Rossi Dea Agatha
SIB 4C – 2141762112

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 Service.

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

- It is a free vulnerability scanning service offered by the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security, designed to help organizations enhance their cybersecurity posture by detecting vulnerabilities on internet-accessible systems.

What other cybersecurity services are available from NCATS?

- NCATS also provides services such as Phishing Campaign Assessment, Risk and Vulnerability Assessment (RVA), and Validated Architecture Design Review (VADR).

Who are these services available to?

- These services are available to federal, state, local, tribal, and territorial government entities, as well as critical infrastructure organizations in both the public and private sectors within 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.

What is the goal of the report?

- The goal of this report is to assist organizations in identifying and addressing vulnerabilities in their network infrastructure to reduce potential security risks and improve overall cybersecurity defenses.

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

- This overview can be found in the *Cyber Hygiene Report Card*, which provides a summary of findings and trends over time.

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

- A detailed list of vulnerabilities and mitigations can be found 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*, making it easier to open the data in a spreadsheet format 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.

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

- 10% or 393 hosts were identified as vulnerable, which is 44 hosts fewer than in the previous scan, showing an improvement in the security posture.

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

- Medium-severity vulnerabilities saw the highest number of newly vulnerable hosts, with an increase of 108 hosts.

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

- Medium-severity vulnerabilities took the longest to mitigate, with an average of 158 days to address.

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

- This is because although 293,005 IP addresses were provided for the scan, only 3,986 were actively reachable at the time of the scan, reflecting the actual active systems in the network.

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 network mapping to identify hosts and vulnerability scanning of internet-accessible hosts found during the mapping process.

How many distinct types of vulnerabilities were identified?

- A total of 63 distinct types of vulnerabilities were identified.

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 frequently identified vulnerabilities.

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 associated with 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, with a severity rating of 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?

- According to the full disclosure report, the vulnerability can be mitigated by either updating the RouterOS to version 6.41.3 or higher, or by disabling the SMB service.

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

- This is a *buffer overflow* vulnerability, and an attacker can execute arbitrary code on the system without authentication if the vulnerability is exploited.

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

- The organization should have regularly monitored security advisories for their network hardware and promptly updated the MikroTik RouterOS to patch the vulnerability as soon as it was disclosed.

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 is 64.69.57.0/24, registered to the U.S. Department of Homeland Security. It is important to inform the Sample Organization to prevent them from mistaking the scanning activity as a malicious attack and to ensure the IP addresses are allowed through their firewalls.

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

- A computer qualifies as a host if it has an IP address with at least one open or listening service, making it detectable during the scan.

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

- 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?

- Nessus is offered by Tenable. 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?

- Vulnerabilities with CVSS scores ranging from 7.0 to 10.0 are categorized as 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.

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 this host is outdated, suggesting that the system lacks proper patch management.

What should be done to mitigate this vulnerability?

- The PHP software should be updated to version 5.6.34 or higher to mitigate this vulnerability.

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

- Enforcing SSL usage for specific protocols.
- Acquiring or generating valid SSL certificates.
- Replacing expired certificates.
- Configuring applications to use stronger cipher suites.
- Upgrading SSL 2.0 or 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.
   - NCCIC conducts free vulnerability scans for eligible organizations by remotely assessing internet-facing systems. The assessment uses Nmap for network discovery and Nessus for scanning vulnerabilities. The findings are compiled into a detailed report that includes trend data, vulnerability severity, and recommended mitigation strategies. This assessment helps organizations address critical security weaknesses.

   How are the Vulnerability names useful for further investigation?

   - The vulnerability names link directly to Tenable's reference pages, which provide detailed information about each vulnerability, including its CVE number, CVSS score, and possible mitigation strategies. These references are valuable for conducting in-depth research on specific vulnerabilities.

2. Provide three actions you could take based on the information provided in a Cyber Hygiene report.
   - Prioritize the remediation of critical vulnerabilities to reduce immediate risks.
   - Identify and address common vulnerabilities that affect multiple hosts across the network.
   - Implement automated patch management to ensure timely updates and prevent future vulnerabilities.