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

# 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>

<http://www.oneilrisk.com/articles/2017/1/24/what-is-a-data-audit>