# Nama : Mochammad Aldo Rizky

# Nim : 2141762002

# Kelas : SIB-4C

# Lab - Evaluate Vulnerabilities

## Objectives

In this lab, we will review the features of an example of a penetrating testing vulnerability report.

**Part 1: Learn About the Creators of a Vulnerability Assessment Report**

**Part 2: Review Sections of the Report**

## Background / Scenario

Vulnerability assessments can be conducted in-house or by external contractors. Vulnerability assessments are usually automated. Reachable network hosts are identified, and then scanned with vulnerability assessment tools. The scan creates a lot of data which maps the host IP addresses to the detected vulnerabilities. From this data, summary data and visualizations can be created to simplify interpretation of the report.

When identified, the vulnerabilities are often rated by severity, frequently using a standard means of doing so, such as CVSS. In addition, reference information is often provided to enable deeper research if required. Typically a CVE number will be provided that is easy to investigate further.

The report may suggest common mitigation techniques that provide guidance to cybersecurity personnel about how to eliminate the vulnerabilities that have been identified.

## Required Resources

- Computer with internet access
- Sample vulnerability assessment report

## Instructions

## Part 1: Learn About the Creators of a Vulnerability Assessment Report

### Step 1: Research the report source.

The report that we will use for this lab was created by the NCATS Cyber Hygiene service.

Research NCATS on the internet and answer the following questions.

What does NCATS stand for?

NCATS stands for National Cybersecurity Assessments and Technical Services. This program is part of the Cybersecurity and Infrastructure Security Agency (CISA) and focuses on helping organizations improve their cybersecurity posture through assessments, guidance, and services..

**National Cybersecurity Assessments and Technical Services**

What is the Cyber Hygiene Vulnerability Scanning Service? Search the web for details.

The Cyber Hygiene Vulnerability Scanning Service is a free vulnerability assessment service provided by the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security. This service helps organizations identify and remediate vulnerabilities in their networks and systems.

Key features of the service include:

Regular Scanning: The service offers automated scans of external IP addresses to detect vulnerabilities that could be exploited by attackers.

Detailed Reports: Organizations receive reports that detail identified vulnerabilities, their severity, and recommended remediation actions.

Guidance and Support: CISA provides assistance in interpreting scan results and implementing necessary security improvements.

Targeted to Organizations: The service is particularly beneficial for federal, state, local, tribal, and territorial government entities, as well as critical infrastructure organizations..

**It is a free vulnerability assessment service that is provided by the Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of Homeland Security.**

What other cybersecurity services are available from NCATS?

In addition to the Cyber Hygiene Vulnerability Scanning Service, NCATS (National Cybersecurity Assessments and Technical Services) offers several other cybersecurity services, including:

1. Phishing Campaign Assessment: This service evaluates an organization's susceptibility to phishing attacks by simulating phishing attempts to test employee awareness and response.

2. Risk and Vulnerability Assessment: NCATS conducts comprehensive assessments to identify and evaluate security risks and vulnerabilities within an organization's systems and processes.

3. Validated Architecture Design Review: This service reviews and validates the security architecture of systems to ensure that they meet best practices and compliance requirements, helping organizations build secure infrastructures..

**In addition to Cyber Hygiene vulnerability scanning, NCATS offers Phishing Campaign Assessment, Risk and Vulnerability Assessment, and Validated Architecture Design Review.**

Who are these services available to?

The services provided by NCATS are available to:

Federal, State, Local, Tribal, and Territorial Governments: This includes various government entities at all levels within the United States.

Public and Private Sector Critical Infrastructure Organizations: These are organizations that are vital to the functioning of the nation's economy and security, which may include sectors such as energy, transportation, healthcare, and finance.

**Federal, state, local, tribal, and territorial governments, and public and private sector critical infrastructure organizations in the USA.**

## Step 2: Locate and open the report.

a. The link to the report that we will review is directly under the Cyber Hygiene: Vulnerability Scanning section of the NCATS page. To access the link from the Google search engine, enter the following: **site:us-cert.cisa.gov/ CyHy** .

b. Open the report and review the table of contents to get an idea of what is included.

## Part 2: Review Sections of the Report

The first two sections of the report explain its intended use and provide a high-level dashboard-like overview of the report results.

### Step 1: Review the How to Use the Report section.

It is important to understand the intended use of any security assessment report. A good report will provide useful and focused guidelines for use of the assessment.

**Note:** Because this report is an example, the organization that the report was prepared for is referred to as Sample Organization (Sample).

Review section one of the report and answer the following questions.

What is the goal of the report?

The services provided by NCATS are available to:

Federal, State, Local, Tribal, and Territorial Governments: This includes various government entities at all levels within the United States.

