CSS300 Vulnerability Assessment and Management

Vulnerability Assessment Project

Hunter Morrison

April 2, 2019

Table of Contents

[Intrusion Tools and Techniques 3](#_Toc5809830)

[Intrusion Detection 3](#_Toc5809831)

[Intrusion Detection/Prevention Systems 3](#_Toc5809832)

[Auditing 4](#_Toc5809833)

[Audit Data Storage 4](#_Toc5809834)

[Audit Data Purpose 5](#_Toc5809835)

[Audit Data Review 5](#_Toc5809836)

[When to Conduct an Audit 5](#_Toc5809837)

[How to Review Audit Data 6](#_Toc5809838)

[Common Vulnerabilities and Exposures 7](#_Toc5809839)

[Attack Methods 8](#_Toc5809840)

[Intrusion Detection System Policies 9](#_Toc5809841)

[Protective Measures 10](#_Toc5809842)

[Works Cited 11](#_Toc5809843)

# Intrusion Tools and Techniques

## Intrusion Detection

Being that a company’s systems, servers, and networks contain their most important and valuable data, there has to be ways to prevent intrusion and know when it is happening. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can work hand in hand to tell when an attack is or was attempted and then stop it with minimal to no damage done. These systems are able to do this by monitoring traffic and either actively preventing it or alerting system admins (“Security: IDS vs. IPS Explained”, 2014).

### Intrusion Detection/Prevention Systems

An IDS constantly monitors traffic on the network and, based on anomalies, is able to determine when or if an attack is being attempted. An anomaly can either be a packet that is not normal traffic (if the IDS is behavior based) or something that doesn’t conform to the rules for allowed traffic (“Security: IDS vs. IPS Explained”, 2014). Once the IDS believes that an attack is occurring it is able to alert to the intrusion to allow for countermeasures to be taken against the issue. While an IDS does not directly act upon a threat, it is like a neighborhood watch program that looks for suspicious activity and then alerts the authorities or in this case systems admins and/or programs that do deal with threats.

An IPS on the other hand handles the attack and actually attempts to prevent it (“Security: IDS vs. IPS Explained”, 2014). The IPS is set in place to prevent certain packets from gaining access to the network or system. These systems detects and then attempts to actively prevent the attack (“Security: IDS vs. IPS Explained”, 2014). The best way to simply explain an IPS is as a customs agent. The IPS checks the incoming traffic for potentially harmful packets and turns them away if they are suspicious or raise any kind of red flag. An IPS is also sometimes able to "grab" the intruder and trap them for identification purposes. This would be considered intrusion deflection. This is a way to make an intruder think they have gained access by putting them into a controlled environment, or honeypot, to keep them busy so that they can be identified (Gupta, 2018).

## Auditing

According to Gadi Eichhorn, a data audit is a process by which data quality and/or utility are carefully assessed. This requires the use of key metrics rather than the quantity of data to determine the overall quality of the dataset being audited. This is essentially a process where every step of the data handling and manipulation process is carefully examined to ensure that all data is of the highest possible quality.

One of the largest issues in data quality, and most important things to take into account during a data audit, is human error. Humans cannot be perfect, therefore there is a certain degree of error to be expected when we are the point of entry for most data sets. It was found that the human error rate can be as high as 10% (Eichhorn, 2014). This can be extremely problematic for a company due to its effect on customer service and even legal proceedings. By accounting for humans, it can become much easier to catch errors in data during an audit and continuously improve the quality by correcting for mistakes that the non-machines may not be able to find otherwise (Eichhorn, 2014). Although other factors can cause inaccuracy, this is one of the largest causes. Just because it was collected and reviewed, does not mean it is 100% accurate. It is entirely possible for mistakes to be overlooked or hidden from the auditors and their tools. In other words, there is never a guarantee of 100% accuracy and security of data.

