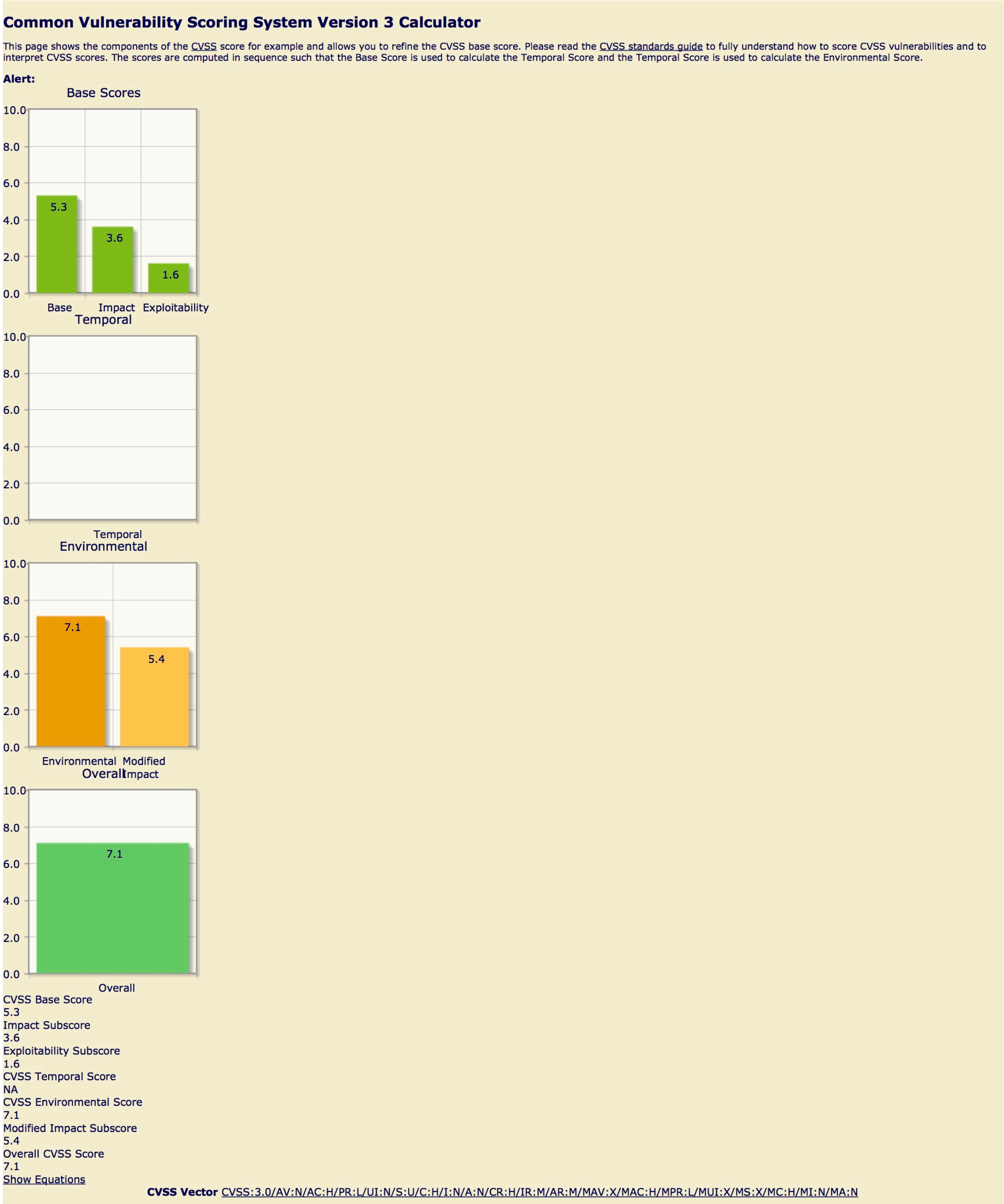
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Junior Partner Machine

**Threat to Organization:** Ability to see all legal materials for Junior Partner cases
**Indicator of Compromise:** ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

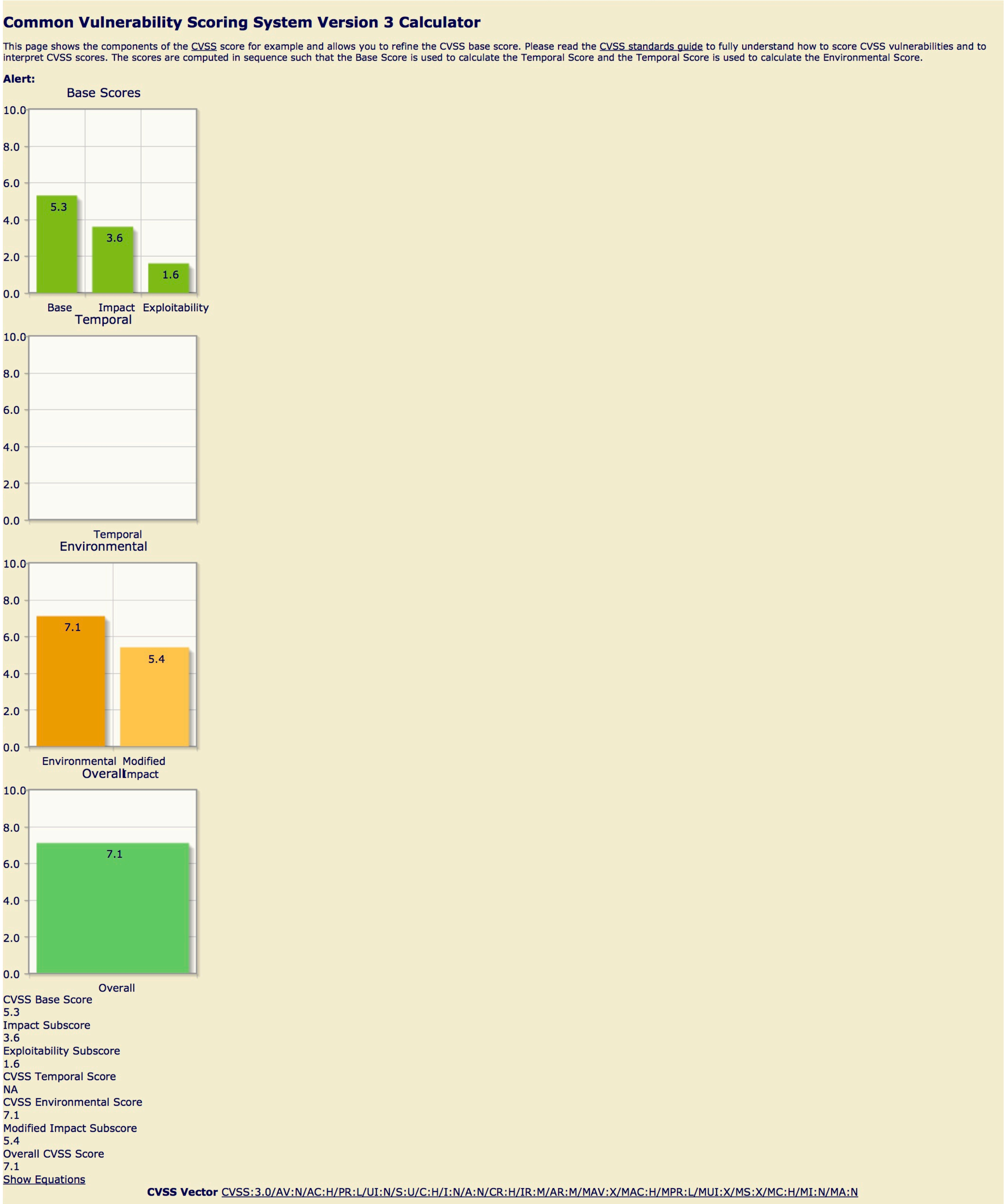
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Junior Partner Secretary Machine

**Threat to Organization:** Ability to see all legal materials for Junior Partner cases
**Indicator of Compromise:** ability to execute code



**Common Vulnerability Scoring System Version 3 Calculator**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

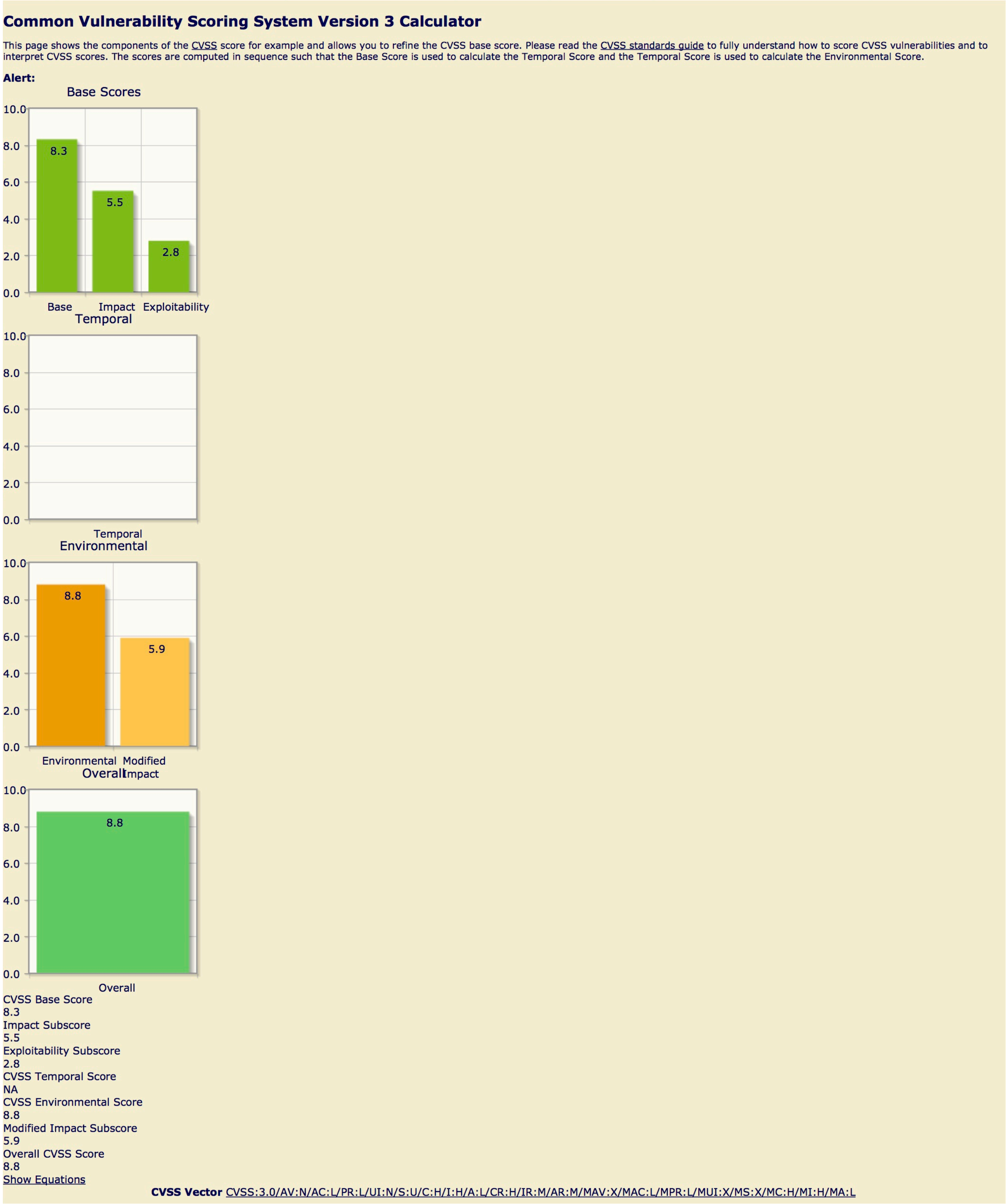
**Alert:**

CVSS Base Score
5.3
Impact Subscore
3.6
Exploitability Subscore
1.6
CVSS Temporal Score
NA
CVSS Environmental Score
7.1
Modified Impact Subscore
5.4
Overall CVSS Score
7.1
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:X/MAC:H/MPR:L/MUI:X/MS:X/MC:H/MI:N/MA:N

## Compromise Item: Open Case Files Server

**Threat to Organization:** Ability to see all legal materials all open cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

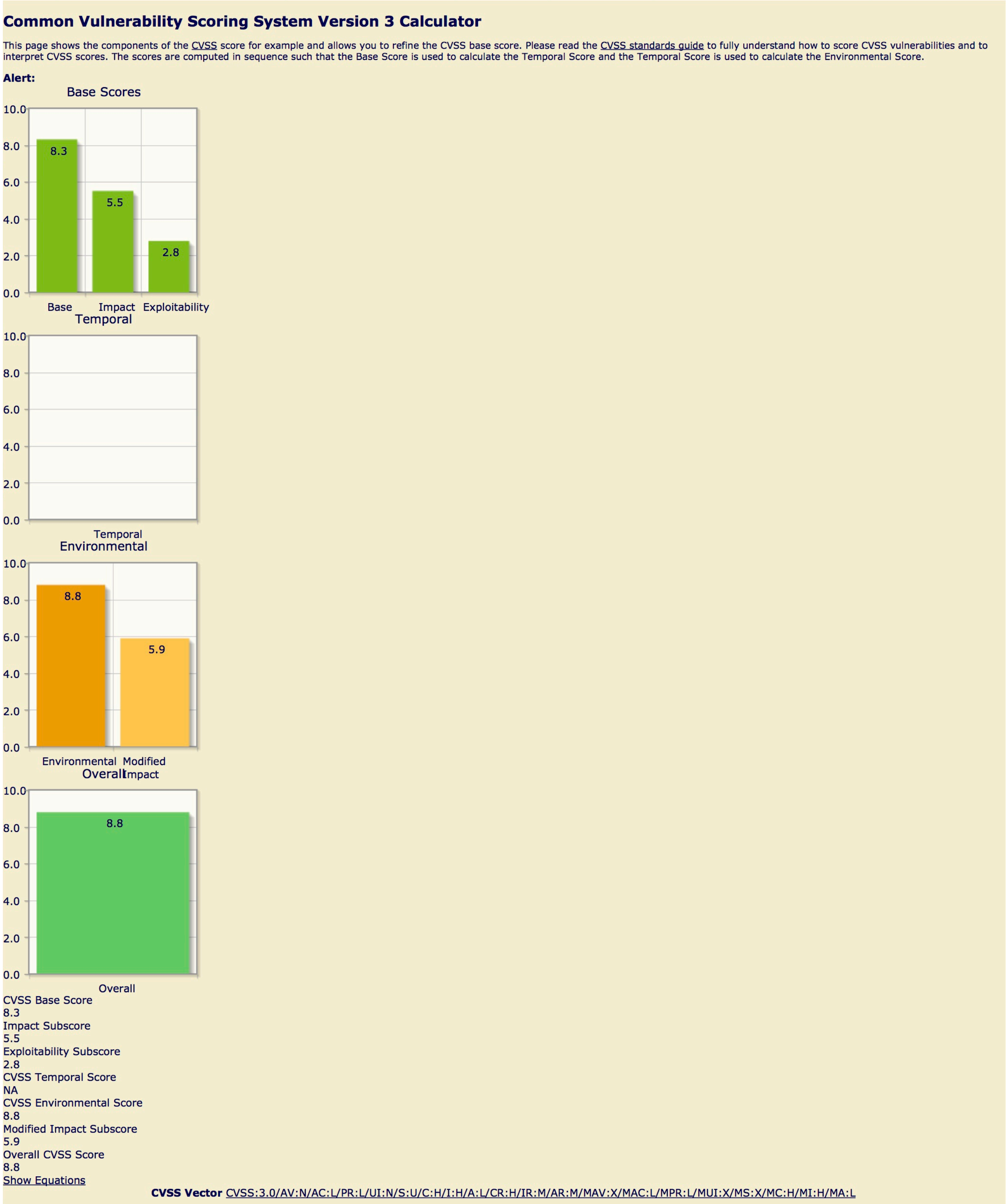
**Alert:**

CVSS Base Score
8.3
Impact Subscore
5.5
Exploitability Subscore
2.8
CVSS Temporal Score
NA
CVSS Environmental Score
8.8
Modified Impact Subscore
5.9
Overall CVSS Score
8.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L/CR:H/IR:M/AR:M/MAV:X/MAC:L/MPR:L/MUI:X/MS:X/MC:H/MI:H/MA:L

## Compromise Item: Closed Case Files Server

**Threat to Organization:** Ability to see all legal materials all open cases
**Indicator of Compromise:** ability to execute code



