Nama : Winda Umi Fatimatus Sa’diyah

NIM : 2141762055

Absen : 19

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.

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

- It is a free service offered by the Cybersecurity and Infrastructure Security Agency (CISA) that helps organizations identify vulnerabilities in their internet-facing systems to improve security.

What other cybersecurity services are available from NCATS?

- NCATS provides additional services like the Phishing Campaign Assessment, Risk and Vulnerability Assessment (RVA), and the Validated Architecture Design Review (VADR).

Who are these services available to?

- These services are available to U.S. government agencies, critical infrastructure organizations, and other public and private entities operating 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 assist organizations in improving their cybersecurity defenses by identifying and mitigating vulnerabilities.

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

- The "Cyber Hygiene Report Card" section provides this high-level overview.

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

- The detailed findings and mitigations are located in **Appendix C**.

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

- The report provides **CSV files** in Appendix G, which can be opened in spreadsheet applications for further analysis.

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% of hosts, or 393, were found to be vulnerable, which is 44 fewer hosts compared to the previous scan.

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

- Medium severity vulnerabilities accounted for the highest number of newly vulnerable hosts, with an additional 108 hosts being affected.

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

- Medium severity vulnerabilities take the longest time to mitigate, averaging 158 days.

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

- While the organization provided a range of 293,005 IP addresses, only 3,986 were active or reachable at the time of the scan.

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 network mapping and vulnerability scanning of internet-facing hosts found during the network mapping process.

How many distinct types of vulnerabilities were identified?

- A total of **63 distinct types** of vulnerabilities were found.

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

- Vulnerabilities related to **SSL certificates and cipher suites** were the most common.

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 the **MikroTik Router OS 6.41.3 SMB** and **MikroTik RouterOS HTTP Server** were specific to **MikroTik routers**.

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 is **9.8**, and the severity rating is **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?

- Updating the MikroTik RouterOS to version 6.41.3 or higher, or disabling the SMB service on the affected routers.

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

- This is a **buffer overflow** vulnerability. An attacker could execute code on the system without authentication.

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

- They should have applied updates to the RouterOS firmware as soon as the vulnerability was disclosed by the vendor.

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 scan was conducted from the IP network **64.69.57.0/24**, which is registered to the U.S. Department of Homeland Security. This is important so that the organization does not mistakenly block the IP addresses or misinterpret the scan as a malicious attack.

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

- A computer is designated as a host if it has at least one open service or port that is actively listening for connections.

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.

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

- Nessus is offered by **Tenable**, and the free version is limited to scanning a maximum of **16 IP addresses**.

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

- High severity vulnerabilities have a CVSS score between **7.0 and 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.

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 is **x.x.124.231**. This vulnerability likely exists because the PHP software on the host has not been updated to the latest secure version.

What should be done to mitigate this vulnerability?

- The PHP service should be updated 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?

- Some recommended mitigation measures include enforcing the use of SSL/TLS, replacing expired certificates, using stronger cipher suites, and upgrading from SSL 2.0/3.0 to 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 vulnerability assessment is a free service that helps organizations identify and mitigate vulnerabilities in their networks. Using tools like **Nmap** for network discovery and **Nessus** for vulnerability scanning, the assessment identifies weaknesses in internet-facing systems and provides detailed reports. These reports categorize vulnerabilities by severity and offer mitigation guidance.

2. How are the Vulnerability names useful for further investigation?

- Vulnerability names can be cross-referenced with external databases like **CVE** and **Tenable's** website, which provide additional details such as descriptions, severity scores, and suggested remediation actions.

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

- Prioritize fixing critical vulnerabilities first, especially those with high CVSS scores.
- Develop a patch management strategy to regularly update vulnerable software.
- Strengthen SSL/TLS configurations to address weaknesses in encryption protocols.

End of document