### Audit Data Storage

Due to the sensitive nature of audit data, the log files and related data should be stored on a separate and hardened server (Gupta, 2018). By using a separate server for storage, it becomes more difficult to gain access to the data without proper permissions. It is also a good idea to configure these servers to shut down if there are any difficulties within the system or if the server becomes full (Gupta, 2018). If the server shuts down when difficulties are encountered, then it should shut down if an intruder attempts to gain access to alter logs and cover their tracks.

### Audit Data Purpose

The data obtained from an audit can be used for many purposes. According to Gadi Eichhorn, the audit data is used to:

* “Ensure the end-to-end integrity of data activities by identifying when modifications are made.”
* “Detect and analyze intentional and accidental breaches in user behavior.”
* “Monitor and analyze the database activities of any user.”
* “Keep track of changes and updates made to data.”

These results can then be used as evidence in a legal case, to determine whether an employee is capable of performing their duties, or to help remedy any problematic protocols and improve security. In the end the audit data is used to help protect and improve the company’s data handling.

## Audit Data Review

### When to Conduct an Audit

While many times an audit may be conducted because of a breach, but this should not be the case if best practices are followed. It is much better to conduct an audit regularly to keep security practices up to date and effective against the everchanging world of technology (Fennelley, n.d.). This will greatly reduce the likelihood of a successful attack occurring and keep clients/investors at ease. Invested parties ease of mind is consequentially another reason an audit may be conducted. Many times, a party may request to see the results of a current audit before agreeing to do business with the company (Fennelley, n.d.). If the audit results are not satisfactory, deals may fall through giving more reason to conduct audits regularly.

### How to Review Audit Data

To get the most out of an audit the review of the data must be thorough and specific to the company. A generalized approach or checklist signifies an ineffective audit and auditor that does not take the weight of the situation seriously (Fennelley, n.d.). Starting the audit by reviewing the company’s security policies gives a foundation of what is and isn’t acceptable risk. This sets a standard to compare the current risks to and to begin suggesting remedies to the current policies. Carole Fennelly states that the auditor should also use experts on particular areas of the systems to find more specific issues as well as a lineup of reputable tools. If this is done, the reports should then be detailed and contain the auditor’s interpretation of the findings as they relate directly to current policies, including suggested remedies to currently perceived problems (tech target).

The audit report should allow the company to determine which fixes are essential and which ones are less pressing. To make these decisions they must look at effect the problems may have on the company. Whether it be possible legal trouble, monetary losses, impact on reputation, etc. (Fennelley, n.d.). All of which should be outlined and easily reviewable by the IT team and their superiors in any report conducted by a quality auditor.

# Common Vulnerabilities and Exposures

## Definition of CVE

## In vulnerability assessment and management, vulnerabilities must be identified before they can be mitigated. To assist the team with threat identification, there is a catalog called the Common Vulnerabilities and Exposures (CVE). The CVE catalog is sponsored by the U.S. Department of Homeland Security (DHS) and is comprised of known security threats (“What is Common Vulnerabilities and Exposures (CVE)?”, 2015). The threats found in the catalog are categorized as vulnerabilities and exposures (“What is Common Vulnerabilities and Exposures (CVE)?”, 2015). According to Margaret Rousse, a vulnerability, for the sake of the CVE, is defined as “a mistake in software code that provides an attacker with direct access to a system or network,” while an exposure would be the same except it provides a hacker with indirect access to a system or network rather than direct access. The great thing about the CVE is that it allows administrators to quickly and easily access technical information about a threat (“What is Common Vulnerabilities and Exposures (CVE)?”, 2015).

## Calculation of CVSS

### What is CVSS?

CVSS stands for Common Vulnerability Scoring System. It is a framework designed to allow organizations to measure and score vulnerabilities numerically so that they can be more easily prioritized (“VULNERABILITY METRICS”, N.D.). The system provides accurate and consistent impact scores to be used in the calculation of the severity of vulnerabilities discovered on a system (“VULNERABILITY METRICS”, N.D.).