Public and Private Sector Critical Infrastructure Organizations: These are organizations that are vital to the functioning of the nation's economy and security, which may include sectors such as energy, transportation, healthcare, and finance..

**To help organizations strengthen their security posture.**

In what section of the report can you find a high-level overview of the assessment results including some comparisons of weekly performance?

The detailed list of findings and recommended mitigations for each vulnerability can be found in the Vulnerabilities section of the report. This section provides specific information on identified vulnerabilities, their severity, and actionable steps for mitigation.

**Cyber Hygiene Report Card**

Where can you find a detailed list of findings and recommend mitigations for each vulnerability?

**Appendix C**

What allows you to easily open the results of the scan into a spreadsheet or other tabular document?

The Comma-Separated Values (CSV) files provided in Appendix G allow you to easily open the scan results in a spreadsheet or other tabular document. These CSV files enable straightforward analysis, sorting, and filtering of data related to identified vulnerabilities and assessment findings

**In Appendix G, Comma-Separated Values (CSV) files are provided for this purpose.**

### Step 2: Review the Cyber Hygiene Report Card.

Look at the Cyber Hygiene Report Card. This provides a high-level summary of the results of the assessment. This organization is scanned weekly, so there is some trend information that is supplied with the results of the current scan.

What percent of the scanned hosts were found to be vulnerable? How does this compare to the previous scan?

In the Cyber Hygiene Report Card, 10% of the scanned hosts (or 393 hosts) were found to be vulnerable. This reflects an improvement, as it is 44 hosts fewer than in the previous scan.

**10%, or 393, hosts were found to be vulnerable. This is 44 hosts fewer than the previous scan.**

Vulnerabilities are classified by severity. Which level of severity represents the highest number of newly vulnerable hosts?

The medium severity level represents the highest number of newly vulnerable hosts, with an additional 108 hosts newly identified as having vulnerabilities at this level.

**An additional 108 hosts were newly identified as having medium severity vulnerabilities**.

Which class of vulnerability requires the most time for the organization to mitigate?

The medium level vulnerabilities require the most time for the organization to mitigate, with a mean time of 158 days.

**It takes the organization a mean time of 158 days to mitigate a medium level vulnerability.**

The scan included 293,005 IP addresses, but assessed only 3,986 hosts. Why do you think this is?

The scan included 293,005 IP addresses, but only 3,986 hosts were assessed because, although the Sample Organization provided access to a large address space, only 3,986 IPs were active and reachable at the time of the scan. This means the remaining IP addresses were likely inactive or not in use during the assessment period.

**The Sample Organization provided access to an address space of 293,005 addresses, but at the time of the scan, only 3,986 were active and reachable for the scan.**

## Step 3: Review the Executive Summary.

Go to the Executive Summary. Read this section and answer the following questions.

What two major functions did the assessment include, and which hosts did it assess?

The assessment included two major functions:

1. Network Mapping: This function was used to identify active hosts and gather information about the network.
2. Vulnerability Assessment: This was conducted on internet-accessible hosts that were identified during the network mapping phase.

**The assessment conducted network mapping to identify hosts and other information, and vulnerability assessment of internet-accessible hosts that were found during mapping.**

How many distinct types of vulnerabilities were identified?

A total of 63 distinct types of vulnerabilities were identified in the assessment.

**63**

Of the top five vulnerabilities by occurrence, what was common system or protocol was most often found to be vulnerable?

Among the top five vulnerabilities by occurrence, SSL certificates and cipher suites were the most commonly found to be vulnerable.

**SSL certificates and cipher suites.**

Of the top five categories by degree of risk, which vulnerabilities appear to be related to a specific piece of network hardware? What is the device?

Among the top five vulnerabilities by occurrence, SSL certificates and cipher suites were the most commonly found to be vulnerable.

**MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary. It is a MikroTik router**.

Search the web on “MikroTik Router OS 6.41.3 SMB.” Locate the CVE entry for this vulnerability on the National Vulnerability Database (NVD) website. What is the CVSS base score and severity rating?

The CVSS base score for the MikroTik Router OS 6.41.3 SMB vulnerability (CVE-2018-7445) is 9.8, with a severity rating of critical.

**CVSS base score 9.8, rating critical (CVE-2018-7445).**

Locate the full disclosure report for this CVE by searching on the web or clicking a reference link. In the full disclosure report, what are two ways of mitigating the vulnerability?

In the full disclosure report for CVE-2018-7445 found on the Seclists.org website, two ways to mitigate the vulnerability are:

1. Update RouterOS: Upgrade to RouterOS version 6.41.3 or higher to address the vulnerability.
2. Disable SMB Service: Disable the Server Message Block (SMB) service to prevent exploitation of the vulnerability.