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

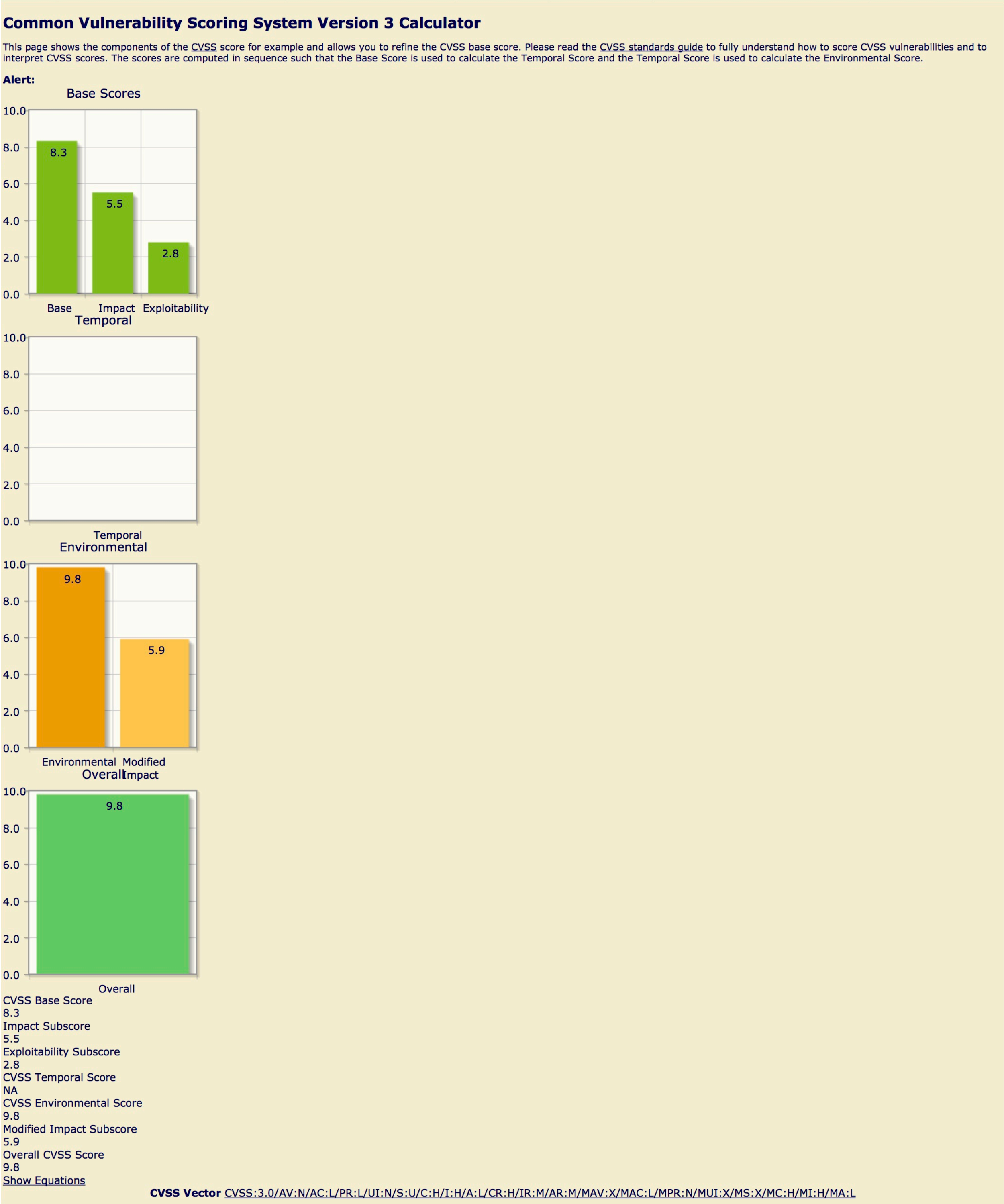
**Alert:**

CVSS Base Score
8.3
Impact Subscore
5.5
Exploitability Subscore
2.8
CVSS Temporal Score
NA
CVSS Environmental Score
8.8
Modified Impact Subscore
5.9
Overall CVSS Score
8.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L/CR:H/IR:M/AR:M/MAV:X/MAC:L/MPR:L/MUI:X/MS:X/MC:H/MI:H/MA:L

## Compromise Item: Case Files Back-Up Server

**Threat to Organization:** Ability to see all legal materials for all open and closed cases as well as stored privileged attorney client information considered lethal if compromised
**Indicator of Compromise:** ability to read case files



### Common Vulnerability Scoring System Version 3 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

**Alert:**

CVSS Base Score
8.3
Impact Subscore
5.5
Exploitability Subscore
2.8
CVSS Temporal Score
NA
CVSS Environmental Score
9.8
Modified Impact Subscore
5.9
Overall CVSS Score
9.8
Show Equations

**CVSS Vector** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L/CR:H/IR:M/AR:M/MAV:X/MAC:L/MPR:N/MUI:X/MS:X/MC:H/MI:H/MA:L

# Appendix C - Resumes

### Systems Administrator

EXPERIENCE SUMMARY:

Mr. Orange is a TS\\SCI with CI Poly cleared security professional with over 11 year's experience specialized in Offensive Computer Network Operations and Network Exploitation Analysis within the Intelligence Community and commercial environments

AREAS OF EXPERTISE:

- Linux / Unix
- TCP/IP
- Offensive Security
- Cisco
- Network Security
- Burp Suite Pro
- Microsoft Windows
- Cobalt Strike
- Metasploit

PROFESSIONAL EXPERIENCE:

*Defense Point Security - Telework* *01/2016 - Present*
*Senior Penetration Tester and Project Manager*

Mr. Orange is the Senior Penetration Tester and Project Manager on the Adobe Digital Marketing Red Team conducting assessment and evaluation of focus areas specified by the customer. During these unique engagements Mr. Orange performs both external web application testing to gain initial access and advanced persistent internal assessment against Windows, Unix and infrastructure devices. Mr. Orange also led engagements against Icon Fitness entities where he was the senior technical leadership and project manager.

*Visionist, Inc. – Fort Meade, Maryland* *11/2014 - 01/2016*
*Network Exploitation Analyst*

Mr. Orange served as a Network Exploitation Analyst for Visionist, Inc., where he analyzed networks in order to identify, assess and exploit vulnerabilities. He worked with customers across the enterprise and intelligence community to drive operations and meet critical, time-sensitive requirements as well as developed techniques and tactics to increase efficiency and success level of operations. Successfully trained analysts and operators on use of those techniques and tactics.

*KEYW Corporation – Fort Meade, Maryland* *06/2013 – 11/2014*
*Course Designer and Lead Instructor*

Mr. Orange served as the Course Developer and Lead Instructor in support of KEYW Corporation. In this role he developed an eight week post graduate level advanced exploitation course. Additionally, Mr. Orange was also responsible for designing and maintaining the large virtualized Windows, Linux and networking device infrastructure used to facilitate the course. Mr. Orange also served as a computer and network exploitation subject matter expert where he aided in the development of a separate foundational computer network operations course.

*U.S.M.C. – Fort Meade, Maryland* *11/2014 – 04/2010*
*Interactive Operator / Technical Director*

Mr. Orange conducted CNE Operations in order to fulfill national level requirements in support of foreign intelligence efforts. Mr. Orange analyzed networks to ascertain vulnerabilities and provide risk management for operations as well as planning and conducting testing of CNE tools. As technical lead Mr. Orange was responsible for training and certifying new operators as well as guiding their technical development. Mr. Orange also used this experience and knowledge to create and implement a training plan for the Marine Forces Cyber Command as part of the stand-up of that unit under U.S Cyber Command

*U.S.M.C. – Camp Leatherneck, Afghanistan* *04/2009 – 04/2010*
*Secure Communications Subject Matter Expert*

Mr. Orange served as the Secure Communications Subject Matter Expert in support of the United States Marine Corps and Camp Leatherneck. In this role, he was responsible for designing and implementing operating procedure, physical security and access standards for the Marine Air Group secure compound. He provided network and physical security expertise to the Senior Staff and Intelligence sections as well as guidance to subordinate security elements of the Air Group on matters of physical security, information storage and information redundancy. Finally, he designed and assisted in the construction of Temporary SCIF for the Air Group as well as providing expertise on handling and implementation of TS\\SI Satellite Communications.

*U.S.M.C. – MCAS Cherry Point, NC* *07/2006 – 04/2009*
*Special Intelligence Communicator*

Mr. Orange served as the Special Intelligence Communicator where he led a six person Secure Communications Team responsible for the administration and maintenance of the JWICS TS\\SI network. After a fire burned down the MCAS Cherry Point JWICS infrastructure, Mr. Orange was responsible for the plan of action and expedited handling of information recovery, new data preservation plans as well as the redesign and stand up of new infrastructure and secure facility.

EDUCATION AND TRAINING:

Dr.Sc., Information Technology, Towson University, Currently in Dissertation

M.S., Technology with a focus on Offensive Security, Eastern Michigan University, 2014

Journeyman Interactive Operator Certification, 2013

B.S., Information Technology Management, American Military University, 2012

Advanced Interactive Operator Training and Certification, 2011

Interactive Operator Training and Certification, 2010

Intermediate Network Analysis course, 2009

Basic Digital Network Analysis course, 2008

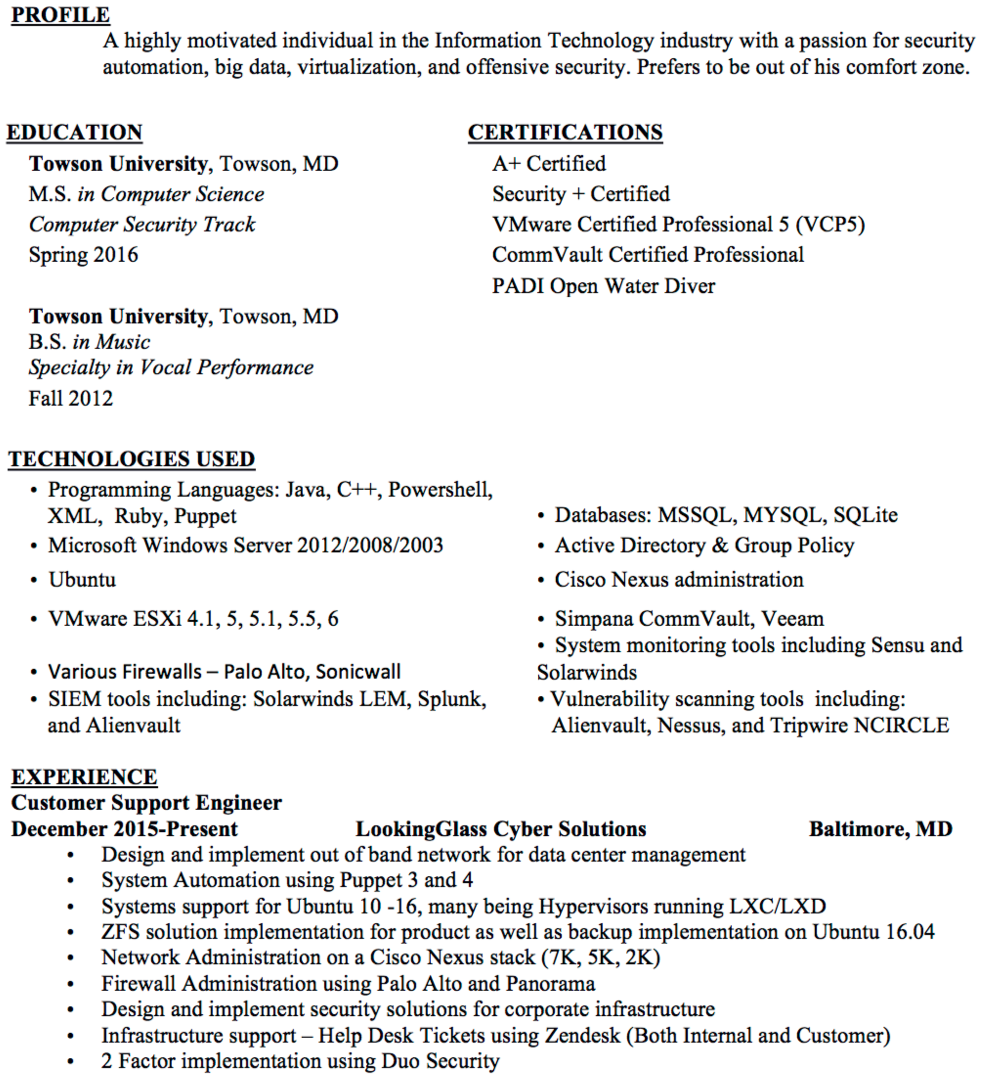
Special Intelligence Communications Course, 2006

CERTIFICATIONS:

CISSP, Original Certification 2012 and still current

CISSP - Certified Information Systems Security Professional Oct. 2012 - Present

## Systems Administration Auditor



**PROFILE**

A highly motivated individual in the Information Technology industry with a passion for security automation, big data, virtualization, and offensive security. Prefers to be out of his comfort zone.

**EDUCATION**

**Towson University**, Towson, MD
M.S. *in Computer Science*
*Computer Security Track*
Spring 2016

**Towson University**, Towson, MD
B.S. *in Music*
*Specialty in Vocal Performance*
Fall 2012

**CERTIFICATIONS**

A+ Certified
Security + Certified
VMware Certified Professional 5 (VCP5)
CommVault Certified Professional
PADI Open Water Diver

**TECHNOLOGIES USED**

- Programming Languages: Java, C++, Powershell, XML, Ruby, Puppet
- Microsoft Windows Server 2012/2008/2003
- Ubuntu
- VMware ESXi 4.1, 5, 5.1, 5.5, 6
- Various Firewalls – Palo Alto, Sonicwall
- SIEM tools including: Solarwinds LEM, Splunk, and Alienvault
- Databases: MSSQL, MYSQL, SQLite
- Active Directory & Group Policy
- Cisco Nexus administration
- Simpana CommVault, Veeam
- System monitoring tools including Sensu and Solarwinds
- Vulnerability scanning tools including: Alienvault, Nessus, and Tripwire NCIRCLE

**EXPERIENCE**

**Customer Support Engineer**
**December 2015-Present** **LookingGlass Cyber Solutions** **Baltimore, MD**

- Design and implement out of band network for data center management
- System Automation using Puppet 3 and 4
- Systems support for Ubuntu 10 -16, many being Hypervisors running LXC/LXD
- ZFS solution implementation for product as well as backup implementation on Ubuntu 16.04
- Network Administration on a Cisco Nexus stack (7K, 5K, 2K)
- Firewall Administration using Palo Alto and Panorama
- Design and implement security solutions for corporate infrastructure
- Infrastructure support – Help Desk Tickets using Zendesk (Both Internal and Customer)
- 2 Factor implementation using Duo Security

**Systems Security Engineer**
**April 2015-December 2015 Skyline Technology Solutions Glen Burnie, MD**

- Systems Security Architect for projects with the State of Maryland.
- Systems and Security audits for state agencies as well as commercial customers
- Design, Implement, and maintain Splunk for State of Maryland Security Operations Center. This included on-boarding new customers, adding devices, creating rules/searches/reports. Main source of log information is from Palo Alto with various other sources.
- Assist in on-boarding state agencies to Security as a Service platform.
- Review Vulnerability Management logs and provide recommendations and implement fixes
- Develop mitigation strategies and implementation plans for known vulnerabilities

**Security Engineer**
**October 2014-April 2015 G2 Inc. Annapolis-Junction, MD**

- Develop and implement bug fixes and feature enhancements in software applications using Java, XML, XSLT, and Schematron
- Automate processes using Python and Powershell
- Analyze and implement Security Requirements as instructed by customer
- Produce CCE mapping for all USGCB CCE's to NIST 800-53
- Create baseline CCSS scores for all CCE's for Windows 7, 8, Server 2012R2, and RHEL 6.
- Validate USGCB configuration baselines for Server 2012 R2

**Systems Engineer**
**February 2014-October 2014 Skyline Technology Solutions Glen Burnie, MD**

- Maintain Servers and Applications (version upgrades, backups, performance, up-time)
- Maintain SAN storage environment
- Maintain VMware environment
- Manage projects to maintain, upgrade, and introduce new systems into the environment
- Support cloud hosted managed services clients
- Test proprietary appliances for vulnerabilities and remediate if/when found
- Work with Network Security team to move toward a DoD compliant infrastructure

