Nama : Sasmita Rachmawati

Absen : 15

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.

Questions:

What does NCATS stand for?

- **NCATS stands for National Cybersecurity Assessments and Technical Services, which is a part of CISA (Cybersecurity and Infrastructure Security Agency). It**

provides technical cybersecurity assessment services to help organizations secure their networks from cyber threats.

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

- **This is a free service offered by CISA to help organizations identify vulnerabilities in their internet-facing systems. The scanning is performed regularly to detect security weaknesses that attackers could exploit.**

What other cybersecurity services are available from NCATS?

NCATS offers various services including:

- **Phishing Campaign Assessment: Tests an organization's resilience to phishing attacks.**
- **Risk and Vulnerability Assessment (RVA): Identifies and tests vulnerabilities in internal systems.**
- **Validated Architecture Design Review (VADR): Reviews the security architecture of networks and systems.**

Who are these services available to?

- **These services are available to critical infrastructure sectors, federal, state, local, tribal, and territorial governments, as well as private sector entities in the United States.**

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.

Questions:

What is the goal of the report?

- **The goal of the report is to help organizations strengthen their security posture by identifying vulnerabilities within their networks and systems and providing actionable recommendations to mitigate these risks.**

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

- **You can find a high-level overview of the assessment results, including comparisons of weekly performance, in the Cyber Hygiene Report Card section of the report.**

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

- **A detailed list of findings and recommended mitigations for each vulnerability is located in Appendix C of the report.**

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

- **The report provides Comma-Separated Values (CSV) files in Appendix G, which allow you to easily open and manipulate the scan results in a spreadsheet or other tabular formats.**

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.

Questions:

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

- **10%, or 393 hosts, were found to be vulnerable in the current scan. This represents a decrease of 44 hosts compared to the previous scan, indicating an improvement in the organization's security posture.**

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

- **Medium severity vulnerabilities represent the highest number of newly vulnerable hosts, with 108 additional hosts identified as having these vulnerabilities.**

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

- **Medium-level vulnerabilities require the most time for the organization to mitigate, with an average mitigation time of 158 days.**

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

- **The Sample Organization provided access to an address space of 293,005 IP addresses, but at the time of the scan, only 3,986 addresses were active and reachable. This means that most of the IP addresses were either inactive, not in use, or blocked, resulting in a smaller number of hosts being assessed for vulnerabilities.**

Step 3: Review the Executive Summary.

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

Questions:

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

The assessment included:

1. **Network Mapping: Identifying hosts and gathering information about the network.**
2. **Vulnerability Assessment: Scanning and evaluating the security of internet-accessible hosts found during the network mapping process.**

These functions collectively help in understanding the network structure and identifying potential security weaknesses in accessible systems.

How many distinct types of vulnerabilities were identified?

- **63 distinct types of vulnerabilities were identified during the assessment.**

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

- **SSL certificates and cipher suites were the most commonly found vulnerable systems or protocols among the top five vulnerabilities by occurrence.**

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?

- **Vulnerabilities related to MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary were identified. The specific device targeted by these vulnerabilities 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 vulnerability CVE-2018-7445 for MikroTik Router OS 6.41.3 SMB has a CVSS base score of 9.8, which is rated as Critical.**

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?

According to the full disclosure report found on Seclists.org, two ways to mitigate this vulnerability are:

1. **Update RouterOS: Upgrade to version 6.41.3 or higher.**
2. **Disable SMB: Turn off the Server Message Block (SMB) service if it is not needed.**

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

- **This is a buffer overflow vulnerability. When exploited, it allows attackers to execute arbitrary code on the affected system without needing to be authenticated, potentially giving them full control over the device.**

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

The Sample Organization should have:

- **Followed Product Advisories: Regularly monitored and adhered to security advisories related to their network hardware.**
- **Promptly Updated RouterOS: Applied updates to RouterOS as soon as the vulnerability was disclosed to ensure that their routers were protected against the exploit.**

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.

