**Vulnerability Assessment and Management**

**[Robert Green]**

CSS300-2205B-02

Instructor: Mark Ford

**[07/02/24]**

Table of Contents

[Section 1: Intrusion Tools and Techniques 3](#_Toc121332092)

[Section 2: Common Vulnerabilities and Exposures 4](#_Toc121332093)

[Section 3: Attack Methods 5](#_Toc121332094)

[Section 4: Intrusion Detection System Policies 6](#_Toc121332095)

[Section 5: Protective Measures 7](#_Toc121332096)

[Conclusion 8](#_Toc121332097)

[References 9](#_Toc121332098)

# Section 1: Intrusion Tools and Techniques

Section 2: Common Vulnerabilities and Exposures

CSSV:

The mission is to identify, define, and catalog

Vulnerabilities. It is a worldwide partnership that

Finds and assigns vulnerabilities. These communications

Are reliable description, CISO use this to make sure that they are talking about the same thing, They effectively produce

Synchronized efforts to categorize these risks.

Descriptions:

Base Metric Group, Temporal metric group, and Environmental metric group.

In the security profession is necessary to be able to recognize risk on way to do this is CSVV Score

This is way to look at risk essentials and produce a score for this. This can be represented in graphs as high, low and medium to help CISO to prioritize Vulnerabilities.

There are to many vulnerabilities and not enough resources

To address them all.

CSSV: score has three groups:

1)Base: including inherent and unchanging characteristics

Attack vector, attack complexity, privileges, User Interaction, Scope, CIA.

2)Temporal: Characteristics that change over time

Exploit code Maturity, remediation level, report confidence

3) Environmental: Characteristics that depend on a vulnerability context

These scores range from 0-10:

ANYLYSIS TO GET THE METRICS AND VALUES, YOU THEN ENCODE THESE AS METRIC STRING.

CVSS: 3.1/AV:/AC: L/PR:N/UI:N/S:U/C:H/I:/A:H

ADD THE TEMPRAL SCORE TO THE ENVORMENTAL SCORE

NVD: is a us government project that was created to help individuals and companies research the automation of vulnerabilities.

SQL injection is an example of High CSSV

# Section 3: Attack Methods

Passive attacks are attacks that are not active like Listing, Dumpster diving and packet sniffing.

Active attacks include Trojan horses, DOS, SQL injection and Malware, Bots,

These are used to incept or gain access to information or to take over ones system.

A passive attack would be when a person or cooperation I has a lot of paper files and the such drives or disk that are old or not useable for the consumer any more this person, decides to throw it away, a Dumpster Diver is a person who goes though you trash to find information that might help them to gain Unauthorized access to on information.

Another from of this is when a actor uses a packet sniffer to analysis traffic on the computer, Lastly there is also Social engineering this is when the actor calls or tries to act like they are the user to gain information so that may Authorize access to ones information.

A person may use a bot to communicate with a controller on port 80 so that they may gain access to through an internet chat protocol, Bot tunnels and this is how they avoid detection, They will control the bot and tell it to do anything. Bots can use controllers to vulnerabilities using controls or trojen horses. Bots have been linked to organized crime, by sending out bots who have malware in there code to get user to press links or communicate in passive attack to preform an active attack.

# Section 4: Intrusion Detection System Policies

|  |
| --- |
| **Week 4** Please populate this Section for **Unit 4** Individual Project –  The project is going well so far, and the analysis and discussion of the vulnerabilities was well-received. You realize that when vulnerability scanning takes place, employees need to know what the expectations are for handling the findings. You want to ensure that the policies and expectations for action are in place. Discuss the following:   * \*\*REFER TO YOUR COMPANY\*\* * The purpose of a policy * Create a policy for your organization that will cover one of the following (choose just 1):   + Intrusion Detection   + Incident Handling   + Vulnerability Assessment and Handling * Your Policy Heads should be:   + Overview   + Scope   + Policy   + Enforcement   + Definitions   + Revision History   Add the discussion about the definition of a policy and the sample policy to the section titled: **Intrusion Detection System Policies.**  *\*Delete this gray box before turning in this Section. \** |

# Section 5: Protective Measures

|  |
| --- |
| **Week 5** Please populate this Section for **Unit 5** Individual Project –  The management team as well as your peers are happy with the work performed to this point:   * Setting up Intrusion Detection Systems and audit data. * Defining and understanding vulnerabilities * Identifying various attack mechanisms * Creating a policy   The last and final step is to perform a vulnerability assessment against a workstation, server or combination and analyze the findings. Recommend the solutions to remediate any serious issues based on the established company policies.  It is important to know and understand the security posture of the devices attached to the network, as these might often be a step in a more sophisticated and multilevel attack of the infrastructure. An important step in the risk management process is to determine what vulnerabilities exist on these devices. Choose a vulnerability assessment tool and perform a vulnerability assessment against your target(s) in your environment, and report the findings. The information should include:   * \*\*REFER TO YOUR COMPANY\*\* * A description about the tool used to perform the scan. * A list of identified hosts (Obfuscate any specific IP addresses). (Screen Shot) * The list of serious (on a scale of 1-5 (1 being the highest) report the 1 and 2 issues) * Describe or list any false positive information. * Discuss potential safeguards and remediation actions that could be implemented for each finding to reduce the risk.   *\*Delete this gray box before turning in this Section. \** |

# Conclusion

# References