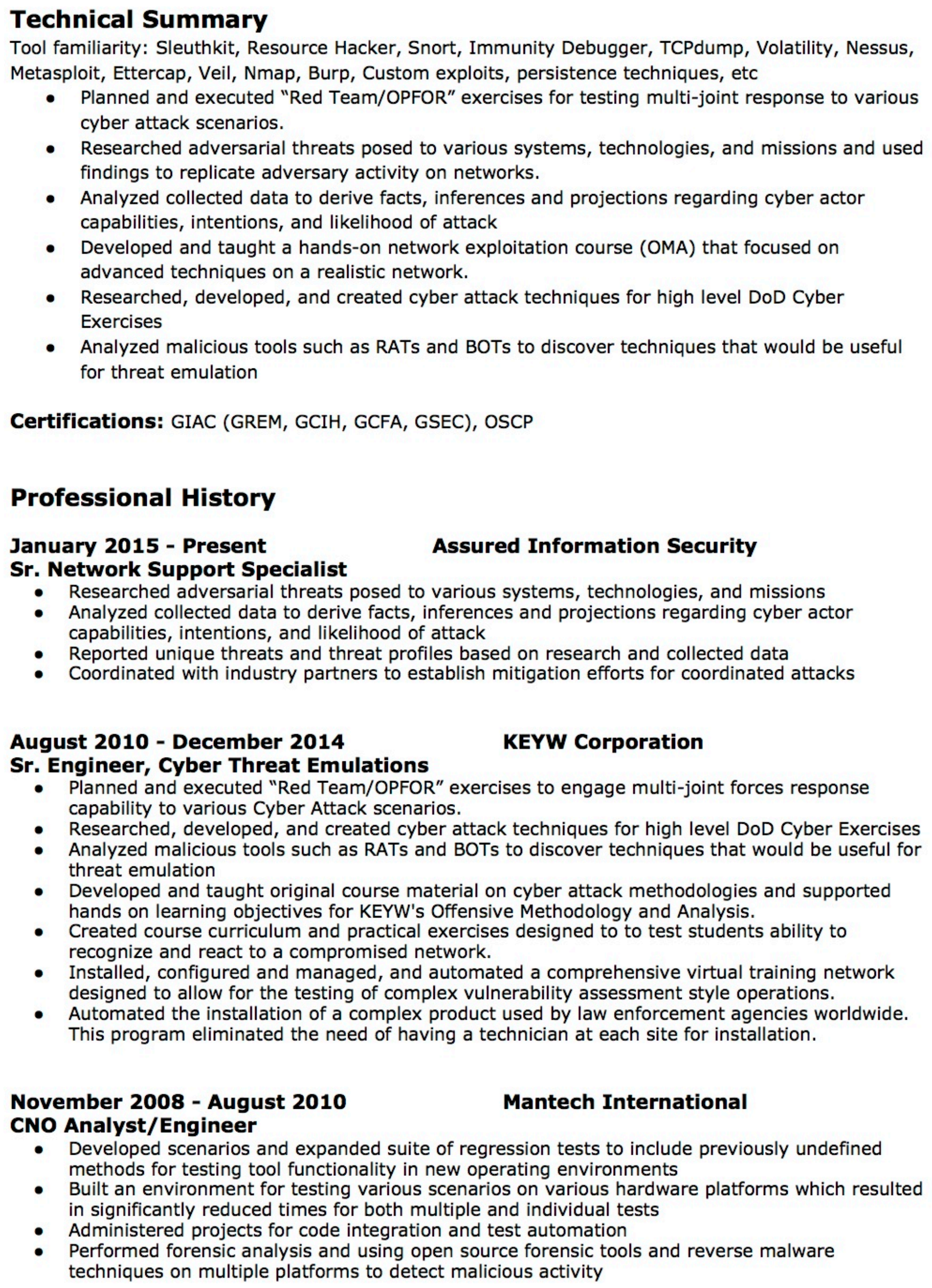
**Security Analyst**
**May 2013-February 2014 Edaptive Systems Owings Mills, MD**

- Review Security logs (SIEM tool) and provide recommendations and implement fixes if possible
- Review Vulnerability scans and mitigate any risks found
- Proactively manage and monitor facilities to include all physical and environmental security controls
- Complete periodic reviews of Security controls and processes as outlined
- Perform and maintain risk analysis on all new or existing systems

**Systems Administrator**
**June 2012-February 2014 Edaptive Systems Owings Mills, MD**

- Managed Project Server 2007 on Microsoft Office Sharepoint Services 3.0
- Managed and provided support for Exchange Server 2010 and Active Directory
- Provided Tier 3 Help Desk support for a company of 300 employees
- Managed over 100 virtual machines with hosts running ESXi 5.1 and ESXi 4.0
- Created and managed server backups using Symantec Backup Exec, Veeam, and Acronis
- Managed and maintained a FIPS compliant Datacenter using tools such as NCIRCLE and Solarwinds.
- Managed and implemented networking and Firewall equipment consisting of Dell Powerconnect, Sonicwall, Fortigate, and Watchguard solutions.

## Red Teamer



### Technical Summary

Tool familiarity: Sleuthkit, Resource Hacker, Snort, Immunity Debugger, TCPdump, Volatility, Nessus, Metasploit, Ettercap, Veil, Nmap, Burp, Custom exploits, persistence techniques, etc

- Planned and executed "Red Team/OPFOR" exercises for testing multi-joint response to various cyber attack scenarios.
- Researched adversarial threats posed to various systems, technologies, and missions and used findings to replicate adversary activity on networks.
- Analyzed collected data to derive facts, inferences and projections regarding cyber actor capabilities, intentions, and likelihood of attack
- Developed and taught a hands-on network exploitation course (OMA) that focused on advanced techniques on a realistic network.
- Researched, developed, and created cyber attack techniques for high level DoD Cyber Exercises
- Analyzed malicious tools such as RATs and BOTs to discover techniques that would be useful for threat emulation

**Certifications:** GIAC (GREM, GCIH, GCFA, GSEC), OSCP

### Professional History

**January 2015 - Present** **Assured Information Security**
**Sr. Network Support Specialist**

- Researched adversarial threats posed to various systems, technologies, and missions
- Analyzed collected data to derive facts, inferences and projections regarding cyber actor capabilities, intentions, and likelihood of attack
- Reported unique threats and threat profiles based on research and collected data
- Coordinated with industry partners to establish mitigation efforts for coordinated attacks

**August 2010 - December 2014** **KEYW Corporation**
**Sr. Engineer, Cyber Threat Emulations**

- Planned and executed "Red Team/OPFOR" exercises to engage multi-joint forces response capability to various Cyber Attack scenarios.
- Researched, developed, and created cyber attack techniques for high level DoD Cyber Exercises
- Analyzed malicious tools such as RATs and BOTs to discover techniques that would be useful for threat emulation
- Developed and taught original course material on cyber attack methodologies and supported hands on learning objectives for KEYW's Offensive Methodology and Analysis.
- Created course curriculum and practical exercises designed to to test students ability to recognize and react to a compromised network.
- Installed, configured and managed, and automated a comprehensive virtual training network designed to allow for the testing of complex vulnerability assessment style operations.
- Automated the installation of a complex product used by law enforcement agencies worldwide. This program eliminated the need of having a technician at each site for installation.

**November 2008 - August 2010** **Mantech International**
**CNO Analyst/Engineer**

- Developed scenarios and expanded suite of regression tests to include previously undefined methods for testing tool functionality in new operating environments
- Built an environment for testing various scenarios on various hardware platforms which resulted in significantly reduced times for both multiple and individual tests
- Administered projects for code integration and test automation
- Performed forensic analysis and using open source forensic tools and reverse malware techniques on multiple platforms to detect malicious activity

**October 2005 - November 2008 Windermere/Essex/Northrop Grumman/KEYW**
**Security Analyst/Lab Manager**

- Led a remote installation team that installed and configured an end-to-end training network consisting of ESX servers, Cisco routers and switches, storage arrays, and computer workstations
- Designed and implemented an automation program to manage backing up and restoring various aspects of the virtual network. This program provided a dramatic increase in production and was essential for timely lab operations for both the manager and the users
- Set up and maintained multiple virtual networks and machines for testing and evaluation of new software and techniques. These networks ranged from simple, flat networks to secure and hardened networks to monitor and prevent malicious activity.
- Tested custom and open source tools against the virtual hardened network

**August 2004 - October 2005 Computer Sciences Corporation (CSC) Eagle Alliance**
**Professional Security Advisor - Part Time (NISIRT)**

- Provided specialized Information System Security support integral to the Client's mission through analysis activities, incident response, and Information System Security Office services
- Responsible for security assurance of NSA networks and information systems as a member of the NSA/CSS Information Systems Incident Response Team (NISIRT)
- Routinely used TCPDump, Cisco IDS, and other tools to monitor the customer network and provide feedback and reporting on malicious activity and fraud waste and abuse cases

**February 1998- June 2005 U. S. Army**
**Signals Intelligence (SIGINT) Analyst / Information Warfare (IW) Specialist**

- Conducted Operations meant to deny, disrupt, or degrade enemy communications in support of DoD combat operations.
- Analyzed computers and networks for vulnerabilities to determine weaknesses in them and subsequently exploit them for access during penetration testing in a "Red Team" environment.
- Conducted vulnerability/external penetration testing and intrusion detection monitoring to prevent future penetrations of U.S. military systems.
- Worked numerous Sensitive Reconnaissance operations (SRO) missions as a SIGINT analyst and was instrumental in resolving mission manning problems that enabled the Advanced Quick look (AQL) Electronic Intelligence mission to effectively provide direct intelligence support.
- Provided near real time Signals Intelligence Analysis necessary for support of several field readiness exercises.

**Technical Training and Education (abbreviated)**

SANS Computer Forensics, Investigation, and Response. (GCFA)
SANS Hacker Techniques, Exploits and Incident Handling. (GCIH)
SANS Reverse Engineering Malware. (GREM)
SANS Security Essentials (GSEC)
Offensive Security Pentesting with Backtrack
Offensive Security Cracking the Perimeter (OSCE)
Digital Network Exploitation and Mapping course at Naval Center for Cryptology, Corry Station

**Tactical Training and Experience:** Available upon request

**Red Team Auditor**

## Summary

A highly accomplished Security Professional with thirteen years of experience in multiple information technology domains, specializing in computer network exploitation, computer network defense, and security incident response. Frequently called upon to develop tactics and techniques to exploit network vulnerabilities, defend vulnerable networks, and conduct formal and informal training sessions for a wide variety of personnel.

## Professional Experience

Mentor and Instructor – NodeSC, Charleston, SC September 2015 – present

Created curriculum and lead instructors for the Cyber Core Curriculum program, focused on educating teenage students on information technology and cybersecurity fundamentals.

Mentor for local magnet high school student conducting year-long thesis research in the cybersecurity field

Created challenges for and moderated "capture the flag" event, providing teams of local middle and high school students an opportunity to test their cybersecurity skills against other teams from the region.

President of Consulting Services – Soteria, LLC, Charleston, SC July 2016 – present

Develop and maintain positive client relationships through the delivery of contracted services

Build a team of highly qualified security experts through extensive recruiting, interviewing, and training processes

Senior Security Consultant – Soteria, LLC, Charleston, SC September 2015 – July 2016

Developed customized forensics tools to assist analysts in detecting malicious software and activity on client networks

Conducted comprehensive security audits for clients in multiple industries.  Created plans to remediate vulnerabilities and security shortcomings without exceeding budget constraints

Vice President - Active Network Defense Lead – JP Morgan Chase and Co., Columbia, MD March 2015 – August 2015

Recruited as initial member of the active network defense team, tasked with building an organization dedicated to pursuing advanced persistent threats targeting JPMC.

Developed techniques and tools to analyze systems for evidence of advanced cyber threats

Worked with multiple organizations within the firm to gather data and automate analysis

Network Exploitation Analyst – Visionist, Inc., Ft. Meade, MD June 2013 – March 2015

Analyzed networks in order to identify and assess vulnerabilities

Worked with customers across the enterprise and intelligence community to drive operations and meet critical, time-sensitive requirements

Developed tools and scripts to increase the efficiency and automation level of operations. Successfully trained analysts and operators on the use of those tools

CNO Operator – USAF, Ft. Meade, MD January, 2011 – June 2013

Lead analysts and operators to successfully exploit targets of interest in order to fulfill national level requirements in support of foreign intelligence efforts

Analyzed source code of malware, CNE tools, and Non-CNE tools for troubleshooting, testing, and various other purposes

Relied on by senior level management to draft standard operating procedures and technical guidance for operators and analysts. Conducted regular formal and informal training sessions to ensure standards were maintained by all personnel

Provided post-mission written analysis and oral briefs to both peers and senior management

Conducted testing and development of CNE tools to ensure functionality and interoperability

Conducted CNE tool testing against multiple security products and vendors

Conducted Active Defense operations to identify and act on suspicious activities in the Air Force Network

Computer Security Incident Response Center Analyst – Internal Revenue Service (IRS), New Carrollton, MD January, 2012 – July 2013 (Part-time)

Responsible for identifying, researching, performing in-depth analysis, and reporting on various types of security incidents

De-obfuscated and analyzed suspicious network traffic to determine attack vectors being used by malicious websites

Enterprise Solutions Steering Group (ESSG) Build Team Lead – USAF, Lackland AFB, TX October, 2006 – April, 2009

Responsible for design, implementation, upgrades, equipment purchases, scheduling and overall operation of the Information Assurance (IA) test range used to support the ESSG and other DoD efforts

Performed testing on multiple Computer Network Defense tools resulting in enterprise-wide contract awards

Counter – Improvised Explosive Device (IED) Database Manager/Administrator – USAF, Kabul, Afghanistan September, 2007 – March, 2008

Developed and maintained database used to track all IED events in the Afghanistan

Developed solution to make data readily available to analysts across five Regional Commands while avoiding budget increases

Developed system to track IED reporting processes, making it possible to identify and address weaknesses in the reporting chain

Automated Security Incident Management System Support Team Project Manager – USAF, Lackland AFB, TX
March, 2008 – April, 2009

Led team of four technicians to configure, deploy, troubleshoot, and maintain intrusion detection systems on Air Force bases world-wide. Coordinated efforts between organizations to ensure infrastructure changes occurred with minimal impact to ongoing operations.

## Education

M.S., Technical Studies, Focus on Offensive Computer Security, Eastern Michigan University (2016)

B.S., Computer Science, University of Maryland University College (2013)

A.A.S., Cyber Security, Community College of the Air Force (2013)

A.A.S., Communications Technology, Community College of the Air Force (2005)

## Certifications

GIAC Reverse Engineering Malware (GREM) (2014)

Certified Information Systems Security Professional (CISSP) (2011)

Interactive Operator Certification (2010)

CompTIA Security+ (2010)

**CAPTR Teamer**

MSns, GSE, CISSP, GCIA, GCFA, GSNA, GSWN, GSEC

Education / Certifications

- Masters in Network Security from Capitol College. GPA 4.0.
- BA in Psychology from Shippensburg University. Graduated Magna Cum Laude.
- Information Security Certifications include: GSE, CISSP, GSEC, GCIA, GSNA, GCFA, GCWN, and GCIH. Also certified MCITP:EA for Windows 2008.

Professional Experience

Network Operator

Department of Defense

May 2013 to Present

Conduct CNE operations in order to fulfill critical national level requirements in support of foreign intelligence collection efforts. Analyze networks in order to identify and assess vulnerabilities to enable and conduct CNE operations. Provide post-mission written analysis and oral briefs to both peers and management. Conduct testing and development of CNE tools to ensure functionality and interoperability. Draft Standard Operating Procedures and tool usage guidance for CNE tools. Conduct CNE tool testing against numerous products. Analyze malware, CNE tools and non-CNE tools for troubleshooting, testing and documentation.

Adjunct Instructor

Stevenson University

June 2006 to Current

Courses taught at undergraduate and graduate level including: computer networking, information security and Microsoft Windows. Developed a Windows 2003 Enterprise Security course at the graduate level, and then later redeveloped for Windows 2008. Also carry a reputation for successfully taking over courses in emergency situations.

Security Architect

Campbell & Company, Inc.

January 2004 to May 2013

Managed corporate security projects including: deploying and managing enterprise antivirus, Intrusion Prevention Systems (IPS), proxy and transparent firewalls, VPN and SSL VPN access. Other roles included security incident handling, risk assessments, secure network and systems design, vulnerability scans, etc. Identified and briefed senior management on new information security threats as they arose.

Championed and led the enterprise virtualization effort. The virtualization project resulted in significantly reduced down time, streamlined administration, reduced hardware requirements and greatly improved recovery times. The resulting consolidation of several hundred workstations and servers produced a savings of nearly one million dollars over four years.

Acted as a 3rd tier support through researching and identifying solutions to complex server and networking problems.

Adjunct Professor

Harrisburg Area Community College

January 2003 to May 2004

Courses taught include computer networking and computer security. Performed significant work on developing an Information Security associate's degree program for the college. Also created a course centered on the Security+ certification program.

Sr. Network Analyst

Planetcable / Provion

June 1998 to December 2003

Consulted as the Sr. Network Administrator for a 1500-node hospital network across 7 remote sites. Duties encompassed proposing new projects, maintaining servers (Windows, Novell, AIX, and Red Hat), and managing the network infrastructure. Projects involved proposing and deploying an enterprise disaster prevention solution utilizing a combination of tape backup, UPS power, off-site storage, and fault tolerant servers. Managed client network perimeter security and VPN connectivity using Checkpoint firewalls.  Performed client security audits, combining reviews of policies, physical security, and disaster preparedness plans.

Other duties included maintaining the Internet backbone for a regional ISP, developing and implementing secure VPNs, conducting security audits, and managing core network routers. Coordinated projects with various clients to increase productivity and reduce costs.  Successful proposals included migration of a large student-loan processing data-center, which significantly reduced the client's hosting costs.

Supplementary responsibilities involved: 3rd tier technical support, network security administration, incident response handling, researching new technologies, technical sales calls and proposing solutions to enhance the operation of various client networks.

Major Accounts Support Analyst

Keystone Medical systems/Companion Technologies

March 1997 to June 1998

Troubleshot a wide variety of software, networking, and hardware problems for large medical billing clients.

**CAPTR Team Auditor**

Employment

March  2013 - PRESENT

Independent Security Researcher / PhD Student

*University of Maryland, College Park, MD*

Experienced in topics dealing with cyber security, and pertaining to computer network operations and exploitation.

Current Research Focuses;

IoT device categorization and emulation

Static and dynamic analysis of firmware for categorization and security vulnerability assessment.

May 2010 - March 2013

IT Security Engineer (Team Lead)

*SAIC, NASA Goddard Space Flight Center*

Technical lead for the NASA Mission Security Vulnerability Scan Team, which performs coordinated vulnerability assessments of all networks/projects residing on the NASA Mission network.

Quarterly and Ad-Hoc vulnerability scan of networked devices on critical mission network.

Assisted in vulnerability remediation and mitigation.

Proof of concept exploit demonstrations and application penetration testing. (CVE-2014-1671).

2007 - 2010

Software Developer

*JBS International, Bethesda, MD*

Primary developer for National Children's Bureau Child Welfare Application, utilizing C# and the Microsoft .NET Framework.