**The full disclosure report is found on the Seclists.org website. Item 5 says that the RouterOS should be updated to version 6.41.3 or higher, or the Server Message Block (SMB) service should be disabled.**

What type of vulnerability is this, and what can an attacker do when it is exploited?

The vulnerability is a buffer overflow. When exploited, attackers can execute arbitrary code on the system because authentication is not required to exploit the vulnerability. This allows them to potentially take control of the affected system, leading to unauthorized access and manipulation of sensitive data or system functions.

**It is a buffer overflow. Attackers could easily execute code of the system because the user does not need to be authenticated to exploit it.**

What should the Sample Organization have done to prevent this critical vulnerability from appearing on their network?

To prevent this critical vulnerability from appearing on their network, the Sample Organization should have:

Followed Product Advisories: Regularly monitored and adhered to product advisories and security updates for their network hardware, specifically for RouterOS.

Timely Updates: Once informed of the vulnerability, they should have acted promptly to update their RouterOS version to a secure release (6.41.3 or higher) to mitigate the risk of exploitation.

**They should have been following product advisories for their network hardware. After they were informed of the vulnerability, they should have updated the RouterOS version as quickly as possible.**

## Step 4: Review assessment methodology and process.

It is important to evaluate the methodology that was used to create a vulnerability assessment to determine the quality of the work that was done. Review the material in that section of the report.

In the Process section, the report mentions an IP network from which the scan was performed. What is the IP network, and to whom is it registered? Why is important to tell this to Sample Organization?

The IP network mentioned in the report is 64.69.57.0/24, which is registered to the US Department of Homeland Security.

It is important to communicate this information to the Sample Organization for several reasons:

1. Reconnaissance Concerns: Since the vulnerability assessment process involves deep scanning of the organization's network, the use of an IP address registered to a government agency could be misinterpreted as a reconnaissance attack by a threat actor. This could cause unnecessary alarm within the organization.

2. Mitigation Responses: If the Sample Organization mistakenly perceives the scanning activity as a threat, they might take actions such as blocking the entire IP range at their network edge, which could inadvertently prevent legitimate assessments from occurring.

3. Firewall Configuration: To ensure the scan is successful, the organization may need to configure their firewall settings to allow traffic from this IP network. Without this, connections originating from the scanning IP may be blocked, leading to incomplete assessments and undetected vulnerabilities.

**64.69.57.0/24. Various IP address lookup sites report that this IP network is registered to the US Department of Homeland Security. Because the vulnerability assessment process performs deep scanning of the organization network, this could be interpreted as a reconnaissance attack from a threat actor. The organization could accidentally attempt to mitigate the threat by blocking the IP addresses in that network at the network edge. In addition, for the scan to be successful, addresses from this network may need to be allowed access through a firewall for connections originating from outside the network.**

What qualifies a computer to be designated as a host for the purposes of this report?

In the context of this report, a computer qualifies to be designated as a host if it is defined as a device with an address that has at least one open or listening service running. This means that the device is actively participating in the network and can communicate with other devices, making it a target for potential assessments and vulnerability scans.

**A host is defined as a device with an address that has at least one open or listening service running.**

Which tool did the scan use for network mapping? Which tool was used for vulnerability assessment?

The scan used Nmap for network mapping and Nessus for vulnerability assessment. These tools allowed the assessment to identify active hosts and detect potential vulnerabilities on the network.

**Nmap was used for network mapping and Nessus was used for vulnerability scanning.**

Who offers the Nessus product, and what is the limitation of the freely downloadable version of Nessus?

The Nessus product is offered by Tenable. The freely downloadable version of Nessus, known as Nessus Essentials, is limited to scanning only 16 IP addresses. This version is intended for personal or small-scale use, while broader enterprise needs require a licensed version.

**Tenable provides the Nessus product. The free version is limited to scanning only 16 IP addresses.**

Vulnerabilities with what range of CVSS scores are labelled as being of “High” severity?

Vulnerabilities with a CVSS base score of 7.0 to 10.0 are labeled as being of High severity.

**Vulnerabilities with a CVSS base score of 7.0-10.0**

### Step 5: Investigate detected vulnerabilities.

Go to section 7 of the report and locate Table 6. The Vulnerability Names consist of a standard descriptive phrase. Select a description and search for it on the web. You should see a link to tenable.com for each of them. Tenable maintains reference pages for the vulnerabilities that can be detected by Nessus.

a. Open the reference page for the vulnerability and review the information that is provided to you by Tenable. Read the synopsis and description for the vulnerability. Some reference pages provide suggested mitigation measures.

b. Select three of the vulnerabilities from the top vulnerabilities list and repeat this process. Review the vulnerability, CVE number, description, and mitigation measures, if any. Investigate the vulnerability further if you are interested.

