Lab #5: How to Identify Risks, Threats & Vulnerabilities in an IT Infrastructure using Zenmap GUI (Nmap) & Nessus Reports

Course Name: IAA202

Student Name: Dang Hoang Nguyen

Lab Due Date: June, 6 2023

Learning objectives and outcomes

Upon completing this lab, students will be able to:

- Review a Zenmap GUI (Nmap) network discovery and port scanning report and a Nessus software vulnerability report from a risk management perspective
- Identify hosts, operating systems, services, applications, and open ports on devices from the Zenmap GUI (Nmap) scan report from a risk management perspective
- Identify critical, major, and minor software vulnerabilities from the Nessus vulnerability assessment scan report
- Assess the exploit potential of the identified software vulnerabilities by conducting a high-level risk impact by visiting the Common Vulnerabilities & Exposures (CVE) online listing of software vulnerabilities at http://cve.mitre.org/
- Craft an executive summary prioritizing the identified critical and major threats andvulnerabilities and their risk impact on the IT organization

Required setup and tools

- **Zenmap GUI (Nmap):** https://nmap.org
- **Nessus Vulnerability Assessment:** https://www.tenable.com/products/nessus (trial professional version)

Lab Assessment Questions

1. What are the differences between Zenmap GUI (Nmap) and Nessus?

   Zenmap GUI is a graphical user interface for the popular Nmap command-line network scanner. It allows users to scan networks by sending packets to target hosts and analyzing the responses. Zenmap provides a variety of options for customizing scans, such as specifying ports, timing, and output formats. Zenmap is primarily used for reconnaissance and vulnerability assessment.

   Nessus, on the other hand, is a comprehensive vulnerability scanner that can detect and report on a wide range of security issues, including vulnerabilities in operating systems, applications, and network services. Nessus performs both active and passive scanning techniques to identify vulnerabilities and misconfigurations. Nessus offers advanced features like compliance checks, risk assessments, and customizable reporting.

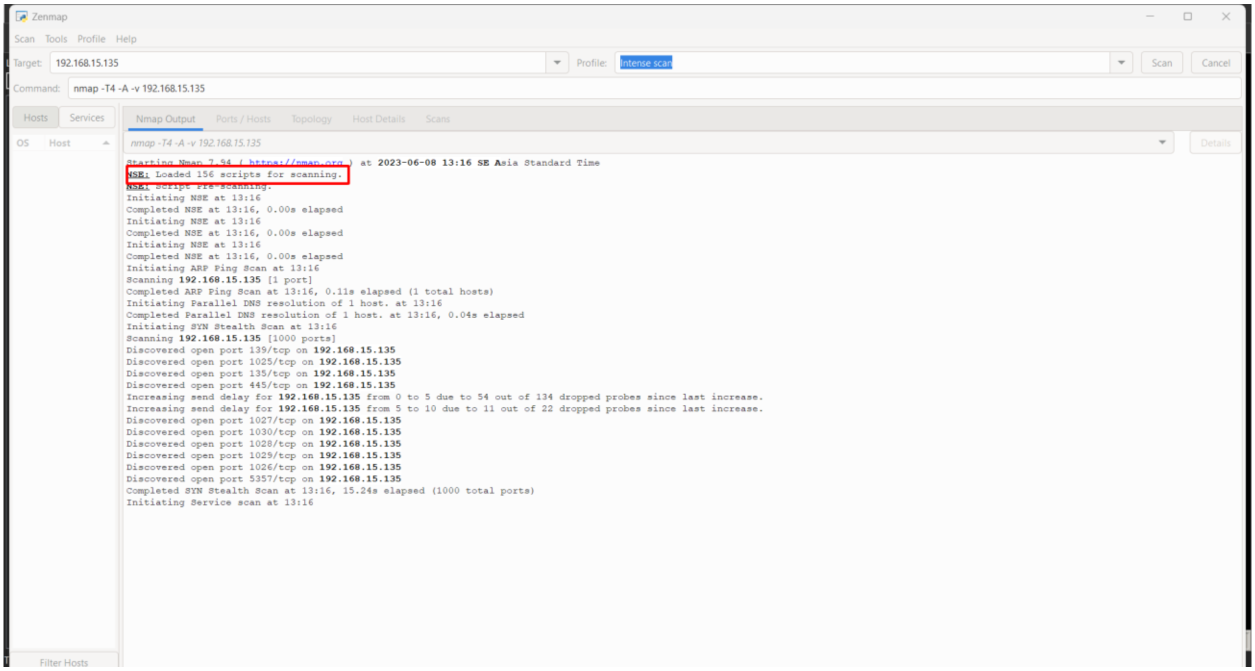
2. Which scanning application is better for performing a network discovery reconnaissance probing of an IP network infrastructure?