Maintained source code and implemented bug fixes and enhancements.

2007 - 2010

Network Associate

*JBS International, Bethesda, MD*

Implementation and management of Microsoft Active Directory Environment and Microsoft Exchange.

Daily Administrator tasks to include user management, email migration, backup, file server access control lists, and new software deployment.

Create, tested, and published group policies to entire enterprise.

Education

Ph.D., Reliability Engineering; University of Maryland at College Park *(Anticipate 2019)*

M.S., Computer Science; Johns Hopkins University *(2011)*

B.S., Computer Engineering; Drexel University *(2005)*

Technical Competency

Topics pertaining to Cyber Network Operation and Exploitation.

Various Operating Systems (Linux, Windows, etc.) and security toolkits (backtrack, Kali).

Penetration testing suites such as Metasploit and Core Impact.

Vulnerability/Network Assessment tools (Nessus, Foundstone, NMAP, etc.)

Security related topics such as exploitation and pivoting, network reconnaissance, vulnerability discovery, etc.

Topics pertaining to networking such as TCP/IP and the OSI model.

Certification/Training

GIAC GPEN, GXPN, C|EH, Security+, MCP

Remote Operator Training
Advanced Windows Operator Course
VMware vsphere: Install Configure and Manage
Microsoft Powershell workshop
SANS 660: Advanced Pen. Testing , Exploit Writing, and Ethical Hacking 91/15)
SANS 560: Network Pen. Testing and ethical Hacking (12/12)
McAfee Foundstone Training (8/10, 8/11, 12/12)

**APT Emulator**

CISSP, GPEN, CEH

Director

EXPERIENCE SUMMARY:

Mr. Black is a cyber security professional and experienced leader of other cyber security professionals. Mr. Black has more than eight years of professional work experience in the Information Technology Security industry with a focus on offensive security and project management. His hands-on work with vulnerability identification and exploit development has led to the development of multiple standard operating procedures and training courses. His technical understanding of software development and network architecture allow him to test vulnerabilities even further for hardening and complete analysis.

AREAS OF EXPERTISE:

- Contract Management

- APT Emulation
- Penetration Testing
- Offensive Security Training

SECURITY CLEARANCE:

TS/SCI

PROFESSIONAL EXPERIENCE:

Defense Point Security 02/2015 – Present

Director/Lead Penetration Tester

Mr. Black serves as the Director of a major commercial contract at Defense Point Security. He oversees several teams of Security Engineers, Penetration Testers, and Security Analysts in addition to managing daily contract operations.

He personally leads several teams of highly skilled Penetration Testers in external and internal network and web application testing and participates in the testing himself. He works with the customer to develop testing objectives and coordinates the team to achieve those objectives.

During his time with Defense Point Security, Mr. Black has written a web application for a major commercial corporation and taught offensive security classes to a major government organization.

KEYW Corporation 11/2013 – 02/2015

Instructor

Mr. Black served as the Instructor at the Advanced Windows Operations Course where he instructed Trainee Windows Operators in advanced tradecraft and skills needed to become an Apprentice Windows Operator. He developed graduate level course material covering all topics related to Computer Network Operations and sustained SIGINT collection. He assessed students' understanding and tradecraft concerning Computer Network Operations practice and methodology. Mr. Black participated in the development of a Learning Management System, contributed content to the Windows Exploitation and Analysis course and created server/client-based malware, backdoor, and command and control for use in course.

National Security Agency 10/2011 - 11/2013 Operator

Mr. Black served as the Operator in support of the National Security Agency. He mentors and guides other operators during, before and after operations. He used advanced software applications for network navigation, tactical forensic analysis, collection of intelligence information, and when directed, execute operations in support of mission critical initiatives. Mr. Black maintained awareness of applicable computer network exploitation policies, regulations, and compliance documents. He performed risk evaluations and assessments, tested specialized software tools and operational techniques in controlled environments, and recommended future strategy needs and tactics to develop and/or establish access. Mr. Black also provided guidance and mentorship to Trainee Operators during ops.

United States Army 07/2010 - 02/2014

Signals Collector/Analyst (355)

Mr. Black served as the Signals Collector/Analyst where he enabled computer network operations that support United States Cyber Command (USCYBERCOM) and United States Army Cyber Command (ARCYBER).

Sam’s Club 11/2008 - 07/2010

RFID Project in Store Lead

Mr. Black served as the Store Lead where he was solely responsible for implementing, monitoring, and maintaining a new store wide technical RFID hardware system. He monitored over 300 RFID tag locations, maintained RFID hardware including forklift monitors, specialized RFID tag printers, and RFID scanning tools and implemented and monitored system upgrades through system audits.

ORGANIZATIONS, CONFERENCES AND AWARDS:

- Army Achievement Medal, August 2011
- Distinguished Honor Graduate, Joint Cyber Analysis Course (1st in Class)
- Distinguished Graduate, Communications Signals Collection/Processing Course (2nd in Class)

EDUCATION AND TRAINING:

- B.S., Network Security, University of Maryland University College, In Progress
- KEYW Windows Exploitation and Analysis Course, November 2013
- Advanced Windows Operations Course, November 2012
- CISSP Course, September 2012
- SANS 560 Network Exploitation Course, March 2012
- ROC Operator Course , October 2011 - February 2012
- Joint Cyber Analysis Course, February 2011 - August 2011
- Communications Signals Collection/Processing Course, September 2010 – January 2011

CERTIFICATIONS:

- Certified Ethical Hacker (CEH), 2015
- Certified Information System Security Professional (CISSP), 2012
- Certification GIAC Penetration Tester (GPEN), 2012

# Appendix D – Control Network

| Description | IP ADDRESS | VLAN | Machine Name | User(s) | Operating System |
|---|---|---|---|---|---|
| DMZ to Internet Router / FW | 172.16.100.253 / 172.16.1.1 | 1 | THEREANDBACKAGAIN | | Vyos |
| Internet FTP | 172.16.100.10 | 1 | HILLROAD.SHIRELAW | | Ubuntu |
| Client Internet Access 1 | 172.16.100.251 | 1 | SHIREWEB1.SHIRELAW | shirelaw.guest | Windows 7 32 Bit |
| Client Internet Acccess 2 | 172.16.100.252 | 1 | SHIREWEB2.SHIRELAW | shirelaw.guest | Windows 7 32 Bit |
| DMZ to Corp Router | 172.16.100.254 / 172.16.201.253 | 1 & 2 | KHAZAD-DUM | | Vyos |
| Intranet FTP | 172.16.201.10 | 2 | PRANCINGPONY.SHIRELAW | | Ubuntu |
| Domain Controller | 172.16.201.100 / 172.16.202.100 | 2 & 3 | SHIRE.SHIRELAW | | Windows 2008 R2 64 bit |
| Back-Up Domain Controller | 172.16.201.101 / 172.16.202.101 | 2 & 3 | HOBBITON.SHIRELAW | | Windows 2008 R2 64 bit |
| Admin Sharepoint | 172.16.201.110 | 2 | GARDEN.SHIRELAW | | Windows 2008 R2 64 bit |
| Admin | 172.16.201.111 | 2 | LBAGGINS.SHIRELAW | Largo.Baggins | Windows 7 64 Bit |
| IT Guy | 172.16.201.113 | 2 | JCOTTON.SHIRELAW | Jolly.Cotton | Windows 7 64 Bit |
| CEO | 172.16.201.210 | 2 | HBOFFIN.SHIRELAW | Hugo.Boffin | Windows 7 32 Bit |
| VP of Human Resources | 172.16.201.211 | 2 | FBOFFIN.SHIRELAW | Folco.Boffin | Windows 7 32 Bit |
| CFO | 172.16.201.221 | 2 | HGAMMIDGE.SHIRELAW | Hob.Gammidge | Windows 7 32 Bit |
| CPA | 172.16.201.222 | 2 | HBRACEGIRDLE.SHIRELAW | Hugo.Bracegirdle | Windows 7 32 Bit |
| CTO | 172.16.201.231 | 2 | ITOOK.SHIRELAW | Isengar.Took | Windows 7 64 Bit |
| Office Assistant 1 | 172.16.201.212 | 2 | FBOLGER.SHIRELAW | Fredegar.Bolger | Windows 7 32 Bit |
| Office Assistant 2 | 172.16.201.213 | 2 | GTOOK.SHIRELAW | Gerontius.Took | Windows 7 32 Bit |
| Big Conference Room Laptop | 172.16.201.80 | 2 | GREENDRAGON.SHIRELAW | | Windows 7 32 Bit |
| Small Conference Room Laptop | 172.16.201.81 | 2 | FLOATINGLOG.SHIRELAW | | Windows 7 32 Bit |
| Interview Room 1 | 172.16.201.82 | 2 | FORSAKENINN.SHIRELAW | | Windows 7 32 Bit |
| Interview Room 2 | 172.16.201.83 | 2 | BRIDGEINN.SHIRELAW | | Windows 7 32 Bit |
| Corp to Law Router | 172.16.201.254 / 172.16.202.253 | 2 & 3 | Deepening-Road | | Vyos |
| Partner 1 | 172.16.202.10 | 3 | BBAGGINS.SHIRELAW | Bilbo.Baggins | Windows 7 32 Bit |
| Partner 1 Nephew | 172.16.202.11 | 3 | FBAGGINS.SHIRELAW | Frodo.Baggins | Windows 7 32 Bit |
| Partner 1 Secretary | 172.16.202.12 | 3 | CSACKVILLE.SHIRELAW | Camellia.Sackville | Windows 7 32 Bit |
| Partner 1 Nephew Secretary | 172.16.202.13 | 3 | CBRANDYBUCK.SHIRELAW | Celadine.Brandybuck | Windows 7 32 Bit |
| Partner 1 Legal Aid 1 | 172.16.202.14 | 3 | CCOTTON.SHIRELAW | Carl.Cotton | Windows 7 32 Bit |
| Partner 1 Legal Aid 2 | 172.16.202.15 | 3 | AROPER.SHIRELAW | Andwise.Roper | Windows 7 32 Bit |
| Partner 2 | 172.16.202.20 | 3 | SGAMGEE.SHIRELAW | Samwise.Gamgee | Windows 7 32 Bit |
| Partner 2 Secretary | 172.16.202.21 | 3 | RCOTTON.SHIRELAW | Rose.Cotton | Windows 7 32 Bit |
| Partner 3 | 172.16.202.30 | 3 | PTOOK.SHIRELAW | Perrigen.Took | Windows 7 32 Bit |
| Partner 3 Secretary | 172.16.202.31 | 3 | FTOOK.SHIRELAW | Faramir.Took | Windows 7 32 Bit |
| Partner 3 Legal Aid | 172.16.202.32 | 3 | ETOOK.SHIRELAW | Esmeralda.Took | Windows 7 32 Bit |
| Other Lawyer 1 | 172.16.202.40 | 3 | PBOLGER.SHIRELAW | Pansy.Bolger | Windows 7 32 Bit |

| | | | | | |
|---|---|---|---|---|---|
| Other Lawyer 2 | 172.16.202.50 | 3 | RSMALLBURROW.SHIRELAW | Robin.Smallburrow | Windows 7 32 Bit |
| Other Lawyers Legal Aid | 172.16.202.45 | 3 | SPROUDFOOT.SHIRELAW | Sancho.Proudfoot | Windows 7 32 Bit |
| Jr Partner | 172.16.202.60 | 3 | MBRANDYBUCK.SHIRELAW | Meriadoc.Brandybuck | Windows 7 32 Bit |
| Jr Partner Secretary | 172.16.202.61 | 3 | TBAGGINS.SHIRELAW | Tanta.Baggins | Windows 7 32 Bit |
| Open Case Files | 172.16.202.99 | 3 | BAGEND.SHIRELAW | | Windows 2008 R2 64 bit |
| Closed Case files | 172.16.202.199 | 3 | BYWATER.SHIRELAW | | Windows 2008 R2 64 bit |
| Case Files backup | 172.16.202.200 | 3 | HARDBOTTLE.SHIRELAW | | Ubuntu |

<table>
<tr><td>Largo.Baggins</td><td>diEAd>9Azp;4rMJ</td></tr>
<tr><td>Jolly.Cotton</td><td>7+K8.?&&>/P\gRz</td></tr>
<tr><td>Hugo.Boffin</td><td>h>97*0#3MQm{0+R</td></tr>
<tr><td>Folco.Boffin</td><td>g5Q98Q:.04t*98b</td></tr>
<tr><td>Hob.Gammidge</td><td>{Hs|%77!6">,*_f</td></tr>
<tr><td>Hugo.Bracegirdle</td><td>5_ []AHGt102+rf</td></tr>
<tr><td>Isengar.Took</td><td>[|~/0C({:+)j01c</td></tr>
<tr><td>Fredegar.Bolger</td><td>8(l409W'9r4kUrA</td></tr>
<tr><td>Gerontius.Took</td><td>7Fc<FOy/)zfA":h</td></tr>
<tr><td>Bilbo.Baggins</td><td>"<Kj+y&i2l'\6UJ</td></tr>
<tr><td>Frodo.Baggins</td><td>1~(248!"D7tP)[E</td></tr>
<tr><td>Camellia.Sackville</td><td>2'62Tk|h4"A8<-l</td></tr>
<tr><td>Celadine.Brandybuck</td><td>K)}86-6_z@#RA5e</td></tr>
<tr><td>Carl.Cotton</td><td>M#^l6=3}(!/a1$J</td></tr>
<tr><td>Andwise.Roper</td><td>2Yz8'e$3\]<@~7M</td></tr>
<tr><td>Samwise.Gamgee</td><td>+x ')<:7sb%$x]X</td></tr>
<tr><td>Rose.Cotton</td><td><'(E"QCK:Ctr5ml</td></tr>
<tr><td>Bandobras.Took</td><td>OQR7<Eq9X0o4BkB</td></tr>
<tr><td>Peregrin.Took</td><td>QQF4<Eq9X0o4BkE</td></tr>
<tr><td>Faramir.Took</td><td>nN31aCWzS}hq6qN</td></tr>
<tr><td>Esmeralda.Took</td><td>@*2+$n;|n!/y/ G</td></tr>
<tr><td>Pansy.Bolger</td><td>;e4Cn*56A/^?V6z</td></tr>
<tr><td>Robin.Smallburrow</td><td>BZMg>q6byY$r[jf</td></tr>
<tr><td>Sancho.Proudfoot</td><td>$=$C@@Y#F&D1);w</td></tr>
<tr><td>Meriadoc.Brandybuck</td><td>"337s419r8E"9kZ</td></tr>
<tr><td>Tanta.Baggins</td><td>{BFf4|zD6CXWres</td></tr>
<tr><td>shirelaw.guest</td><td>$hireL@w</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Local Admin</td><td>12#$FShirelaw</td></tr>
<tr><td>Domain Admin</td><td>ShireLaw111</td></tr>
</table>

