

Nama : Yusuf Haidar

Kelas : SIB – 4C

Absen : 21

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?

National Cybersecurity Assessments and Technical 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, provided by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), is a free service that helps organizations identify and mitigate security risks in their

internet-facing assets. It is designed to continuously scan for known vulnerabilities and weak configurations in systems that are accessible from the internet.

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?

The National Cybersecurity Assessments and Technical Services (NCATS), operated by CISA, offers a range of cybersecurity services designed to reduce risks and improve the security posture of organizations. In addition to the **Cyber Hygiene Vulnerability Scanning**, NCATS provides several other key services:

1. **Phishing Campaign Assessments:** These simulate phishing attacks to help organizations identify how vulnerable they are to email-based social engineering attacks. It tests users' ability to recognize phishing attempts and can improve cybersecurity awareness among staff.
2. **Risk and Vulnerability Assessments (RVA):** These comprehensive assessments evaluate network infrastructure through penetration testing, vulnerability scanning, and network mapping to identify and mitigate risks before they can be exploited by attackers.
3. **Remote Penetration Testing:** NCATS offers testing that mimics real-world cyberattacks to assess how well an organization's external defenses hold up against unauthorized attempts to infiltrate their networks.
4. **Red Team Assessments:** A more in-depth service, where the NCATS team simulates targeted attacks, including social engineering, to evaluate an organization's ability to detect and respond to persistent threats.
5. **Validated Architecture Design Review:** This service reviews the design and architecture of an organization's networks and systems, identifying potential weaknesses and offering recommendations for security improvements.
6. **Training and Qualification for Third Party Assessment Organizations:** NCATS provides training to organizations that assess others' cybersecurity, ensuring that third-party evaluators are equipped with the latest knowledge and techniques.

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 cybersecurity services offered by NCATS, including vulnerability scanning, phishing assessments, and penetration testing, are available to a wide range of organizations. These include:

1. **Federal, State, Local, Tribal, and Territorial (SLTT) Governments:** NCATS prioritizes governments at all levels, ensuring they have the necessary support to secure their infrastructure from cyber threats.
2. **Critical Infrastructure Entities:** This covers organizations responsible for critical sectors such as energy, healthcare, finance, water, transportation, and more. Protecting these sectors is vital due to their importance to national security and daily life.
3. **Private Sector Organizations in Critical Industries:** Companies that operate in industries deemed critical to national infrastructure, such as communications and defense, are also eligible to receive these services.

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?

Provide an organization with a comprehensive analysis of its current cybersecurity posture

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?

Executive Summary or Cyber Hygiene Report Card

Cyber Hygiene Report Card

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

Appendix C

Appendix C

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

To easily open the results of a scan into a spreadsheet or other tabular document, **CSV (Comma-Separated Values) file exports** are typically provided in the report.

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?.

10%. The hosts is 44 fewer than 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?

108 Hosts are identified as Medium Severity

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?

158 Days to mitigate the vulnerability

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?

Because the only active hosts are only 3986

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?

In the **Executive Summary** of a Cyber Hygiene report, the two major functions typically included in the assessment are:

1. **Vulnerability Scanning:** This function involves scanning the organization's internet-facing systems for known vulnerabilities. The scan identifies weak points such as outdated software, misconfigurations, and unpatched systems that attackers could exploit.
2. **Risk Assessment:** This function evaluates the severity and impact of the identified vulnerabilities. It assesses how these vulnerabilities could affect the organization's systems and overall cybersecurity posture, prioritizing the risks based on their potential impact.

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?

63

63

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

In most Cyber Hygiene reports, the **top five vulnerabilities by occurrence** typically highlight common system weaknesses or misconfigurations. A common system or protocol that is often found to be vulnerable includes:

- **Outdated Software Versions:** Many vulnerabilities stem from unpatched or outdated software.
- **Open or Misconfigured Ports:** Frequently, the **Remote Desktop Protocol (RDP)** or **Secure Shell (SSH)** may be found to be misconfigured, exposing systems to unauthorized access.
- **Common Web Application Vulnerabilities:** These include vulnerabilities in web servers or applications, such as Apache or NGINX, which are often targeted due to improper configurations or lack of updates.

