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?

Answer: National Cybersecurity Assessments and Technical Services

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

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

What other cybersecurity services are available from NCATS?

Answer: 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?

Answer: These services are available to federal, state, local, tribal, and territorial governments, as well as 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?

Answer: 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?

Answer: Cyber Hygiene Report Card.

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

Answer: Appendix C.

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

Answer: 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?

Answer: 10% (393 hosts) were found to be vulnerable, which 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?

Answer: 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?

Answer: 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?

Answer: The Sample Organization provided access to an address space of 293,005 addresses, but only 3,986 were active and 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.

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

Answer: The assessment included network mapping to identify hosts and other information, and vulnerability assessment of internet-accessible hosts found during mapping.

How many distinct types of vulnerabilities were identified?

Answer: 63.

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

Answer: 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?

Answer: MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary; the device 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?

Answer: 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?

Answer: Update RouterOS to version 6.41.3 or higher, or disable the Server Message Block (SMB) service.

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

Answer: It is a buffer overflow. Attackers 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?

Answer: They should have monitored product advisories for their network hardware and updated RouterOS promptly after being informed of the vulnerability.

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?

Answer: 64.69.57.0/24; registered to the US Department of Homeland Security. It is important to inform the Sample Organization to prevent misinterpretation as a reconnaissance attack and ensure firewall configurations allow for the scan.

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

Answer: 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?

Answer: Nmap for network mapping and Nessus for vulnerability scanning.

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

Answer: Tenable provides Nessus; 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?

Answer: 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?

Answer: The IP address is x.x.124.231. The vulnerability exists likely due to a lack of patch management and software updates.

What should be done to mitigate this vulnerability?

Answer: 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?

Answer: Force the use of SSL for some protocols, obtain proper certificates, replace expired certificates, configure applications to use strong ciphers, and replace SSL 2.0/3.0 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.

   Answer: NCCIC conducted a remote vulnerability scanning service for qualified organizations. They used Nmap for network mapping to identify hosts and Nessus for scanning these hosts for vulnerabilities. The results included detailed reports that help identify vulnerabilities, assess trends over time, and guide remediation efforts. Each vulnerability is rated by severity based on CVSS scores.

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

   Answer: Vulnerability names correspond to references maintained by Tenable, which provide additional information, mitigation strategies, and CVE specifications. This facilitates further research and understanding of the vulnerabilities.

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

   Answer:

   - Identify and prioritize critical vulnerabilities for immediate remediation.
   - Assess and implement mitigation measures for hosts with multiple vulnerabilities.
   - Recommend a centralized patch management system to ensure timely updates and reduce vulnerabilities across the network.