# Appendix E – Clone 1 (Red Team Assessed Network)

| Description | IP ADDRESS | Machine Name | User(s) | Operating System |
|---|---|---|---|---|
| Internet to DMZ Router | 192.168.253.1 / 172.16.1.1 | STARBASE42.FEDLAW | | Vyo |
| DMZ | 192.168.253.0 | | | |
| Firewall | 192.168.253.200 | WORMHOLE.FEDLAW | | Pfsense |
| Internet FTP | 192.168.253.210 | TURBOLIFT.FEDLAW | | Ubuntu |
| Internet Web-Server | 192.168.253.220 | DS9.FEDLAW | | Windows 2008 R2 64 bit |
| Client Internet Access 1 | 192.168.253.230 | ENTERPRISE.FEDERALE | fedlaw.guest | Windows 7 32 Bit |
| Client Internet Acccess 2 | 192.168.253.240 | VOYAGER.FEDERALE | fedlaw.guest | Windows 7 32 Bit |
| DMZ to Corp Router | 192.168.253.2 / 192.168.254.1 | DEEPSPACENINE.FEDLAW | | Vyo |
| Corp Subnet | 192.168.254.0 | | | |
| Intranet FTP | 192.168.254.50 | SHUTTLEBAY.FEDLAW | | Ubuntu |
| Domain Controller | 192.168.254.222 / 192.168.255.222 | FEDERATION.FEDLAW | | Windows 2008 R2 64 bit |
| Back-Up Domain Controller | 192.168.254.223 / 192.168.255.223 | STARFLEET.FEDLAW | | Windows 2008 R2 64 bit |
| Admin Sharepoint | 192.168.254.51 | RUNABOUT.FEDLAW | | Windows 2008 R2 64 bit |
| Admin | 192.168.254.52 | MOBRIEN.FEDLAW | miles.obrien | Windows 7 64 Bit |
| Security Machine | 192.168.254.53 | ENGINEERING.FEDLAW | | Kali 2 |
| IT Guy | 192.168.254.54 | GLAFORGE | geordi.laforge | Windows 7 64 Bit |
| CEO | 192.168.254.55 | JKIRK.FEDLAW | james.t.kirk | Windows 7 32 Bit |
| VP of Human Resources | 192.168.254.56 | NUHURA.FEDLAW | nyota.uhura | Windows 7 32 Bit |
| CFO | 192.168.254.57 | QUARK.FEDLAW | quark | Windows 7 32 Bit |
| CPA | 192.168.254.58 | NOG.FEDLAW | nog | Windows 7 32 Bit |
| CTO | 192.168.254.59 | MSCOTT.FEDLAW | montgomery.scott | Windows 7 64 Bit |
| Office Assistant 1 | 192.168.254.60 | KOBRIEN.FEDLAW | keiko.obrien | Windows 7 32 Bit |
| Office Assistant 2 | 192.168.254.61 | HSATO.FEDLAW | hoshi.sato | Windows 7 32 Bit |
| Big Conference Room Laptop | 192.168.254.62 | TENFORWAD.FEDLAW | | Windows 7 32 Bit |
| Small Conference Room Laptop | 192.168.254.63 | QUARKS.FEDLAW | | Windows 7 32 Bit |
| Interview Room 1 | 192.168.254.64 | RIOGRANDE.FEDLAW | | Windows 7 32 Bit |
| Interview Room 2 | 192.168.254.65 | RUBICON.FEDLAW | | Windows 7 32 Bit |
| Corp to Law Router | 192.168.254.2 192.168.255.1 | CONTAINMENTFIELD.FEDLAW | | Vyo |
| Partner 1 | 192.168.255.150 | JPICCARD.FEDLAW | jeanluc.piccard | Windows 7 32 Bit |
| Partner 1 Nephew | 192.168.255.151 | WRIKER.FEDLAW | william.riker | Windows 7 32 Bit |
| Partner 1 Secretary | 192.168.255.152 | WCRUSHER.FEDLAW | wesley.crusher | Windows 7 32 Bit |
| Partner 1 Nephew Secretary | 192.168.255.153 | DTROI.FEDLAW | deanna.troi | Windows 7 32 Bit |
| Partner 1 Legal Aid 1 | 192.168.255.154 | WORF.FEDLAW | worf | Windows 7 32 Bit |
| Partner 1 Legal Aid 2 | 192.168.255.155 | BCRUSHER.FEDLAW | beverly.crusher | Windows 7 32 Bit |
| Partner 2 | 192.168.255.156 | KJANEWAY.FEDLAW | kathryn.janeway | Windows 7 32 Bit |
| Partner 2 Secretary | 192.168.255.157 | TPARIS.FEDLAW | tom.paris | Windows 7 32 Bit |
| Partner 2 Legal Aid | 192.168.255.158 | SEVEN.FEDLAW | seven | Windows 7 32 Bit |
| Partner 3 | 192.168.255.159 | BCISCO.FEDLAW | benjamin.cisco | Windows 7 32 Bit |
| Partner 3 Secretary | 192.168.255.160 | JDAX.FEDLAW | jadzia.dax | Windows 7 32 Bit |
| Partner 3 Legal Aid | 192.168.255.161 | KNERYS.FEDLAW | kira.nerys | Windows 7 32 Bit |
| Other Lawyer 1 | 192.168.255.162 | SPOCK.FEDLAW | spock | Windows 7 32 Bit |
| Other Lawyer 2 | 192.168.255.163 | TUVOK.FEDLAW | tuvok | Windows 7 32 Bit |
| Other Lawyers Legal Aid | 192.168.255.164 | SAAVIK.FEDLAW | saavik | Windows 7 32 Bit |
| Jr Partner | 192.168.255.165 | VASH.FEDLAW | VASH | Windows 7 32 Bit |
| Jr Partner Secretary | 192.168.255.166 | TYAR.FEDLAW | tasha.yar | Windows 7 32 Bit |
| Open Case Files | 192.168.255.111 | DATA.FEDLAW | | Windows 2008 R2 64 bit |

|  |  |  |  |  |
|---|---|---|---|---|
| Closed Case files | 192.168.255.121 | LOR.FEDLAW |  | Windows 2008 R2 64 bit |
| Case Files backup | 192.168.255.131 | ODO.FEDLAW |  | Ubuntu |

|  |  |
|---|---|
| fedlaw.guest | 12#$FederationLaw |
| miles.obrien | \8wPj!]$hS\7A\|V |
| geordi.laforge | ),U.H_%ZV5.N<sj |
| james.t.kirk | m3p[e= Hw+'{[dq |
| nyota.uhura | >8A<?^/]{m7k/r |
| quark | )5)72J&8767J3de |
| nog | n8Sk=XvpR0MDu7z |
| montgomery.scott | novKQoNjxtj?9[r |
| keiko.obrien | C3!I(Rh-S}F^~fn |
| hoshi.sato | H'0:Zja+3t<4,\|j |
| jeanluc.piccard | *C41k_:M^B^u_-L |
| william.riker | 983G=W;Ruqq&*75N |
| wesley.crusher | fP/8zBU utg;/qS |
| deanna.troi | 7XPwhN\\|LvQN.+J |
| worf | 8#~{!'r$f}8#!6W |
| beverly.crusher | pq":<\|pOv]0h?GP |
| kathryn.janeway | novKQoNjxtj?9[r |
| tom.paris | 17r6C39/0mqmYVJ |
| seven | Dlb4"O-\eM,.-@n |
| benjamin.cisco | 530s}=0T&,5p-_G |
| jadzia.dax | :$e7+MR Nuw17}I |
| kira.nerys | 3C24l01vQ+88A6U |
| spock | L8"#}{dwdK>FBcf |
| tuvok | \|s5[p!58n^ *%&I |
| saavik | 68q07Y9WC7l15=T |
| vash | cF7;du.)7j*(b-i |
| tasha.yar | G61\|P-8!%=w\!2M |
|  |  |
| Domain Admin | F3dL@w!!! |
| Local Admin | !!FEDlaw22 |

# Appendix F – Clone 2 (CAPTR Team Assessed Network)

| Description | IP ADDRESS | Machine Name | User(s) | Operating System |
|---|---|---|---|---|
| Internet to DMZ Router | 10.0.1.100 / 172.16.1.1 | PLANETNAMEK.DRAGONLAW | | |
| Internet FTP | 10.0.1.230 | MOUNTKIWI.DRAGONLAW | | Ubuntu |
| Client Internet Access 1 | 10.0.1.130 | GINGER.TOWN | | Windows 7 32 Bit |
| Client Internet Acccess 2 | 10.0.1.30 | BRIDGE.TOWN | | Windows 7 32 Bit |
| DMZ to Corp Router | 10.0.1.200 / 10.0.2.100 | PLANETYARDRAT.DRAGONLAW | | Vyo |
| Intranet FTP | 10.0.2.230 | FIREMOUNTAIN.DRAGONLAW | | Ubuntu |
| Domain Controller | 10.0.2.1 / 10.0.3.1 | DRAGONBALL.DRAGONLAW | | Windows 2008 R2 64 bit |
| Back-Up Domain Controller | 10.0.2.2 / 10.0.3.2 | CAPSULECORP.DRAGONLAW | | Windows 2008 R2 64 bit |
| Admin Sharepoint | 10.0.2.4 | KAMEHOUSE.DRAGONLAW | | Windows 2008 R2 64 bit |
| Admin | 10.0.2.5 | BULMA.DRAGONLAW | bulma | Windows 7 64 Bit |
| IT Guy | 10.0.2.7 | TRUNKS.DRAGONLAW | trunks | Windows 7 64 Bit |
| CEO | 10.0.2.8 | GOKU.DRAGONLAW | goku | Windows 7 32 Bit |
| VP of Human Resources | 10.0.2.9 | GOTEN.DRAGONLAW | goten | Windows 7 32 Bit |
| CFO | 10.0.2.10 | GOHAN.DRAGONLAW | gohan | Windows 7 32 Bit |
| CPA | 10.0.2.11 | PAN.DRAGONLAW | pan | Windows 7 32 Bit |
| CTO | 10.0.2.12 | YAMCHA.DRAGONLAW | yamcha | Windows 7 64 Bit |
| Office Assistant 1 | 10.0.2.13 | CHICHI.DRAGONLAW | chichi | Windows 7 32 Bit |
| Office Assistant 2 | 10.0.2.14 | BEERUS.DRAGONLAW | beerus | Windows 7 32 Bit |
| Big Conference Room Laptop | 10.0.2.15 | BANSHOSPA.DRAGONLAW | | Windows 7 32 Bit |
| Small Conference Room Laptop | 10.0.2.16 | PAPAYAISLAND.DRAGONLAW | | Windows 7 32 Bit |
| Interview Room 1 | 10.0.2.17 | MOUNTPAOZU.DRAGONLAW | | Windows 7 32 Bit |
| Interview Room 2 | 10.0.2.18 | MOUNTFRAPPE.DRAGONLAW | | Windows 7 32 Bit |
| Corp to Law Router | 10.0.2.200 / 10.0.3.100 | PLANETVEGETA.DRAGONLAW | | Vyo |
| Partner 1 | 10.0.3.1 | MAJINBOO.DRAGONLAW | Majin.boo | Windows 7 32 Bit |
| Partner 1 Nephew | 10.0.3.2 | OOB.DRAGONLAW | oob | Windows 7 32 Bit |
| Partner 1 Secretary | 10.0.3.3 | ANDROID16.DRAGONLAW | Android.16 | Windows 7 32 Bit |
| Partner 1 Nephew Secretary | 10.0.3.4 | ANDROID17.DRAGONLAW | Android.17 | Windows 7 32 Bit |
| Partner 1 Legal Aid 1 | 10.0.3.5 | ANDROID18.DRAGONLAW | Android.18 | Windows 7 32 Bit |
| Partner 1 Legal Aid 2 | 10.0.3.6 | BOBBIDI.DRAGONLAW | bobbidi | Windows 7 32 Bit |
| Partner 2 | 10.0.3.7 | CELL.DRAGONLAW | cell | Windows 7 32 Bit |
| Partner 2 Secretary | 10.0.3.8 | CHAMPA.DRAGONLAW | champa | Windows 7 32 Bit |
| Partner 2 Legal Aid | 10.0.3.9 | DENDE.DRAGONLAW | dende | Windows 7 32 Bit |
| Partner 3 | 10.0.3.10 | FREEZA.DRAGONLAW | freeza | Windows 7 32 Bit |
| Partner 3 Secretary | 10.0.3.11 | BURDOCK.DRAGONLAW | burdock | Windows 7 32 Bit |
| Partner 3 Legal Aid | 10.0.3.12 | BROLY.DRAGONLAW | broly | Windows 7 32 Bit |
| Other Lawyer 1 | 10.0.3.13 | JACO.DRAGONLAW | jaco | Windows 7 32 Bit |
| Other Lawyer 2 | 10.0.3.14 | GERO.DRAGONLAW | gero | Windows 7 32 Bit |
| Other Lawyers Legal Aid | 10.0.3.15 | VIDEL.DRAGONLAW | videl | Windows 7 32 Bit |
| Jr Partner | 10.0.3.16 | PICCOLO.DRAGONLAW | piccolo | Windows 7 32 Bit |
| Jr Partner Secretary | 10.0.3.17 | WHIS.DRAGONLAW | whis | Windows 7 32 Bit |
| Open Case Files | 10.0.3.70 | ONESTAR.DRAGONLAW | | Windows 2008 R2 64 bit |
| Closed Case files | 10.0.3.71 | TWOSTAR.DRAGONLAW | | Windows 2008 R2 64 bit |
| Case Files backup | 10.0.3.72 | FOURSTAR.DRAGONLAW | | Ubuntu |

| | |
|---|---|
| miles.obrien | sP3F?juSt?dr |
| geordi.laforge | pReP7e3ra$#v |
| james.t.kirk | Trec33Ura$RU |
| nyota.uhura | mazafet_cUm7 |
| quark | kazepR46!sPA |
| nog | #terude-w2Ch |
| montgomery.scott | sEb#!Adrug4w |
| keiko.obrien | waNa5hat4=sT |
| hoshi.sato | ?-ga2emanUju |
| jeanluc.piccard | sPuqufewa4!e |
| william.riker | S6g?q5Jucre+ |
| wesley.crusher | ma8+sturUf-p |
| deanna.troi | T8WUNe5uzat$ |
| worf | PRus@a4abEB? |
| beverly.crusher | wet=ebUV22aw |
| kathryn.janeway | Z2@uspusEsut |
| tom.paris | Pha8AceFra*2 |
| seven | brU$epu@7ake |
| benjamin.cisco | wra3eKadrU?3 |
| jadzia.dax | juSW?c3asaph |
| kira.nerys | 6umup$ES5ugE |
| spock | pap3=ujAfr5b |
| tuvok | Wa4rEXAthah# |
| saavik | tUmE3eyu?a6u |
| vash | MAY!Qe5ha3ru |
| tasha.yar | caCasux4z5s= |
| | |
| Domain Admin | !@34DRAGONlaw |
| Local Admin | DR@g0n!!! |

## Appendix G – Letter to Red Teamer

The scenario is as follows. A small law firm has recently acquired a new partner and with it a case in which they represent a protected witness in a mafia mass murder trial. The new lawyer's historical privileged attorney client information with the patient will now be stored on the case file servers of the firm. Security has not been a focus or in the budget previously for the firm but given the sensitive nature of this newly acquired case files and the likelihood of the mafia to pay hackers to see what the witness has said the firm has shifted more of a focus to security. They have had a virtual representation of the network set up so that you can assess it and recommend changes to it. These changes will be put into effect by the firms Systems Administrator and confirmed with you after. The security of the network will then be evaluated and compared to an evaluation of other types of security recommendations and the baseline network.  You will do your best to accurately represent a traditional Red Team assessment of this network.

The rules of engagement for the red team assessment are straight forward. You are going to be given access to a beaconing implant in the DMZ of the network simulating a grey box test. Given the time constraints there will be no authorized exploitation or kinetic testing of systems such as brute forcing. You will be expected to enumerate the virtual environment from the perspective of the DMZ via whatever scanning and enumeration you deem necessary. You will also be expected to utilize the access you have to the host in the DMZ to ascertain any additional information from it. Any information or credentials discovered on this host may be tested on boxes identified during your scanning however accessing other systems using these credentials to further network enumeration is beyond the scope of this short test.

The 172.16.1.0/24 Is out of scope and does not need to be enumerated. For the purposes of this scenario this subnet is the 'internet'. Below are the subnets of the corporation that are to be assessed.

172.16.100.0/24

172.16.201.0/24

172.16.202.0/24

Once you have completed your assessment of the network please write your recommendations to the Systems Administrator as outlined in the attached document.

## Appendix H – Red Team Recommendations

Provided the following information, network reconnaissance and light enumeration was performed from the perspective of a threat actor having access to a system in the DMZ of the targetted network.

172.16.100.0/24 - DMZ; Comprimised host in this range
172.16.201.0/24 - User network
172.16.202.0/24 - User network

Each network range was initially scanned using unicorn scanner and then further enumerated with nmap scripts as follows:

```
unicornscan -msf -pa <host>
```

```
nmap -Pn -sSUV -p <ports-discovered-via-unicorn> --open -O --script=default,banner,dns-zone-transfer,ftp-anon,ftp-vuln-cve2010-4221,http-apache-negotiation,http-auth,http-methods,http-brute,http-config-backup,http-default-accounts,http-enum,http-headers,http-iis-webdav-vuln,http-majordomo2-dir-traversal,http-method-tamper,http-open-proxy,http-open-redirect,http-passwd,http-php-version,http-phpself-xss,http-rfi-spider,http-robots.txt,http-sitemap-generator,http-title,http-unsafe-output-escaping,http-userdir-enum,krb5-enum-users,smb-vuln-*,smb-enum-domains,smb-enum-groups,smb-enum-sessions,smb-enum-shares,smb-enum-users,smb-ls,smb-enum,smb-os-discovery --append-output -oX host-enum-all.xml --script-args=unsafe=1 <host>
```

Discoveries

Vulnerability: Weak firewall settings

Importance: Critical

Estimated Time to Mitigation: 6 Hours

Mitigation: This should be mitigated by dropping all traffic originating from the DMZ and destined for internal networks

Details: During routine evaluation, It was discovered that DMZ hosts were capable of initiating communications with hosts on both user networks. DMZ hosts should not have access to internal subnets.

Vulnerability: CVE-2009-3103

Importance: High

Estimated Time to Mitigation: 4 Hours

Mitigation: Ensure these hosts are patched and updated to the lasted standard as provided by the distribution.

Details: Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location, aka "SMBv2 Negotiation Vulnerability."

The following hosts were found to be vulnerable to CVE-2009-3103:

172.16.202.10

172.16.202.11

172.16.202.12

172.16.202.13

172.16.202.14

172.16.202.15

172.16.202.20

172.16.202.21

172.16.202.30

172.16.202.31

172.16.202.32

172.16.202.40

172.16.202.45

172.16.202.50

172.16.202.60

172.16.202.61

172.16.202.99

172.16.202.100

172.16.202.101

172.16.202.199

Vulnerability: Anonymous SMB access

Importance: High

Estimated Time to Mitigation: 8 Hours

Mitigation: Ensure that anonymous access is disabled for all SMB shared.

