Name : Rizqi Zamzami Jamil

Class : SIB-4C

NIM : 2141762089

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:

NCATS stands for National Cybersecurity Assessment and Technical Services.

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

Answer:

The Cyber Hygiene Vulnerability Scanning Service is a free service provided by the Cybersecurity and Infrastructure Security Agency (CISA). It aims to secure internet-accessible systems by continuously scanning for known vulnerabilities and configuration errors. This helps organizations reduce their risk and exposure to cyber threats by identifying and addressing vulnerabilities before they can be exploited.

What other cybersecurity services are available from NCATS?

Answer:

In addition to the Cyber Hygiene Vulnerability Scanning Service, NCATS offers the Risk and Vulnerability Assessment (RVA) service. This service includes penetration testing to determine weaknesses in an organization's cybersecurity posture and provides actionable remediation recommendations.

Who are these services available to?

Answer:

These services are available to federal agencies, state, local, tribal, and territorial governments, and other organizations that are part of 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:

The goal of the report is to provide detailed technical findings about vulnerabilities discovered during security scans of Sample Organization's public-facing systems and to help prioritize remediation efforts.

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" section.

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

Answer:

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?

Answer:

The CSV (Comma Separated Values) file format allows easy opening of scan results in spreadsheets or other tabular documents.

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?

Answer:

A total of 393 hosts, representing 10%, were found to be vulnerable44 fewer than in 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 recently detected with medium-severity vulnerabilities.

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

Answer:

The organization takes an average of 158 days to address 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 granted access to an address space of 293,005 addresses, but only 3,986 were active and reachable during 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?

Answer:

The assessment included network mapping to identify hosts and gather information, followed by a vulnerability evaluation of the internet-accessible hosts discovered during the mapping process.

How many distinct types of vulnerabilities were identified?

Answer:

There are 63 types.

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:

The vulnerability appears to be related to MikroTik Router OS 6.41.3 SMB.

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:

The full disclosure report is available on the Seclists.org website. According to item 5, RouterOS should be updated to version 6.41.3 or later, 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?

Answer:

This is a buffer overflow vulnerability, allowing attackers to execute code on the system without requiring user 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. Once informed of the vulnerability, they should have promptly updated the RouterOS version.

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?

Answer:

The 64.69.57.0/24 IP range is reported by various lookup sites as registered to the U.S. Department of Homeland Security. Since the vulnerability assessment involves deep scanning of the organization’s network, it could be mistaken for a reconnaissance attack by a threat actor. As a result, the organization might unintentionally try to mitigate the perceived threat by blocking these IP addresses at the network edge. Furthermore, to ensure the scan's success, firewall rules may need to allow traffic from this IP range for connections originating outside the network.

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

Answer:

A device can be classified as a host when it possesses an address and runs at least one active or accessible service.

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

Answer:

The network assessment involved Nmap for infrastructure mapping purposes, combined with Nessus for scanning security vulnerabilitie.

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

Answer:

Nessus is manufactured by Tenable, and users of its free edition can only scan up to 16 IP addresses.

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

Answer:

High-severity vulnerabilities identified by CVSS scores 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?

Answer:

System at x.x.124.231 needs software updates, suggesting an absence of patch management and update service implementation.

What should be done to mitigate this vulnerability?

Answer:

Update the PHP service software to version 5.6.34 or later.

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

Answer:

1. Enforce the use of SSL for specific protocols.
2. Acquire or generate valid certificates for services.
3. Renew any expired certificates.
4. Set up applications to utilize ciphers of adequate strength.
5. Upgrade from 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.

Answer:

The NCCIC offers a complimentary vulnerability scanning service for eligible government and private sector organizations. This scanning is performed remotely and on a regular basis. Beneficiaries receive reports detailing the outcomes of these scans, which can be utilized to identify vulnerabilities, monitor weekly trends, and inform mitigation strategies. NCCIC employs Nmap to develop a network map that identifies hosts and utilizes Nessus to assess those hosts for vulnerabilities. The resulting reports are comprehensive, containing various details, tables, and graphs that effectively convey the network security issues needing attention to the beneficiaries. Each vulnerability is assessed and categorized based on its severity, indicated by its CVSS score.

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

Answer:

The names of the vulnerabilities correspond to a reference managed by Tenable, the company behind Nessus. This reference provides additional insights into the vulnerabilities and frequently includes links to other resources for further information. It also offers connections to CVE specifications related to each vulnerability, along with the CVSS vectors provided by Tenable.

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

Answer:

1. Prioritize and Remediate Vulnerabilities.
2. Enhance Security Awareness and Training.
3. Improve Network and System Security.

.