CSS300 Vulnerability Assessment and Management

Vulnerability Assessment Project

Hunter Morrison

April 2, 2019

Table of Contents

[Intrusion Tools and Techniques 3](#_Toc5788673)

[Common Vulnerabilities and Exposures 4](#_Toc5788674)

[Attack Methods 5](#_Toc5788675)

[Intrusion Detection System Policies 6](#_Toc5788676)

[Protective Measures 7](#_Toc5788677)

# 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 (compBus).

### 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 (compBus). 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 (compBus). The IPS is set in place to prevent certain packets from gaining access to the network or system. These system detects and then attempts to actively prevent the attack (compBus). 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 (windowsClub).

## 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% (RealiseDS). 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 (RealiseDS). 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 (museSecTool). 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 (museSecTool). If the server shuts down when difficulties are encountered then it should shut down if and intruder attempts to gain access to alter logs and cover their tracks.

# Common Vulnerabilities and Exposures

TBD

# Attack Methods

TBD

# Intrusion Detection System Policies

TBD

# Protective Measures

TBD

# Works Cited

<https://www.comparebusinessproducts.com/fyi/ids-vs-ips>

<https://www.thewindowsclub.com/what-are-honeypots>

<https://www.realisedatasystems.com/why-exactly-is-data-auditing-important/>