Details: Anonymous SMB enumeration can allow an attacker to access information that would be useful in further attacks. The following hosts were found to have vulnerable SMB access:

172.16.100.251

172.16.100.252

172.16.201.31

172.16.201.100

172.16.201.101

172.16.201.110

172.16.201.111

172.16.201.113

172.16.201.210

172.16.201.211

172.16.201.212

172.16.201.213

172.16.201.221

172.16.202.10

172.16.202.11

172.16.202.12

172.16.202.13

172.16.202.14

172.16.202.15

172.16.202.20

172.16.202.21

172.16.202.30

172.16.202.31

172.16.202.32

172.16.202.40

172.16.202.45

172.16.202.50

172.16.202.60

172.16.202.61

172.16.202.99

172.16.202.100

172.16.202.101

172.16.202.199

Vulnerability: Weak Group Policy Updates

Importance: High

Estimated Time to Mitigation: 4 Hours

Mitigation: This should be mitigated by dropping all traffic originating from the DMZ and destined for internal networks

Details: Windows domain members can be vulnerable to malicious Group Policy Updates regardless of whether they are currently connected to the domain. Ensure SMB signing is enabled on the Domain controllers and domain members by enabling "Extended Protection for Authentication". Please note that testing for this scenario was outside the scope of the test.

https://support.microsoft.com/en-us/kb/968389

Vulnerability: Unnecessary Service

Importance: Medium

Estimated Time to Mitigation: 4 Hours

Mitigation: . Disable this service for all workstations where it is not needed, and block any unnecessary traffic from the DMZ.

Details: Remote Desktop (RDP) can be vulnerable to brute force attacks and used by an attacker for further access on systems using discovered credentials. RDP was found to be enabled on the following workstations172.16.201.31

172.16.201.100

172.16.201.101

172.16.201.110

172.16.201.111

172.16.201.113

172.16.201.210

172.16.201.211

172.16.201.212

172.16.201.213

172.16.201.221

172.16.202.10

172.16.202.11

172.16.202.12

172.16.202.13

172.16.202.14

172.16.202.15

172.16.202.20

172.16.202.21

172.16.202.30

172.16.202.31

172.16.202.32

172.16.202.40

172.16.202.45

172.16.202.50

172.16.202.60

172.16.202.61

172.16.202.99

172.16.202.100

172.16.202.101

172.16.202.199

Vulnerability: Unnecessary Service

Importance: Medium

Estimated Time to Mitigation: 4 Hours

Mitigation: Ensure FTP and SSH servers are configured to protected against brute force by ensuring complexity and lock out requirements. Drop or block unnecessary traffic from the DMZ to these services.

Details: FTP and SSH services were discovered on the user networks and were accessible from the DMZ. The services were found to be vulnerable to a Brute Force attack.

172.16.201.10

172.16.202.200

## Appendix I – Recommendation Guidelines

Recommendation Guidelines:

- The Systems Administrator will have no more than 20 hours to implement your recommended changes to the network.

- Please recommend an estimated 30 hours worth of changes to the network in case the Systems Administrator is able to accomplish more than you thought.

- If some of the changes you recommend are outside the scope or ability of the Systems Administrator in this scenario a dialogue will be initiated to determine if slightly different changes may accomplish the same goals you had in mind for the security of the network.

- Some changes you may recommend may simply not be feasible and the Systems Administrator will let you know they cannot be done. If changes are identified as such and they take the total recommended changes you suggest below 20 hours, you will be allowed to recommend further changes.

- 443 and 80 still must always be allowed out of the networks

- Legal staff of the firm must always be able to access their open and closed case files

- User machines must remain on the domain

- FTP must always be allowed in to the DMZ and from the DMZ to the corporate subnet and vice versa.

- Only free software may be recommended for installation

- Changes to versions of operating systems are outside the budget and scope of this scenario

- Changes involving physical devices are outside the scope of the scenario as it is virtualized

- Please submit recommendations in a bulleted list describing what you want changed and also including how many hours you think each change would take. Be as detailed as you deem appropriate when talking to a systems administrator however understand that failure to be specific enough or being too specific will likely lead to a required dialogue for clarification.

Upon completion of any dialogue and implementation of changes the systems administrator will submit a log of what exactly was performed in the network to enact the changes. If any of the changes are deemed inadequate by you then they will be reconciled as much as possible via further dialogue with the systems administrator. This will not count against the time used to implement changes in the network.

If you have any questions regarding changes please email oakleydissertation@gmail.com with the title of Recommendation Question.

## Appendix J – Red Team Recommendation Changelog

Vulnerability: Weak firewall settings

Importance: Critical

Estimated Time to Mitigation: 6 Hours

Mitigation: This should be mitigated by dropping all traffic originating from the DMZ and destined for internal networks

**Administrator Solution:** Prevent traffic from DMZ going into the networking, must still allow FTP to Intranet FTP server. The following firewall / rules were enacted on the interface handling traffic from the DMZ towards the internal subnets. After implementation of the rules I verified hosts could not talk in on TCP, UDP or IMCP and that the specific FTP hosts could still communicate as necessary.

```
set firewall name MyFirewall

set firewall name MyFirewall default-action drop

set firewall name MyFirewall rule 1 action accept

set firewall name MyFirewall rule 1 source address 192.168.253.210

set firewall name MyFirewall rule 1 destination address 192.168.254.50

set firewall name MyFirewall rule 1 protocol 'tcp'

set interfaces ethernet eth3 firewall out name MyFirewall
```

**Vulnerability: CVE-2009-3103**

Importance: High

Estimated Time to Mitigation: 4 Hours

Mitigation: Ensure these hosts are patched and updated to the lasted standard as provided by the distribution.

**Administrator Solution:** Updated the Windows 2008 SP2 servers in the network. The Windows 7 x32 workstations are not affected according to Microsoft technet.

**Vulnerability: Anonymous SMB access**

Importance: High

Estimated Time to Mitigation: 8 Hours

Mitigation: Ensure that anonymous access is disabled for all SMB shared.

Details: Anonymous SMB enumeration can allow an attacker to access information that would be useful in further attacks. The following hosts were found to have vulnerable SMB access:

**Administrator Solution:** used Microsoft recommended changes to address anonymous access to shares and pipes found here: https://technet.microsoft.com/en-us/library/jj852166(v=ws.11).aspx

*GPO_name*\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Enable the **Network access: Restrict anonymous access to Named Pipes and Shares** setting.

**Vulnerability: Weak Group Policy Updates**

Importance: High

Estimated Time to Mitigation: 4 Hours

Mitigation: This should be mitigated by dropping all traffic originating from the DMZ and destined for internal networks

**Administrator Solution:** This issue is also mitigated by blocking traffic originating from the DMZ from going into the internal subnets.

**Vulnerability: Unnecessary Service**

Importance: Medium

Estimated Time to Mitigation: 4 Hours

Mitigation: . Disable this service for all workstations where it is not needed, and block any unnecessary traffic from the DMZ.

**Administrator Solution:** RDP is necessary for administration of the network however IT Guy, Admin, CTO, Domain Administrator accounts were only ones added to remote desktop users group

**Vulnerability: Unnecessary Service**

Importance: Medium

Estimated Time to Mitigation: 4 Hours

Mitigation: Ensure FTP and SSH servers are configured to protect against brute force by ensuring complexity and lock out requirements. Drop or block unnecessary traffic from the DMZ to these services.

**Administrator Solution:** Ssh and FTP into the internal networks from the DMZ will be blocked except FTP from external FTP to internal FTP. FTP lockout and SSH lockout to routing devices and internal subnets protected by ISP filtering

## Appendix K – Intent of CAPTR Team

CAPTRed or CAPTR Team: Counter- A.P.T. Red Team

A CAPTR Team assesses the security of an organization by initially focusing on the compromises of highest possible impact regardless of their likelihood. The CAPTRed Team analyzes possible ways for such compromises to be accomplished from inside the environment they reside in. When ways of achieving lethal compromise are identified the team then aids the existing security apparatus of the organization in mitigation or detection. This mortality centric, inside out approach may not be appropriate for all organizations. However in ones with the possibility of lethal impact compromises it provides a valuable tool to mitigate those specific assets from being compromised both by internal and external sources in ways that may not be normally identified by traditional Red Team / Blue Team practices.

The CAPTR team looks at lethal impact as opposed to the more likely but less severe compromises. This means that this security posture is less likely to be adopted in situations where there is no extremely high impact cyber compromise that an organization can identify. An organization traditionally may not want to focus on a lethal compromise because the assessed risk is low due to the assessed rarity of occurrence that compromising such an item could happen. Using a CAPTRed Team however lets you take that severe risk with assumed low likelihood of compromise and see if there is a way that maybe several other more likely compromises may lead to a situation where the lethal compromise could happen and address that.

This CAPTR Team methodology is an attempt to adopt the non-cyber strategies of counter-sniper teams  to the cyber realm. Counter-sniping is the use of highly skilled current and former snipers to assess and address the threat of enemy snipers. The Army's FM 3-06.11 (FM 90-10-1) COMBINED ARMS OPERATIONS IN URBAN TERRAIN states that U.S. Snipers are one of the most effective active countermeasures to enemy snipers to detect and destroy enemy snipers before they fire due to their in depth knowledge of sniping. Similarly CAPTRed Teams should be made up of current or former hackers and penetration testers. They will case the security environment surrounding the potential lethal compromise and identify the tactics, techniques and procedures that an enemy hacker might use so that they and the rest of the security construct of an organization can better detect, defend and mitigate.

The scenario is as follows. A small law firm has recently acquired a new partner and with it a case in which they represent a protected witness in a mafia mass murder trial. The new lawyers historical privileged attorney client information with the patient will now be stored on the case file servers of the firm. Security has not been a focus or in the budget previously for the firm but given the sensitive nature of this newly acquired case files and the likelihood of the mafia to pay hackers to see what the witness has said the firm has shifted more of a focus to security. They have had a virtual representation of the network set up so that you can assess it and recommend changes to it. These changes will be put into effect by the firms Systems Administrator and confirmed with you after. The security of the network will then be evaluated and compared to an evaluation of other types of security recommendations and the baseline network.  The firm has made it clear that a compromise of the data on Open Case Files, Closed Case Files and Case File

Backup servers would be lethal to the company and potentially literally lethal to the protected witness.

Please use the perspective and intended focus of a CAPTR Team and perform an assessment in that spirit of the network and recommend changes to be be enacted on the network. You are allowed to utilize the network documentation you have received in the same email that contained this document. You are also allowed to have a dialogue with the Systems Administrator regarding network configuration and policies by sending an email to oakleydissertation@gmail.com with the subject “CAPTR Team Questions for Systems Administrator”. These questions will be answered by the person fulfilling the role of the systems administrator and the answers will be sent back to you in a timely manner. If you have questions outside the scope of this dialogue please send them to the same email address but using a different title. If a question or answer are outside the scope of a normal systems administrator’s purview of a network you may not get the answers you wish. Please follow the guidelines for recommendations which are also attached in this email when submitting your recommendations to the Systems Administrator to secure the network. Please title this email “CAPTR Team Recommendations”

## Appendix L – CAPTR Team Recommendations

Overview

Some of this is gone over in detail and some in more generalities. This is an artifact of attempting to get all this done within the 10 hour allotment. The highest-priority items are listed 1st.

Normally I would be configuring monitoring in addition to security. Detecting an intrusion is as important as securing a network. In this case, I am prioritizing prevention over detection.

Concerns that can't be addressed:

Anti-malware solution such as Bit9 and/or Faronics deep freeze. Enforcing applocker is the best I can do here.

Air-gapping the Legal network. For maximum protection this VLAN should be air-gapped. File transfers would be done by using single-use USB flash drives.

Two-factor authentication. Because relying on only a password sucks.

Latest version of Windows. Windows server should be 2012r2 at a minimum and workstations should be 8.1 or Windows 10. The specific concern is encrypted SMB traffic. I have suggested the stop-gap measure of IPSC if time permits.

1st priority Edge

1) Configure Egress filtering on the Internet gateway Vyos router/firewall as follows:

Ingress filtering: only traffic from the Internet over port 22 to the Ubuntu FTP server at 172.16.100.10 (1). Further, SCP port access (from the internet) should be restricted to only static host addresses supplied by clients/peers. SCP access from the inside should be only from the appropriate administrators. [this sounds like a big pain, but I've done it before at a hedge fund and made it work; despite significant whining from some banks we worked with]

Egress filtering: Only traffic destined to web ports (80 and 443) and established connections should be allowed [I'm assuming stateful-inspection firewalls here]. All other ports should be blocked (and logged) for outgoing traffic, except DNS (53) from the domain controllers and ClientInternet1 & 2.

Verify no management ports are open to the Internet on the Vyos router. (do a full nmap scan of all ports on the host from the external interface). Configure firewall so that management interface is only allowed from the appropriate administrator station.

Yes, I know we just broke ICMP. Don't expect PING to work.

2) Reconfigure the Ubuntu FTP server into an SCP secure file transfer server:

Use SCP for file transfers and disable/uninstall FTP.

Configure the server so that SCP accepts certificate authentication only (no username-password access REF: http://www.beginninglinux.com/home/server-administration/openssh-keys-certificates-authentication-pem-pub-crt ).

Make sure that the users using FTP (now SCP) are configured to NOT have a shell (no ability to actually log on, only transfer files). Also, make sure permissions are properly set on SCP user directories, so they can not see other directories. [Taken from stack overflow. Should work (REF: http://askubuntu.com/questions/420652/how-to-setup-a-restricted-sftp-server-on-ubuntu)

Create separate group for SFTP users.

```
sudo addgroup ftpaccess
```

Step 3 : Edit `/etc/ssh/sshd_config` file and make changes as below. (comment below line.)

```
#Subsystem sftp /usr/lib/openssh/sftp-server
```

Add these lines to the end of the file.

```
Subsystem sftp internal-sftp

Match group ftpaccess

ChrootDirectory %h

X11Forwarding no

AllowTcpForwarding no

ForceCommand internal-sftp
```

Restart sshd service.

```
sudo service ssh restart
```

Add user with ftpaccess group, create password, no shell access.

```
sudo adduser paul --ingroup ftpaccess --shell /usr/sbin/nologin
```

Modify home directory permission.

```
sudo chown root:root /home/paul
```

Create a directory inside home for upload and modify permission with group.

```
sudo mkdir /home/paul/www sudo chown paul:ftpaccess /home/paul/www
```

CRITICAL - Use ufw (uncomplicated firewall) on Host to **rate limit incoming connections** to 10/minute (ufw may be installed by default):

```
sudo apt-get install ufw && sudo ufw limit OpenSSH
```

Test and verify that:

SCP is working.

Users can't SSH into server, only SCP.

That ONLY certificate-based authentication is enabled – Users should not be able to log in with username/password, only their certificate.

That rate limiting is working.

3) On ClientInternet1 & 2:

Remove from the domain if they are on it.

Configure a unique RANDOM local administrator password on each computer

Create a local policy (this is similar to the domain policy detailed later). I would actually suggest having multiple windows open – one to these computers and another with a the Domain GPO we will be creating, because a lot of these settings are going to be the same:

Make sure passwords are 14 characters minimum.

Lock out accounts after 3 unsuccessful attempts. [Can this be done with a local policy? Can't remember and I'm out of time!]

Configure applocker to only allow Microsoft executables and block PowerShell, PSEXEC. Disable WMI service. Disable server service. (http://www.windowsnetworking.com/kbase/WindowsTips/Windows2000/UserTips/Network/Disableunnecessaryservicestoimproveworkstationsperformance.html )

Block access to the command prompt. [User Cfg - Admin Templates - System - Prevent access to the command prompt]

Use AppLocker to disable all scripting (for everyone): https://technet.microsoft.com/en-us/library/ee460958(WS.10).aspx. This includes .ps1, .bat, .cmd, .vbs and .js

Disable all office macros [if possible with local policy – not sure] and/or uninstall Office altogether: http://superuser.com/questions/1073060/disable-all-microsoft-office-macros-globally-for-all-users. Note: you will need to download the office administrative templates to access these settings: https://www.microsoft.com/en-us/download/details.aspx?id=35554

Disable the creation of scheduled tasks(computer configuration) https://msdn.microsoft.com/en-us/library/ms815152.aspx

Block execution of all untrusted applications. This will need to be done from a known-trusted system with all necessary applications already installed: (see Blocking All Untrusted Applications REF: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Securing-Application-Execution-Microsoft-AppLocker.html )

prevent execution of UTILMAN.exe and sethc.exe (can be replaced with cmd.exe to bypass login prompt)

Disable WMI service (REF: https://technet.microsoft.com/en-us/library/cc732482(v=ws.11).aspx)

Disable server service.

Disable Remote Desktop service.

Configure Windows firewall  to allow access to the Internet on 80, 443, and 53 UDP to the ISP's DNS server only.  Do NOT allow access to the local network.  Block all other outgoing traffic unless specifically needed.  The incoming traffic rules should not need to be changed.

2nd priority, DMZ firewall

The DMZ firewall should be configured as follows:

Outgoing traffic to the InternetFTP [now SCP] server on port 22.

Outgoing DNS (53 TCP and UDP) from the Domain Controllers.

Outgoing traffic to the web ports (80 & 443) for workstations.

Deny all other traffic.

3th priority, Firewall to VLAN3 [legal VLAN]

Isolate the VLANs – no comms between VLANs. [Assuming we can have separate Domains on VLAN2 & 3 as detailed below]

Allow port 80 & 443 traffic to the Internet

Allow DNS from the Domain controller [assuming we were able to create separate VLAN Domains] to the Internet.

Allow SCP to IntranetFTP and InternetFTP [now SCP] as specifically required.

Allow port 445 traffic to VLAN2 file server [was Sharepoint] from the backup server as required.

Block all other traffic between VLAN2 & VLAN3.

4th priority: VLAN3

Isolate VLAN3 from VLAN2.

Decommission one of the DCs from VLAN2 and move it to VLAN3.  Create a new domain in VLAN3 and isolate it from VLAN2. [If possible, just add another domain controller on VLAN3. If that isn't possible, remove the existing DC form the domain, Move it to VLAN3 and set it up as the Domain Controller of VLAN3.  Yes, this removes redundancy.  We are more concerned with protecting confidentiality than availability in this network.)