### Step 6: Investigate vulnerability mitigation.

Go to Appendix C of the report. Mitigation techniques are listed for many of the detected vulnerabilities. Answer the following questions.

What is the IP address of the host that is running a vulnerable PHP service? Why do you think this vulnerability exists on this host?

The IP address of the host running a vulnerable PHP service is x.x.124.231. This vulnerability likely exists because the host's software has not been updated. It appears that patch management and update services are either not in place or not effectively used for this host, which leaves it susceptible to known vulnerabilities.

**x.x.124.231. The host requires its software to updated. Apparently patch management and update services are not used for the host.**

What should be done to mitigate this vulnerability?

To mitigate this vulnerability, the PHP service software should be updated to version 5.6.34 or higher. This update will address the known security issues in the current version and reduce the risk of exploitation.

**Update the PHP service software to version 5.6.34 or higher.**

There are many problems that are associated with SSL. What are some of the mitigation measures that are recommended in the report?

The report recommends several mitigation measures to address problems associated with SSL:

Force the Use of SSL for certain protocols to secure data in transit.

Purchase or Generate Proper Certificates for services to ensure authenticity and trust.

Replace Expired Certificates promptly to maintain secure communication.

Configure Applications to Use Strong Ciphers to protect against cryptographic attacks.

Replace SSL 2.0 or 3.0 with TLS 1.1 or Higher, as TLS offers improved security over outdated SSL versions.

- **Force the use of SSL for some protocols.**
- **Purchase or generate proper certificates for services.**
- **Replace expired certificates.**
- **Configure applications to use appropriate strength cyphers.**
- **Replace SSL 2.0 or 3.0 with TLS 1.1 or higher.**

## Reflection Questions

1. Describe the vulnerability assessment that was conducted by NCCIC, including how it was performed, the tools used and a brief description of the results.

The NCCIC conducts a remote, periodic vulnerability assessment as a free service for qualified government and private sector organizations. The assessment is designed to identify network vulnerabilities and provide beneficiaries with reports that can be used for tracking weekly trends, identifying newly discovered vulnerabilities, and guiding mitigation efforts.

To perform the assessment:

Nmap is used to create a network map, identifying active hosts.

Nessus then scans these identified hosts to detect vulnerabilities.

**NCCIC provides a free service of vulnerability scanning for qualified government and private sector organizations. Scanning is done remotely, and periodically. Reports of the results are available to beneficiaries. The reports can be used to discover vulnerabilities, prepare weekly trends and updates, and guide in mitigation of vulnerabilities. NCCIC uses Nmap to create a network map in which hosts are identified, and Nessus to scan the identified hosts for vulnerabilities. The reports include numerous details, tables, and graphs to help communicate to the beneficiaries the security issues in the network that require attention. Each vulnerability is rated by severity according to its CVSS score.**

How are the Vulnerability names useful for further investigation?

Vulnerability names are valuable for further investigation because they match a reference maintained by Tenable, the company behind Nessus. This reference offers:

Detailed Descriptions: Information on each vulnerability, including potential impacts and affected systems.

Links to External Resources: Often includes links to other sources, such as official vendor advisories, for more in-depth information.

CVE Specifications: Direct links to Common Vulnerabilities and Exposures (CVE) entries for standardized vulnerability details.

CVSS Vectors: These vectors help assess the risk level, providing insights into factors like exploitability and impact.

**The vulnerability names match a reference that is maintained by the Tenable, the company that offers Nessus. The Tenable reference provides further details on the vulnerabilities and often provides links to other sources for more information. The Tenable reference also provides links to CVE specifications for the vulnerability. Tenable provides the CVSS vectors for the vulnerability as well.**

2. Provide three actions you could take based on the information provided in a Cyber Hygiene report.

Based on the information provided in a Cyber Hygiene report, three actions you could take are:

Prioritize Critical Vulnerabilities: Use the report to quickly identify and address the most critical vulnerabilities that require immediate attention to reduce risk.

Focus on Vulnerable Hosts: Identify specific hosts with multiple vulnerabilities and prioritize them for mitigation to improve overall network security.

Implement Centralized Solutions: Recommend solutions like patch management systems to proactively manage updates and reduce the occurrence of critical or high-severity vulnerabilities across the network.

**Answers will vary. Some examples are:**

- **Use the report to identify critical vulnerabilities that should be addressed immediately.**
- **Identify hosts that require mitigation measures to address vulnerabilities, especially if the host is found to have multiple vulnerabilities.**
- **Identify vulnerabilities that are shared by many hosts on the network.**
- **Recommend centralized solutions, such as patch management systems to lower the likelihood that critical or high severity vulnerabilities appear on the network.**