   I suppose that Zenmap is used to performing a network discovery reconnaissance better because we can use lots of command to scan port of the IP network infrastructure

3. Which scanning application is better for performing a software vulnerability assessment with suggested remediation steps?

   Nessus offers a wide range of advanced features such as customizable scan policies, support for multiple operating systems, integration with other security tools, and detailed reporting capabilities, which makes it one of the most popular vulnerability scanners in the market. So I think that Nessus is better

4. How many total scripts (i.e., test scans) does the Intense Scan using Zenmap GUI perform?
   For scanning by Intense Scan using ZenMap Gui, wwe can see that ZenMap used total 156 scripts for scannning



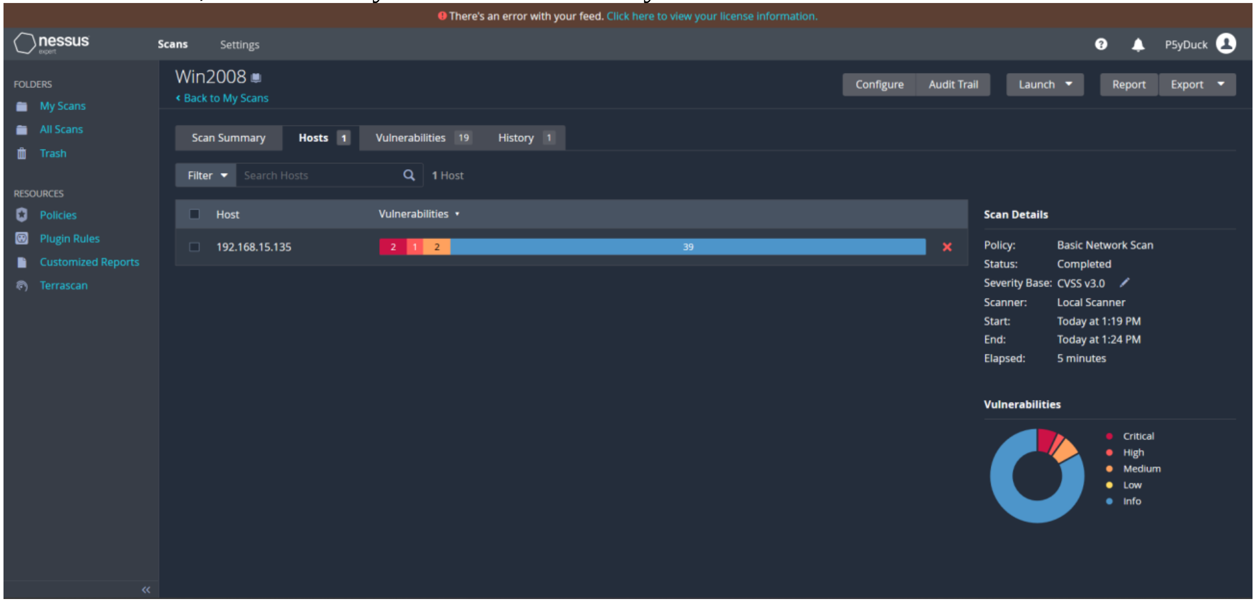
Target: 192.168.15.135

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.15.135

```
nmap -T4 -A -v 192.168.15.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-08 13:16 SE Asia Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:16
Completed NSE at 13:16, 0.00s elapsed
Initiating NSE at 13:16
Completed NSE at 13:16, 0.00s elapsed
Initiating NSE at 13:16
Completed NSE at 13:16, 0.00s elapsed
Initiating ARP Ping Scan at 13:16
Scanning 192.168.15.135 [1 port]
Completed ARP Ping Scan at 13:16, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:16
Completed Parallel DNS resolution of 1 host. at 13:16, 0.04s elapsed
Initiating SYN Stealth Scan at 13:16
Scanning 192.168.15.135 [1000 ports]
Discovered open port 139/tcp on 192.168.15.135
Discovered open port 1025/tcp on 192.168.15.135
Discovered open port 135/tcp on 192.168.15.135
Discovered open port 445/tcp on 192.168.15.135
Increasing send delay for 192.168.15.135 from 0 to 5 due to 54 out of 134 dropped probes since last increase.
Increasing send delay for 192.168.15.135 from 5 to 10 due to 11 out of 22 dropped probes since last increase.
Discovered open port 1027/tcp on 192.168.15.135
Discovered open port 1030/tcp on 192.168.15.135
Discovered open port 1028/tcp on 192.168.15.135
Discovered open port 1029/tcp on 192.168.15.135
Discovered open port 1026/tcp on 192.168.15.135
Discovered open port 5357/tcp on 192.168.15.135
Completed SYN Stealth Scan at 13:16, 15.24s elapsed (1000 total ports)
Initiating Service scan at 13:16
```

5. How many IP hosts were identified in the Nessus vulnerability scan? List them.
   In this scenario, we can easily see that there is only 1 host that is 192.168.15.135



There's an error with your feed. Click here to view your license information.

Win2008

‹ Back to My Scans