Move all assets on VLAN3 to the new VLAN3 domain controller.

Configure Group Policy similarly to VLAN2. [see below].

Configure additional security measures on systems similarly to VLAN2 [Disable SMBv1, disable NetBIOS, Local administrator accounts with separate random passwords, etc]

CRITICAL - **Configure EFS on files on the server(s) with critical docs.** Add only the users who need access to these files to each file (must be done individually, unfortunately). Also, **for each document, enable Mocrosoft Office security with a 12-character password [should default to 128-bit AES encryption].** Ideally a different password would be used for each document [may not be realistic, and the last thing we want is users keeping password lists on their PCs].

Remember, the files will still be encrypted with EFS and Microsoft Office security. The EFS keys will be necessary to decrypt the first layer of protection. A password will need to be entered into MSoffice to get the second layer of encryption. Use AES encryption with SHA512 hashing.

EFS REF: https://msdn.microsoft.com/en-us/library/cc875821.aspx

It is suggested a EFS recovery certificate be included to enable recovery in the event of catastrophic server error; however, this recovery certificate should be exported and kept offline on a USB key stored in a bank vault.

Office 2007: https://support.office.com/en-us/article/Password-protect-documents-workbooks-and-presentations-ef163677-3195-40ba-885a-d50fa2bb6b68

Office 2013: Enable length requirement(Group policy): https://technet.microsoft.com/en-us/library/ff657853.aspx

Office 2016: https://support.office.com/en-us/article/Add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826

Any documents that are not Microsoft office will need to be saved as ZIP files with 12+ character passwords.

CRITICAL - On the backup server all administrators will need to log onto the console locally.

Disable and uninstall remote access (RDP/VNC, SSH, etc). Configure the firewall to:

Allow outgoing connections to specific server IPs on port 445 (SMB) for backing up files.

Allow DNS to VLAN3 domain controller

Block outgoing connections

Block incoming connections

Save the configuration so it is activated on reboot.

When necessary admins can insert a rule to allow the server to download updates. This rule should be removed when the update process is complete. Generally, apt-get uses 80 or 443, but may also use FTP. (REF: http://serverfault.com/questions/433295/what-is-the-right-iptables-rule-to-allow-apt-get-to-download-programs)

REF: https://wiki.ubuntu.com/BasicSecurity/Firewall
REF: https://help.ubuntu.com/community/IptablesHowTo

```
#outgoing traffic rules:
iptables -P OUTPUT DROP    # set default outbound policy to drop
iptables -A OUTPUT -o lo -j ACCEPT      #allow loopback traffic
iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -
j ACCEPT  #allow established connections
iptables -A OUTPUT -p tcp --dport 445 --destination <Server_1> -
j ACCEPT #Allow SMB to server for backups

iptables -A OUTPUT -p tcp --dport 445 --destination <Server_2> -
j ACCEPT #Allow SMB to server_2 for backup

iptables -A OUTPUT -p tcp --dport 53 --destination <DNS_IP> -
j ACCEPT #DNS/TCP
iptables -A OUTPUT -p udp --dport 53 --destination <DNS_IP> -
j ACCEPT #DNS/UDP

# incoming traffic rules:
iptables -P INPUT DROP     # set default inbound policy to drop
iptables -A INPUT -i lo -j ACCEPT   #allow loopback traffic
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -
j ACCEPT   #allow established connections
# log & drop incoming traffic
iptables -N LOGNDROP iptables -A INPUT -j LOGNDROP

iptables -A LOGNDROP -j LOG iptables -A LOGNDROP -j DROP


iptables -P FORWARD DROP   # we are not a router

#save the rules:
iptables-save > /etc/iptables.rules
```

Make sure these rules activate on reboot.

CRITICAL – Windows firewall on **Active Case Files** (ACF) and **Closed Case Files** (CCF) should only allow access from the **Case files Backup** server and VLAN3 PCs on an as needed basis (port 445 only). All other ports should be blocked. Egress traffic should be limited to traffic to the VLAN3 DC. RDP is to be disabled [admins will have to log in locally].

Domain Group policy should prevent non-Microsoft executables from running and block script access.

Internet access can occasionally be enabled to allow the box to download Windows updates.

5rd priority, Non-legal-department VLAN2

This is going to get somewhat detailed with Group Policy, and may take a majority of the time to configure and test these policies.

I am suggesting splitting VLAN2 and VLAN3 into separate domains. This limits several possible pivot points within the network, as well as further limiting access to the file servers in VLAN3. This effectively makes VLAN2 a secondary DMZ.

Rip out Sharepoint – the attack surface is too tempting. If this server is critical for its fileshare, keep it, otherwise decommission this server.

Decommission one Domain Controller and move it to the legal VLAN3. These systems are virtual, so snapshots and VM backups would allow for speedy recovery of a DC. Only do this if you can't add a computer to VLAN3 to be its Domain controller.

On IntranetFTP, uninstall FTP and configure SCP similarly to InternetFTP. This includes certificate-based authentication, etc. Instead of using the ISP for DNS, use the Domain Controller(s) on this VLAN.

Allow SCP only from appropriate systems that require the service. Still require rate limiting.

Block all connectivity outside VLAN2 & 3.

Disable/uninstall Microsoft Shockwave, Adobe Flash, Adobe AIR, Adobe Acrobat, Java and any other 3rd party apps. If a PDF reader is required, use a trusted version of Foxit reader and allow execution through Applocker policy.

On to Group Policy! [this same policy will be used on the VLAN3 domain]

Password policy: Require 14-character passwords, account lockout after 3 unsuccessful attempts (requiring admin to unlock).

Screensaver requires password after 10 min of idle time.

Configure Applocker to only allow Microsoft executables and block PowerShell, PSEXEC. Disable WMI service (details below). Disable server service, on everything but the fileserver and Domain Controller. (http://www.windowsnetworking.com/kbase/WindowsTips/Windows2000/UserTips/Network/Disableunnecessaryservicestoimproveworkstationsperformance.html )

Block access to the command prompt for all but administrative users (will require a separate 'admin user' policy): User Cfg - Admin Templates - System - Prevent access to the command prompt

Use group policy and AppLocker to disable all scripting (for everyone): https://technet.microsoft.com/en-us/library/ee460958(WS.10).aspx. This includes .ps1, .bat, .cmd, .vbs and .js

Use group policy to disable all office macros: http://superuser.com/questions/1073060/disable-all-microsoft-office-macros-globally-for-all-users. Note: you will need to download the office administrative templates to access these settings: https://www.microsoft.com/en-us/download/details.aspx?id=35554

Disable the creation of scheduled tasks using GPO (computer configuration) https://msdn.microsoft.com/en-us/library/ms815152.aspx

CRITICAL - Block execution of all untrusted applications. This will need to be done from a known-trusted system with all necessary applications already installed: (see Blocking All Untrusted Applications REF: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Securing-Application-Execution-Microsoft-AppLocker.html )

prevent execution of UTILMAN.exe and sethc.exe (can be replaced with cmd.exe to bypass login prompt)

Disable WMI service (REF: https://technet.microsoft.com/en-us/library/cc732482(v=ws.11).aspx)

Disable server service on all workstations and servers, except the ones that need to serve files (requires a 'non-file-server' GPO and group).

Disable Remote Desktop service on all systems except the ones that specifically need it. On the systems that require RDP, specifically configure only the users that need it for access.

Configure Windows firewall for user PCs to allow access to the DC (all ports - it's a pain to restrict to the proper ports). Configure only port 445 to file server IPs as needed. 445 should not be allowed to any other system on the network. Allow 80 and 443 to the Internet, but **not** the local network. Block all other outgoing traffic unless specifically needed. The incoming traffic rules should not need to be changed (with the possible exception of RDP, which should be minimized)

Use GPO to fix the membership of local and domain administrator accounts: http://www.grouppolicy.biz/2010/01/how-to-use-group-policy-preferences-to-secure-local-administrator-groups/ [this prevents the addition of unauthorized users to admin groups].

Take local admin rights away from regular users. They will not be able to install programs [indeed, the installers shouldn’t even run due to group policy at this point, unless it’s a Microsoft-signed installer.] or change configurations.

On everything, disable NETBios and IPv6. Disable older versions of SMB. https://support.microsoft.com/en-us/kb/2696547 . This can be done manually if necessary, but most of this should be able to be accomplished through Group Policy.

Reboot computers daily: Computer Config > Preferences>Control Panel Settings > Scheduled tasks > Scheduled Task (Name: Reboot) >

Task:

Name: Reboot

Run: c:\windows\system32\shutdown.exe

Argument: shutdown /r /f /t 0

Enable idle timeouts of 5 min for locking the computer screen. [Note to self, there is no idle logout GPO setting. That's sad!]

Admin GPO

Configure group policy to block any admin accounts from being able to use a web browser.

Ideally, configure group policy to block all Internet access to admin accounts. Unfortunately, this can only be limited to disabling IE, as I was not able to find a way of configuring Windows firewall per user [except through scheduled tasks]

Enable Command-line access.

Additional items:

Configure a unique RANDOM local administrator on each computer (except the DC, which will not have a local account). Disable all other local accounts (guest, etc.) unless specifically needed.

Use unique admin accounts (per admin) that have rights to domain client PCs, but NOT servers. Use SEPERATE unique (per admin) administrative accounts on servers and configure group policy to prevent those admin accounts from having any rights to user PCs. This will result in admins having two separate admin accounts: one for managing client PCs and one for managing servers. Also configure group policy to block any admin accounts from being able to use a web browser.

As time permits:

Configure SMB encrypted traffic.

To properly do this, Upgrade to Windows 2012 and Windows 8 (REF: https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-in-windows-server-2012/)

Otherwise use IPSEC (https://support.microsoft.com/en-us/kb/942957, http://www.it.cornell.edu/services/managed_servers/howto/ipsec.cfm). The primary Priority is VLAN3, specifically the case files servers and the backup server [which will be fun considering its not Windows].

Install and configure EMET http://www.microsoft.com/emet. First priority is VLAN3 and associated servers. 2nd Priority is VLAN2 and associated servers, then the DMZ.

## Appendix M – CAPTR Team Recommendations Changelog

- move VLAN3 router from behind VLAN2 to also connecting to VLAN1 router
- implement the firewall rules on all 3 routers as you suggested (minus some that addressed external traffic to the network as it was whitecarded)
- test traffic between subnets to insure firewall is acting on them as intended tho RDP was left allowed from only the admin box in VLAN2 to VLAN3 machines (not the servers) so administration could continue.
- remove ftp from ftp servers and only allow scp
- create a non root user for individuals to use to scp
- place case files into encrypted password protected zips on scp and storage servers
- implement firewall rules limiting traffic as recommended for the file servers and making administration done only possible physically at the machine
- move back up DC strictly to VLAN3
- dcpromo back-up DC to new dc in new domain just for VLAN3
- Join VLAN3 machines to new domain
- In both domains create separate admin accounts for IT and admin users different from domain administrator account and their normal user accounts
- implemented via GPO no creation of tasks or WMI
- made only the new admin accounts capable of RDP
- applocker is 2k8 r2 and we have only 2k8 sp2 and time was not going to allow for it to be implemented
- the same goes for the rest of the gpo items unfortunately.

# References

Anderson, K. A., 2015. Evaluating Information Security Solutions: Swapping the Cost of Failure for Success. *IASACA Journal,* Volume 2.

Anon., 2013. *Data Classification Standard.* [Online]
Available at: https://security.berkeley.edu/data-classification-standard
[Accessed 16 7 2017].

Applebaum, A. et al., 2016. *Intelligent, automated red team emulation.* Los Angeles, ACM, pp. 363-373.

Applebaum, A. et al., 2016. *Intelligent, automated red team emulation.* New York, ACM, pp. 363-373.

AppliedTrust, n.d. *The Importance of Periodic Security Assessments.* [Online]
[Accessed 15 7 2017].

Arbor Networks, n.d. *9th Annual Worldwide Infrastructure Security Report,* s.l.: NETSCOUT.

Barth, B., 2016. *Cybercriminals increasingly launching APT-style attacks against banks, finds Kaspersky.* [Online]
Available at: https://www.scmagazine.com/cybercriminals-increasingly-launching-apt-style-attacks-against-banks-finds-kaspersky/article/528327/
[Accessed 16 March 2017].

Bauer, M., 2001. Paranoid Penguin: Designing and Using DMZ Networks to Protect Internet Servers. *Linux Journal,* March.2001(83es).

Berger, H. & Jones, A., 2016. *Cyber Security & Ethical Hacking For SMEs.* New York, ACM.

Boneh, D., Segev, G. & Waters, B., 2012. *Targeted malleability: homomorphic encryption for restricted computations.* Cambridge, ACM, pp. 350-366.

Boulton, C., 2016. *6 Trends That Will Shape Cloud Computing in 2017.* [Online]
Available at: http://www.cio.com/article/3137946/cloud-computing/6-trends-that-will-shape-cloud-computing-in-2017.html
[Accessed 2017].

Brangetto, P., Caliskan, E. & Roigas, H., 2015. *Cyber Red Teaming, Organisational, technical and legal implications in a military context,* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence .

Brangetto, P., Caliskan, E. & Roigas, H., 2015. *www.ccdcoe.org.* [Online]
Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Cyber_Red_Team.pdf
[Accessed 26 February 2017].

Brustoloni, J., 2002. *Protecting electronic commerce from distributed denial-of-service attacks.* Honolulu, s.n., pp. 553-561.

Carroll, M. D., n.d. *Information Security: Examining and Managing the insider Threat.* New York, ACM.

Ceccato, M., Nguyen, C. D., Appelt, D. & Briand, L. C., 2016. *SOFIA: an automated security oracle for black-box testing of SQL-injection vulnerabilities.* Singapore, IEEE, pp. 167-177.

CERT, 2009. *Common Sense Guide to Prevention and Detection of Insider Threat.* [Online]
Available at: http://www.ncix.gov/issues/ithreat/csg-v3.pdf
[Accessed 7 2017].

Chapple, M., 2012. *Four Tips for Securing a Network DMZ.* [Online]
Available at: https://fedtechmagazine.com/article/2012/05/four-tips-securing-network-dmz-fed
[Accessed 17 July 2017].

Chaudet, C., Fluery, E., Lassous, I. G. & Rivano, H., 2005. *Optimal Positioning of Active and Passive Monitoring Devices.* Toulouse, ACM, pp. 71-82.

choo, c. s., chua, c. l. & tay, s.-h. v., 2007. *Automated red teaming: a proposed framework for military application.* New Yotk, ACM, pp. 1936-1942.

Choo, C. S., Chua, C. L. & Tay, S.-H. V., 2007. *Automated red teaming: a proposed framework for military application.* London, ACM.

Clayton, G. E., 2011. *SEC Requires Disclosure of Cyber Attacks.* [Online]
Available at: https://www.irmi.com/articles/expert-commentary/sec-requires-disclosure-of-cyber-attacks
[Accessed 4 March 2017].

Computer Hope, 2017. *What is the most popular operating system?.* [Online]
Available at: https://www.computerhope.com/issues/ch001777.htm
[Accessed 12 January 2018].

Computer Incidents Investigation Department, GReAT, 2016. *APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks.* [Online]
Available at: https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/
[Accessed 2 March 2017].

Dandurand, L., 2011. *Rationale and Blueprint for a Cyber Red Team Within NATO.* Talinn, NATO, pp. 71-86.

DARKReading, 2013. Choosing, Managing, And Evaluating A Penetration Testing Service. 20 September.

EC-Council, 2017. *www.eccouncil.org.* [Online]
Available at: https://www.eccouncil.org/programs/licensed-penetration-tester-lpt-master/
[Accessed 9 March 2017].

Eeye Security Inc., 2001. *Microsoft IIS Buffer Overflow Advisory.* [Online]
Available at: http : //www.eeye.com/html/ − Research/Advisories/AD20010618.html
[Accessed 7 2017].

Elasticsearch, 2017. *The Open Source Elastic Stack.* [Online]
Available at: https://www.elastic.co/products
[Accessed 12 October 2017].

Epling, L., Hinkel, B. & Hu, Y., 2015. *Penetration testing in a box.* Kennesaw, s.n.

Feid, A., 2009. *Easy Pentesting: Metasploit's db_autopwn.* [Online]
Available at: http://allanfeid.com/content/easy-pentesting-metasploits-dbautopwn
[Accessed 12 October 2017].

Fidler, D., 2014. *IU law professor says accusing North Korea of Sony hack raises cybersecurity incident to new level.* [Online]
Available at: http://archive.news.indiana.edu/releases/iu/2014/12/north-korea-cyberthreat-raised-after-sony.shtml
[Accessed 10 March 2017].

FireEye, 2016. *M-Trends EMEA Report,* s.l.: FireEye.

FireEye, 2017. *Anatomy of Advanced Persistent Threats.* [Online]
Available at: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html
[Accessed 17 March 2017].

Formyduval, W., 2009. *Integrating static analysis and testing for firewall policies.* Orlando, ACM.

Francia, G., Thornton, D. & Brookshire, T., 2012. *Wireless vulnerability of SCADA systems.* Tuscaloosa, ACM, pp. 331-332.

ghosh, s. & juneja, s., 2006. *Computing worst-case tail probabilities in credit risk.* s.l., s.n., pp. 246-254.