The **Remote Desktop Protocol (RDP)** is commonly noted as a vulnerable protocol, as attackers frequently exploit it to gain remote access to systems. It is often associated with brute-force attacks or ransomware campaigns.

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?

MikroTik Router

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?

9.8

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?

The RouterOS should be updated and the Server Message Block service should be disabled

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?

It's called buffer overflow. Attackers can easily execute the code of the system.

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?

Should've follow the product advisories for the network hardware

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?.

64.69.57.0/24.

Importance of This Information:

- **Understanding the Source:** Knowing the source of the scan helps **Sample Organization** confirm that the assessment was conducted from a legitimate and recognized network. This can mitigate concerns about potential false positives that might arise from external traffic.
- **Risk Assessment:** It provides context regarding potential threats. If the scan originated from a trusted or well-known IP range, it indicates that the findings are less likely to be related to malicious activity. Conversely, if it came from an untrusted or suspicious source, it could indicate potential external threats.
- **Communication and Coordination:** This information can aid in communication with the network provider. If any issues arise from the scanning process, **Sample Organization** can coordinate with the entity that owns the IP address to clarify or address any concerns.

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?

Host is defined as device with address with at least one listening service running

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?

Nmap for network, Nessus for vulnerability

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?

Tenable, and only 16 Addresses

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?

With the score of 7 - 10

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.

- 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.
- 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?

x.x.124.231. Because the host don't have patch management and update service

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?

Updating the PHP Service

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?

- Enforcing the use of SSL for certain protocols.
- Purchasing or generating valid certificates for services.
- Replacing expired certificates.
- Configuring applications to use strong cipher suites.
- Upgrading from SSL 2.0 or 3.0 to TLS 1.1 or higher.

â€¢ **Force the use of SSL for some protocols.**
â€¢ **Purchase or generate proper certificates for services.**
â€¢ **Replace expired certificates.**
â€¢ **Configure applications to use appropriate strength cyphers.**
â€¢ **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 offers a complimentary vulnerability scanning service for eligible government and private sector organizations. This service involves conducting remote and periodic scans to identify vulnerabilities within their networks. To facilitate the assessment, NCCIC utilizes Nmap for network mapping, which helps in identifying hosts, and Nessus for vulnerability scanning to detect potential security issues. The comprehensive reports generated provide valuable insights into vulnerabilities, including details, tables, and graphs, which help organizations track weekly trends and guide their remediation efforts. Each identified vulnerability is rated by severity using CVSS scores, enabling organizations to prioritize the most pressing security issues. Overall, this free service supports entities in enhancing their network security posture and addressing critical vulnerabilities effectively.

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 in the reports are valuable for further investigation, as they correspond to references maintained by Tenable, the provider of Nessus. These references offer detailed information on each vulnerability, often including links to additional resources and CVE (Common Vulnerabilities and Exposures) specifications. Furthermore, they provide CVSS (Common Vulnerability Scoring System) vectors, which help organizations understand the severity and implications of the vulnerabilities more effectively. This comprehensive information is crucial for prioritizing mitigation efforts and gaining a deeper understanding of the context surrounding each vulnerability, ultimately aiding organizations in strengthening their security posture.

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, several actions can be taken to enhance security. First, **address critical vulnerabilities** by using the report to pinpoint issues that require immediate remediation to prevent potential exploitation. Second, implement **mitigation measures for affected hosts** by identifying systems with multiple vulnerabilities and taking necessary actions to secure them. Finally, consider recommending **centralized solutions**, such as patch management systems, to minimize the risk of critical or high-severity vulnerabilities appearing on the network. These steps are essential for strengthening the overall security posture and ensuring that vulnerabilities are effectively managed.

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.