Questions:

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 is 64.69.57.0/24, which is registered to the US Department of Homeland Security. It is important to inform the Sample Organization about this because:

- **Avoid Misinterpretation: The vulnerability assessment involves deep scanning, which might be mistaken for a reconnaissance attack by threat actors. Knowing the origin helps prevent unnecessary blocking of legitimate IP addresses.**
- **Firewall Configuration: To ensure the scan is successful, the organization may need to allow access from this IP network through their firewall for connections originating from outside the network.**

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

- **A host is defined as a device with an IP address that has at least one open or listening service running. This means any device that is actively providing a service over the network, such as a web server, email server, or database server, qualifies as a host.**

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

- **Network Mapping Tool: Nmap was used to map the network and identify active hosts.**
- **Vulnerability Assessment Tool: Nessus was used to scan the identified hosts for vulnerabilities.**

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

- **Tenable offers the Nessus product. The limitation of the freely downloadable version of Nessus is that it is restricted to scanning only 16 IP addresses. For larger-scale vulnerability assessments, a paid version is required.**

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

- **Vulnerabilities with a CVSS base score between 7.0 and 10.0 are labeled as being of "High" severity.**

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.

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 on this host because the software is outdated, and there is lack of proper patch management and update services. Without regular updates, known vulnerabilities remain unaddressed, making the host susceptible to attacks.**

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. Keeping software up-to-date ensures that known vulnerabilities are patched, reducing the risk of exploitation.**

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 the following mitigation measures for SSL-related issues:

- **Force the Use of SSL: Ensure that certain protocols only use SSL to secure communications.**
- **Purchase or Generate Proper Certificates: Use valid and trusted certificates for all services.**
- **Replace Expired Certificates: Regularly update and renew certificates before they expire.**
- **Configure Applications to Use Appropriate Strength Ciphers: Use strong encryption algorithms to protect data.**
- **Replace SSL 2.0 or 3.0 with TLS 1.1 or Higher: Upgrade to more secure versions of the TLS protocol to prevent vulnerabilities associated with older SSL versions.**

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 (National Cybersecurity and Communications Integration Center) conducted a free vulnerability assessment for qualified government and private sector organizations. The assessment was performed remotely and periodically to identify security weaknesses.

Tools Used:

- **Nmap: Utilized for network mapping to identify active hosts and gather information about the network structure.**
- **Nessus: Employed for vulnerability scanning to detect and assess security vulnerabilities on the identified hosts.**

Results:

- **The assessment identified 63 distinct types of vulnerabilities across the scanned hosts.**
- **10% of hosts were found vulnerable, showing an improvement with 44 fewer vulnerable hosts compared to the previous scan.**
- **The vulnerabilities were categorized by severity, with medium severity being the most common among newly identified vulnerabilities.**
- **Detailed reports included tables, graphs, and recommendations to help organizations understand and mitigate the identified security issues effectively.**

This comprehensive assessment helps organizations prioritize their security efforts and implement necessary measures to protect their infrastructure from cyber threats.

How are the Vulnerability names useful for further investigation?

Vulnerability names are crucial for further investigation because they:

- **Reference Maintenance: They correspond to references maintained by Tenable, the company behind Nessus, providing detailed information about each vulnerability.**
- **Detailed Information: These references offer in-depth descriptions, CVE numbers, and mitigation measures, facilitating a better understanding of the vulnerabilities.**
- **Link to CVE Specifications: They often include links to official CVE (Common Vulnerabilities and Exposures) specifications, allowing analysts to access standardized information about the vulnerabilities.**
- **CVSS Vectors: Tenable provides CVSS (Common Vulnerability Scoring System) vectors for each vulnerability, which help in assessing the severity and potential impact.**

By using these names, cybersecurity professionals can efficiently locate comprehensive details, prioritize remediation efforts, and implement appropriate security measures to address the vulnerabilities.

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, you could take the following actions:

1. **Identify and Address Critical Vulnerabilities Immediately:**
    - **Action: Use the report to pinpoint critical vulnerabilities that pose the highest risk and prioritize them for immediate remediation.**
    - **Benefit: Reduces the likelihood of successful attacks exploiting these high-risk vulnerabilities.**
2. **Target Hosts with Multiple Vulnerabilities:**
    - **Action: Identify hosts that have multiple vulnerabilities and implement mitigation measures to secure these systems.**
    - **Benefit: Enhances overall network security by addressing the most vulnerable points that could be exploited in combination.**
3. **Implement Centralized Patch Management Systems:**
    - **Action: Recommend the deployment of centralized patch management solutions to ensure that all systems are regularly updated with the latest security patches.**

- **Benefit: Streamlines the process of maintaining software updates, reducing the chances of vulnerabilities remaining unpatched across the network.**

These actions help in systematically improving the organization's security posture by focusing on high-impact areas and ensuring continuous protection against emerging threats.