Gosh, N. et al., 2015. *NetSecuritas: An Integrated Attack Graph-based Security Assessment Tool for Enterprise Networks.* Goa, s.n.

Guarda, T. et al., 2016. *Penetration Testing on Virtual Environments.* kual Lumpur, ACM, pp. 9-12.

Guarda, T. et al., 2016. *Penetration Testing on Virtual Environments.* New York, ACM, pp. 9-12.

Hafner, K. & Markoff, J., 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* New York: Simon & Shuster.

Han, C. & Dongre, R., 2014. *Q&A What Motivates Cyber-Attackers?.* [Online]
Available at: https://timreview.ca/article/838
[Accessed 18 July 2017].

harmj0y, sixdub & enigma0x3, 2017. *Powershell Empire.* [Online]
Available at: http://www.powershellempire.com/?page_id=2
[Accessed 13 October 2017].

Haselton, T., 2017. *Credit reporting firm Equifax says data breach could potentially affect 143 million US consumers,* s.l.: CNBC.

Health and Human Resources, 2017. *Enforcement Highlights.* [Online]
Available at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
[Accessed 19 September 2017].

Heiser, J., 2017. *Understanding Data Leakage,* s.l.: Gartner Research Report.

Help Net Security, 2017. *Top obstacles and benefits of security framework adoption.* [Online]
Available at: https://www.helpnetsecurity.com/2017/01/09/security-framework-adoption/
[Accessed 17 March 2017].

Hinden, R. M., n.d. *Protecting Critical Infrastructure is Critical.* San Francisco, RSA.

Hoang, V. T., Katz, J. & Malozemoff, A. J., 2015. *Automated Analysis and Synthesis of Authenticated Encryption Schemes.* Denver, ACM, pp. 84-95.

Hoffman, C., 2014. *10 of the Most Popular Linux Distributions Compared.* [Online]
Available at: linux-distributions-compared/
[Accessed 12 January 2018].

Immunity, 2017. *Canvas.* [Online]
Available at: https://www.immunityinc.com/products/canvas/
[Accessed 12 October 2017].

Imperva, 2016. *Hacker Intelligence Initiative Report,* s.l.: Imperva.

Industrial Control Systems Cyber Emergency Response Team, 2016. *ICS-CERT Year in Review ,* s.l.: NCCIC.

Intel Security, 2015. *Grand Theft Data,* s.l.: McAfee.

Investopedia, 2017. *www.investopedia.com.* [Online]
Available at: http://www.investopedia.com/terms/a/advanced-persistent-threats-apt.asp
[Accessed 1 March 2017].

IT Governance, 2018. *Penetration Testing Overview.* [Online]
Available at: https://www.itgovernance.co.uk/choosing-the-right-penetration-test
[Accessed 18 January 2018].

John, J. P. et al., 2011. *Heat-seeking honeypots: design and experience.* Hyderabad, ACM, pp. 207-216.

Kirsch, C., 2013. *Firewall Egress Filtering: Why And How You Should Control What's Leaving Your Network.* [Online]
Available at: https://community.rapid7.com/community/metasploit/blog/2013/08/28/firewall-egress-filtering-why-and-how-you-should-control-whats-leaving-your-network
[Accessed 14 March 2017].

Kirsch, C., 2013. *What is Penetration Testing?.* [Online]
Available at: https://community.rapid7.com/docs/DOC-2248
[Accessed 19 July 2017].

Kucuksille, E. U., Yalcinkaya, M. A. & Ganal, S., 2015. *Developing a penetration test methodology in ensuring router security and testing it in a virtual laboratory.* Sochi, ACM, pp. 189-195.

Levine, M. & Date, J., 2015. *22 Million Affected by OPM Hack, Officials Say.* [Online]
Available at: http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731
[Accessed 22 February 2017].

Lewis, M. J., 2013. *Characterizing risk.* s.l., ACM.

Liu, V., Musen, M. A. & Chou, T., 2015. *Data Breaches of Protected Health Information in the United States.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4479128/
[Accessed 20 March 2017].

Lund, et al., 2011. *Model-Driven Risk Analysis.* 1 ed. s.l.:Springer-Verlag Berlin Heidelberg.

Mallouli, W. et al., 2007. *A formal approach for testing security rules.* Sophia Antipolis, ACM, pp. 127-132.

Manadhata, P., Wing, J., Flynn, M. & McQueen, M., 2006. *Measuring the attack surfaces of two FTP daemons.* Alexandria, ACM, pp. 3-10.

Martin, B. & Titcomb, J., 2016. *Regulators could fine Tesco Bank over cyber attack.* [Online]
Available at: http://www.telegraph.co.uk/business/2016/11/07/tesco-bank-to-freeze-customer-transactions-after-hacking-attack/
[Accessed 19 March 2017].

Masson, P.-A.et al., 2007. *Automatic generation of model based tests for a class of security properties.* London, ACM, pp. 12-22.

McGeehan, R., 2015. *Red Teams.* [Online]
Available at: https://medium.com/starting-up-security/red-teams-6faa8d95f602
[Accessed 15 March 2017].

Melin, A., 2017. *Three Equifax Managers Sold Stock Before Cyber Hack Revealed.* [Online]
Available at: https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack
[Accessed 8 September 2017].

Merriman, C., 2016. *Windows 10 is now the second most popular desktop operating system.* [Online]
Available at: https://www.theinquirer.net/inquirer/news/2449298/windows-10-is-now-the-second-most-popular-desktop-operating-system
[Accessed 12 January 2018].

Microsoft, 2008. *Microsoft Security Bulletin MS08-067 - Critical ,* s.l.: Microsoft.

Microsoft, 2008. *MS08-067,* s.l.: Microsoft.

Microsoft, 2014. *Microsoft Security Bulletin MS14-058 - Critical ,* s.l.: Microsoft.

Microsoft, 2017. *Microsoft Security Bulletin MS17-010 - Critical,* s.l.: Microsoft.

Microsoft, 2017. *MS17-010,* s.l.: Microsoft.

Mirkovic, J. et al., 2006. *Measuring denial Of service.* Alexandria, ACM, pp. 53-58.

MITRE, 2015. *CVE ID Syntax Change.* [Online]
Available at: https://cve.mitre.org/cve/identifiers/syntaxchange.html
[Accessed 20 March 2017].

Mokube, I. & Adams, M., 2007. *Honeypots: concepts, approaches, and challenges.* Winston-Salem, ACM, pp. 321-326.

Mudge, R., 2013. *The Origin of Armitage's Hail Mary Mass Exploitation Feature.* [Online]
Available at: https://blog.cobaltstrike.com/2013/07/17/the-origin-of-armitages-hail-mary-mass-exploitation-feature/
[Accessed 12 October 2017].

Mueller, P. & Yadegari, B., 2012. *The Stuxnet Worm,* s.l.: University of Arizona.

Naghmouchi, M. Y. et al., 2016. *A New Risk Assessment Framework Using Graph Theory for Complex ICT Systems.* Vienna, s.n., pp. 97-100.

Narayanan, G., 2015. *Cyber Security in SCADA Networks.* Singapore, s.n., pp. 107-107.

Net Marketshare, 2017. *Operating System Market Share.* [Online]
Available at: https://www.netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22platform%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22platformsDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222017-01%22%2C%22dateEnd%22%3A%222017-12%22%2C%22plotKeys%22%3A%5B%7B%22platform%22%3A%22Windows%22%7D%5D%2C%22segments%22%3A%22-1000%22%7D
[Accessed 12 January 2018].

NIST, 2003. *Guide to Selecting Information Technology Security Products ,* s.l.: National Institute of Standards and technology.

NIST, 2018. *Common Vulnerability Scoring System Calculator.* [Online]
Available at: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
[Accessed 12 January 2018].

NMAP.org, 1997. *NMAP.org.* [Online]
Available at: https://nmap.org/
[Accessed 21 September 2017].

Offensive Security, 2017. *Our Most Advanced Penetration Testing Distribution, Ever..* [Online]
Available at: https://www.kali.org/
[Accessed 13 October 2017].

pentest-standard, 2014. *pre-engagement.* [Online]
Available at: http://www.pentest-standard.org/index.php/Pre-engagement
[Accessed 18 July 2017].

Perlroth, N., 2017. *Shadow Brokers Group Leaks Stolen National Security Agency Hacking Tools* [Interview] (29 June 2017).

Peterson, A., 2015. *h 2015 is already the year of the health-care hack — and it's only going to get worse..* [Online]
Available at: https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/?utm_term=.6788fb9ea0a6
[Accessed 3 March 2017].

Polychronakis, M., Anagostakis, K. & Markatos, E., 2008. *Real-world polymorphic attack detection using network-level emulation.* Oak Ridge, ACM.

Poore, K., 2001. Nimda Worm - Why is it Different?. *SANS Institute InfoSec Reading Room,* 11 November.

Raspberry Pi Foundation, 2017. *Raspberry Pi.* [Online]
Available at: https://www.raspberrypi.org/
[Accessed 12 October 2017].

Ray, A. & Cleaveland, R., 2014. *An analysis method for medical device security.* Raleigh, ACM.

Relan, K. & Singhal, V., 2016. *Pentest Ninja: XSS And SQLi Takeover Tool.* Udaipur, s.n.

Russel, D. & Gangemi, G. T., n.d. *Computer Security Basics.* Sebastopol: O'Reilly & Associates.

SANS Technology Institute, 2016. *Security Laboratory: Defense In Depth Series.* [Online]
Available at: https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface
[Accessed 17th July 2017].

SANS, 2003. *IDFAQ: An analysis of SQL.Spider-B (Digispid.B.Worm, Spida, MSSQL Worm and SQLSnake),* s.l.: SANS.

Scarfone, K., Souppaya, M., Cody, A. & Orebaugh, A., 2008. *www.nist.gov.* [Online]
Available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
[Accessed 7 March 2017].

Schmidt, M. et al., 2007. *Building a demilitarized zone with data encryption for grid environments.* Lyon, s.n.

sd, 2013. *Exploit Database.* [Online]
Available at: https://www.exploit-db.com/exploits/25444/
[Accessed 19 September 2017].

SECPOINT, 2017. *What is a Script Kiddie?.* [Online]
Available at: https://www.secpoint.com/what-is-a-script-kiddie.html
[Accessed 7 April 2017].

SECUREWORKS, 201. *www.Secureworks.com.* [Online]
Available at: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a
[Accessed 22 February 2017].

Services, D. o. H. a. H., 2017. *Civil Money Penalty.* [Online]
Available at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/index.html?language=es
[Accessed 18 March 2017].

Siddiqui, S., Khan, M. S., Ferens, K. & Kinser, W., 2016. *Detecting Advanced Persistent Threats using Fractal Dimension based Machine Learning Classification.* New Orleans, ACM, pp. 64-69.

Singh, S., Lyons, J. & Nicol, D. M., 2004. *Fast Model-Based Penetration Testing.* s.l., ACM.

Splunk, Inc, 2017. *Splunk Enterprise 7.0.0.* [Online]
Available at: https://www.splunk.com
[Accessed 12 October 2017].

Splunk, 2017. *Detect and Stop Data Exfiltration.* [Online]

Available at: https://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/use-cases/detect-and-stop-data-exfiltration.html

[Accessed 14 March 2017].

Statistica, 2017. *Market share held by the leading computer (desktop/tablet/console) operating systems worldwide from January 2012 to July 2017.* [Online]

Available at: https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/

[Accessed 12 January 2018].

Stepanova, T., Pechenkin, A. & Lavrova, D., 2015. *Ontology-based Big Data Approach to Automated Penetration Testing of Large-scale Heterogeneous Systems.* Sochi, ACM, pp. 142-149.

Stevens, J., 2016. *List of Internet, E-commerce & Hosting statistics for 2016.* [Online]

Available at: https://hostingfacts.com/internet-facts-stats-2016/

[Accessed 27 February 2017].

Strategic Cyber LLC, 2017. *Documentaion - Privilege Escalation.* [Online]

Available at: https://www.cobaltstrike.com/help-elevate

[Accessed 19 September 2017].

Strategic Cyber, LLC, 2017. *Cobalt Strike.* [Online]

Available at: https://www.cobaltstrike.com/

[Accessed 13 October 2017].

Stuckman, J. & Purtilo, J., 2012. *Comparing and applying attack surface metrics.* Lund, ACM, pp. 3-6.

Sun, K. & Jajodia, S., 2014. *Protecting Enterprise Networks through Attack Surface Expansion.* Scottsdale, ACM, pp. 29-32.

Symantec, 2016. *2016 Internet Security Threat Report,* s.l.: Symantec.

That Security Blog, 2016. *Penetration Testing and Rules of engagement.* [Online]
Available at: https://fl0x2208.wordpress.com/2016/09/03/penetration-testing-and-rules-of-engagement/
[Accessed 18 July 2017].

The Open Web Application Security Project (OWASP), 2015. *What is Attack Surface Analysis and Why is it Important?.* [Online]
Available at: https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet
[Accessed 17 July 2017].

The TREsPASS Project, 2017. *TREsPASS.* [Online]
Available at: https://www.trespass-project.eu/
[Accessed 4 October 2017].

Trend Labs, 2013. *Data Exfiltration: How Do Threat Actors Steal Your Data?.* [Online]
Available at: http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf
[Accessed 2 March 2017].

TrendLabs APT Research Team, 2012. *Spear-Phishing Email: Most Favored APT Attack Bait,* s.l.: Trend Micro Incorporated.

Ullrich, J. B., 2017. *ETERNALBLUE: Windows SMBv1 Exploit (Patched).* [Online]
Available at:
https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/
[Accessed 12 January 2018].

US-CERT, 2013. *CVE-2013-2094,* s.l.: MITRE.

US-CERT, 2016. *CVE-2016-5195 ,* s.l.: MITRE.

Vedder Price, 2012. *FCC Issues $10 Million Fine in Data Breach.* [Online]
Available at: https://www.vedderprice.com/fcc-10-million-data-breach-fine
[Accessed 19 September 2017].

Verizon, 2016. *2016 Data Breach Investigations Report,* s.l.: Verizon.

Verizon, 2017. *2017 Data Breach Investigations Report (DBIR),* s.l.: Verizon.

Verton, R., 2016. *Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' '/proc/self/mem' Race Condition Privilege Escalation (SUID Method).* [Online]
Available at: https://www.exploit-db.com/exploits/40616/
[Accessed 21 September 2017].

Vyos, 2018. *New to Vyos?.* [Online]
Available at: https://vyos.io/
[Accessed 12 January 2018].

W3Counter, 2017. *Browser & Platform Market Share.* [Online]

Available at: https://www.w3counter.com/globalstats.php

[Accessed 12 January 2018].

Wace, C., 2017. *'It's life and death to us,' patients tell cyber crooks as one surgeon reveals the NHS attack led to a computer blackout during a heart operation Read more: http://www.dailymail.co.uk/news/article-4503420/It-s-life-death-NHS-patients-say-cyber-attack.html#ixzz4s6jq18YI Follow us: @MailOnline on Twitter | DailyMail on Facebook.*

[Online]

Available at: http://www.dailymail.co.uk/news/article-4503420/It-s-life-death-NHS-patients-say-cyber-attack.html

[Accessed 8 September 2017].

Wai, C. T., 2002. Conducting a Penetration Test on an Organization. *SANS Institute InfoSec Reading Room.*

Wai, C. T., 2002. *www.sans.org.* [Online]

Available at: https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67

[Accessed 8 March 2017].

Weisman, A., 2014. *A Timeline Of The Crazy Events In The Sony Hacking Scandal.* [Online]

Available at: http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12

[Accessed February 26 2017].

Wood, B. J. & Duggan, R. A., 2000. *Red Teaming of Advanced Information Assurance Concepts.* Hilton Head, IEEE.

Yegneswaran, V., Barford, P. & Johannes, U., 2003. *Internet Intrusions: Global Characteristics and Prevalence.* s.l., ACM.

Zetter, K., 2014. *www.wired.com.* [Online]
Available at: https://www.wired.com/2014/11/what-is-a-zero-day/
[Accessed 16 March 2017].

# Curriculum Vitae

**Education:**

D. Sc. Towson University, Information Technology

M.S. Eastern Michigan University, Technology Studies

B.S. American Military University, Information Technology Management

**Dissertation:**

"Towards Improved Offensive Security Assessment Using Counter APT Red Teams"

This research aims to improve ethical hacker conducted offensive security assessments such as penetration testing or red teaming. This is accomplished through use of augmented scoping processes, initialization perspective and pivot chaining.

Dissertation Readers: Professor Mike O'Leary (advisor), Professor Lu Chao (chair), Professor Siddharth Kaza, Professor Yu Wei, Professor Suranjan Chakraborty.

**Professional Experience:**

Defens Point Security LLC, an Accenture Federal Services Company
Deputy Director and Senior Penetration Tester, 2016 – Present

Visionist Inc,
Network Exploitation Analyst, 2014-2015

KEYW Corporation
Instructor, 2013-2014

United States Marine Corps
Systems Administrator, Digital Network Operator, 2006 – 2013

**Papers:**

"Improving Cyber Defensive Stratagem Through APT Centric Offensive Security Assessment", 13th International Conference on Cyber Warfare and Security, March 2018.

"Improving Offensive Cyber Security Assessments Using Varied and Novel Initialization Perspectives", ACM South East Conference 2018, March 2018.

"Towards Improving APT Mitigation: A Case for Counter-APT Red Teaming", Journal of Information Warfare, Spring / Summer issue for 2019.