1 Host

Host	Vulnerabilities
192.168.15.135	2 1 2 39

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:19 PM
End: Today at 1:24 PM
Elapsed: 5 minutes

Vulnerabilities

6. While Nessus provides suggestions for remediation steps, what else does Nessus provide that can help you assess the risk impact of the identified software vulnerability?

   In addition to providing suggestions for remediation steps, Nessus also provides a risk score or severity level for each identified software vulnerability. This allows you to prioritize which vulnerabilities to address first based on their potential impact on your system or network. The risk score is typically based on the CVSS (Common Vulnerability Scoring System) framework, which takes into account factors such as exploitability, impact, and affected users to calculate a score between 0 and 10. A higher score indicates a greater risk, while a lower score indicates a lower risk. By using these risk scores, you can focus your attention on the most critical vulnerabilities and allocate resources accordingly to mitigate the greatest risks to your system or network.

7. Are open ports necessarily a risk? Why or why not?
   I suppose that open too many ports will make the web/ server goes into risk. For instance, in web server, opening the port such as port 22 for web server, you can access the remote control to the server or you can brute forcing ssh to get the password

8. When you identify a known software vulnerability, where can you go to assess the risk impact of the software vulnerability?

   When you identify a known software vulnerability, there are several resources you can use to assess the risk impact of the vulnerability:

   The National Vulnerability Database (NVD): The NVD is a publicly accessible database that contains information on known vulnerabilities in software products. It includes a Common Vulnerability Scoring System (CVSS) score for each vulnerability, which can help you assess the risk impact.

   The Common Vulnerabilities and Exposures (CVE) database: This is a dictionary of publicly disclosed cybersecurity vulnerabilities and exposures. Each CVE entry includes an identification number, a description of the vulnerability, and references to sources of information about the vulnerability.

   Vendor advisories and security bulletins: When a vulnerability is discovered in a product, the vendor typically issues an advisory or bulletin that provides information about the vulnerability and any available patches or workarounds. These advisories often include a severity rating or CVSS score to help customers assess the risk impact.