### How it is Calculated

CVSS is calculated using three separate severity rating scores along with a specific algorithm (“What is CVSS (Common Vulnerability Scoring System)?”, 2016). Those 3 scores, or metrics, are base (deals with inherent qualities of a vulnerability), temporal (represents the qualities of a vulnerability that change over time), and environmental (represents the vulnerabilities qualities that are specific to the user’s environment) (“What is CVSS (Common Vulnerability Scoring System)?”, 2016). The difference between the base and temporal scores is that the temporal is affected by external events while the base deals solely with the qualities directly related to the vulnerability (“VULNERABILITY METRICS”, N.D.). These scores range from 0.0 to 10.0 with the higher score being the most severe (“What is CVSS (Common Vulnerability Scoring System)?”, 2016). The NVD (National Vulnerability Database) breaks the scores down into ranges of low (0.0 – 3.9), medium (4.0 – 6.9), and high (7.0 – 10.0).

### My Company

In my company, like most, we have a website which indirectly uses WordPress. According to CVSS, there is a vulnerability (CVE-2019-10637) with WordPress that allows attackers to become an admin by changing the email address on the profile and then resetting the password with a simple forgotten password link (“Security Vulnerabilities (CVSS score between 9 and 10)”, n.d.). This is particularly worrisome because with very little effort someone can easily take over the company’s website. The company is also vulnerable to CVE-2019-0856 that allows remote code execution if Windows improperly handles objects in memory (“Security Vulnerabilities (CVSS score between 9 and 10)”, n.d.). This is particularly dangerous due to how easily a windows system can become overloaded in the typical work environment causing mishandling of memory objects. A similar vulnerability (CVE-2019-0828) exists in the Excel software when memory objects are handled properly (“Security Vulnerabilities (CVSS score between 9 and 10)”, n.d.). In a business that relies on spreadsheets this can be problematic, but easily fixed by using a different spreadsheet software.

## The use of NVD

The NVD is a database that works alongside the CVSS to provide calculated scores for many vulnerabilities, but currently only provides base scores (“VULNERABILITY METRICS”, N.D.). This is particularly important to understand because most organizations use the CVSS and the NVD helps break it down even more for easy classification of scoring. NVD is tool used for security management and compliance in order to help understand CVSS vulnerability scores and rankings (“VULNERABILITY METRICS”, N.D.).

# Attack Methods

TBD

# Intrusion Detection System Policies

TBD

# Protective Measures

TBD

# Works Cited

Eichhorn, G. (2014, October 14). Why exactly is data auditing important? Retrieved April 10, 2019, from https://www.realisedatasystems.com/why-exactly-is-data-auditing-important/

Fennelley, C. (n.d.). IT security auditing: Best practices for conducting audits. Retrieved April 10, 2019, from https://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits

Gupta, A. (2018, August 16). What are Honeypots and how can they secure computer systems. Retrieved April 10, 2019, from https://www.thewindowsclub.com/what-are-honeypots

Rouse, M. (2015, April). What is Common Vulnerabilities and Exposures (CVE)? Retrieved April 17, 2019, from https://searchfinancialsecurity.techtarget.com/definition/Common-Vulnerabilities-and-Exposures

Rouse, M. (2016, August). What is CVSS (Common Vulnerability Scoring System)? Retrieved April 17, 2019, from https://searchsecurity.techtarget.com/definition/CVSS-Common-Vulnerability-Scoring-System

Security: IDS vs. IPS Explained. (2014, March 18). Retrieved April 10, 2019, from https://www.comparebusinessproducts.com/fyi/ids-vs-ips

Security Vulnerabilities (CVSS score between 9 and 10). (n.d.). Retrieved April 17, 2019, from https://www.cvedetails.com/vulnerability-list/cvssscoremin-9/cvssscoremax-10/vulnerabilities.html

Vulnerability Metrics. (n.d.). Retrieved April 17, 2019, from https://nvd.nist.gov/vuln-metrics/cvss