   Security research firms and websites: There are many independent security research firms and websites that provide information on software vulnerabilities and their risk impacts. Examples include the SANS Institute, US-CERT, and the Mitre Corporation.

9. If Nessus provides a pointer in the vulnerability assessment scan report to look up CVE-2023-25690 when using the CVE search listing, specify what this CVE is, what the potential exploits are, and assess the severity of the vulnerability.

Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

For example, something like:

```
RewriteEngine on

RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]

ProxyPassReverse /here/ http://example.com:8080/
```

Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

Acknowledgements: finder: Lars Krapf of Adobe

10. What must an IT organization do to ensure that software updates and security patches are implemented timely?

To ensure that software updates and security patches are implemented in a timely manner, an IT organization should:

1. Establish a patch management process: Implement a formal process for identifying, testing, and deploying patches and updates. The process should include procedures for prioritizing patches based on their severity and impact, testing patches before deployment, and verifying successful implementation.
2. Automate patch deployment: Use automation tools to automate patch deployment wherever possible. This can help ensure that patches are deployed quickly and consistently across all systems, reducing the risk of human error and oversight.
3. Maintain an up-to-date inventory of systems: Maintain an accurate inventory of all hardware and software systems within the organization. This can help ensure that all systems are covered by the patch management process and that no systems are overlooked.
4. Monitor vendor alerts and advisories: Stay informed about new vulnerabilities and patches by monitoring vendor alerts and advisories. This can help ensure that your organization is aware of new threats and can prioritize patch deployment accordingly.
5. Conduct regular vulnerability scans: Regularly scan your systems for vulnerabilities to identify any potential risks that may require patching. This can help ensure that your organization is aware of any existing vulnerabilities and can take action to mitigate them.
6. Educate end-users: Educate end-users about the importance of patching and keep them informed about any patches or updates that may affect their systems. This can help ensure that they are aware of the risks and can take appropriate action to protect their systems.

11. Write a four-paragraph executive summary written to executive management providing a summary of findings, risk impact to the IT asset and organization, and recommendations for next steps.

This report provides an overview of the findings and risk impact of CVE-2023-25690, a recently identified vulnerability in our IT infrastructure. The vulnerability poses a significant threat to our organization and requires immediate attention. This report outlines the potential impact of this vulnerability and offers recommendations for next steps to mitigate the risks.

CVE-2023-25690 is a critical vulnerability that affects our organization's systems and could allow attackers to gain unauthorized access to sensitive information. The vulnerability is caused by a flaw in our system's authentication mechanism, which could be exploited by hackers to bypass security controls and gain escalated privileges on our network. The vulnerability leaves our organization open to various types of attacks, including data theft and ransomware attacks.

The risk impact of CVE-2023-25690 is severe, as it could result in unauthorized access to sensitive data and cause significant financial losses and reputational damage to our organization. Attackers could exploit this vulnerability to steal confidential information, such as customer data, employee records, and financial information. In addition, a successful attack could lead to system downtime and disrupt our operations, causing significant financial losses.

To mitigate the risks associated with CVE-2023-25690, we recommend taking immediate action to patch all affected systems and verify that the patch has been applied correctly. We also recommend reviewing our authentication mechanisms and implementing additional security controls, such as two-factor authentication and user behavior analytics, to prevent similar vulnerabilities from arising in the future. Additionally, we should conduct regular vulnerability assessments and penetration testing to identify and remediate any other potential vulnerabilities in our IT infrastructure.

In conclusion, the identification of CVE-2023-25690 highlights the critical importance of maintaining a secure and well-maintained IT infrastructure. Failure to address this vulnerability could result in significant financial losses and reputational damage to our organization. It is essential that we take immediate action to patch affected systems and implement additional security controls to prevent similar vulnerabilities from arising in the future. Regular vulnerability assessments and penetration testing should be conducted to identify and remediate any other potential vulnerabilities.