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?

Answer Area

National Cybersecurity Assessments and Technical Services.

Show Answer

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

Answer Area

The Cybersecurity and Infrastructure Security Agency (CISA), part of the US Department of Homeland Security, offers a free service for vulnerability assessments.

Show Answer

What other cybersecurity services are available from NCATS?

Answer Area

Along with Cyber Hygiene vulnerability scanning, NCATS also provides Phishing Campaign Assessments, Risk and Vulnerability Assessments, and Validated Architecture Design Reviews.

Show Answer

Who are these services available to?

Answer Area

The service is available to federal, state, local, tribal, and territorial governments, as well as public and private critical infrastructure organizations in the USA.

Show Answer

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?

Answer Area

The goald of the report to help organizations strengthen their security posture.

Show Answer

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

Answer Area

Cyber Hygiene Report Card.

Show Answer

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

Answer Area

Appendix C.

Show Answer

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

Answer Area

In Appendix G, Comma-Separated Values (CSV) files are provided for this purpose.

Show Answer

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 Area

10%, or 393, hosts were found to be vulnerable. This is 44 hosts fewer than the previous scan.

Show Answer

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

Answer Area

An additional 108 hosts were newly identified as having medium severity vulnerabilities.

Show Answer

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

Answer Area

It takes the organization a mean time of 158 days to mitigate a medium level vulnerability.

Show Answer

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

Answer Area

The Sample Organization allocated a range of 293,005 addresses, but during the scan, only 3,986 of these addresses were active and accessible for scanning.

Show Answer

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 Area

The assessment performed network mapping to discover hosts and gather related information, as well as a vulnerability evaluation of internet-accessible hosts identified during the mapping process.

Show Answer

How many distinct types of vulnerabilities were identified?

Answer Area

63 distinct types of vulnerabilities were identified.

Show Answer

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

Answer Area

SSL certificates and cipher suites.

Show Answer

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 Area

MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary. It is a MikroTik router.

Show Answer

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 Area

CVSS base score 9.8, rating critical (CVE-2018-7445).

Show Answer

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 Area

The complete disclosure report is available on the Seclists.org website. According to item 5, Router OS should be upgraded to version 6.41.3 or later, or alternatively, the Server Message Block (SMB) should be disabled.

Show Answer

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

Answer Area

It is a buffer overflow vulnerability. Attackers can easily execute system code since authentication is not required to exploit the issue.

Show Answer

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

Answer Area

They should have adhered to product advisories for their network hardware. Once notified of the vulnerability, they should have promptly updated their RouterOS version.

Show Answer

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 Area

The IP network 64.69.57.0/24 is reported by various IP lookup sites as being registered to the US Department of Homeland Security. Given that the vulnerability assessment process involves in-depth scanning of the organization's network, this might be misinterpreted as a reconnaissance attack by a potential threat actor. Consequently, the organization might mistakenly try to mitigate the perceived threat by blocking the IP addresses from this network at the network perimeter. Additionally, to ensure the scan is successful, the addresses within this network may need to be granted access through a firewall for connections coming from outside the network.

Show Answer

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

Answer Area

A host is defined as a device with an address that has at least one service actively open or listening.

Show Answer

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

Answer Area

Nmap was utilized for network mapping, while Nessus was employed for vulnerability scanning.

Show Answer

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

Answer Area

Tenable offers the Nessus product, with the free version restricted to scanning up to 16 IP addresses.

Show Answer

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

Answer Area

Vulnerabilities with a CVSS base score of 7.0-10.0.

Show Answer

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 Area

The host with IP address x.x.124.231 needs its software updated. It appears that patch management and update services are not being utilized for this host.

Show Answer

What should be done to mitigate this vulnerability?

Answer Area

Update the PHP service software to version 5.6.34 or higher.

Show Answer

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

Answer Area

- Enforce SSL usage for certain protocols.
- Acquire or create valid certificates for services.
- Renew expired certificates.
- Set up applications to use strong ciphers.
- Upgrade from SSL 2.0 or 3.0 to TLS 1.1 or newer.

Show Answer

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 Area

NCCIC offers a complimentary vulnerability scanning service for eligible government and private sector entities. The scanning process is conducted remotely and on a periodic basis. Beneficiaries receive detailed reports of the findings, which can be used to identify vulnerabilities, track weekly trends, and guide the remediation efforts. To perform the assessment, NCCIC utilizes Nmap for network mapping to identify hosts, and Nessus for scanning these hosts to detect vulnerabilities. The resulting reports are comprehensive, including various details, tables, and graphs to effectively communicate the security issues within the network that need addressing. Each identified vulnerability is assessed and rated based on its severity, according to its CVSS score.

Show Answer

How are the Vulnerability names useful for further investigation?

Answer Area

Vulnerability names are valuable for further investigation as they correspond to a reference maintained by Tenable, the provider of Nessus. This reference offers detailed information about the vulnerabilities and often includes links to additional resources for deeper insights. Additionally, the Tenable reference provides links to CVE (Common Vulnerabilities and Exposures) specifications related to the vulnerabilities, along with the CVSS (Common Vulnerability Scoring System) vectors, which help in understanding the severity and impact of each vulnerability.

Show Answer

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

Answer Area

Based on the information provided in a Cyber Hygiene report, you could take the following actions:
- Address Critical Vulnerabilities: Use the report to pinpoint critical vulnerabilities that need immediate remediation to prevent potential exploitation.
- Mitigate Vulnerabilities on Affected Hosts: Identify hosts with multiple vulnerabilities and implement mitigation measures to address these issues, ensuring that affected systems are secured.
- Implement Centralized Solutions: Recommend and deploy centralized solutions like patch management systems to reduce the risk of critical or high-severity vulnerabilities appearing on the network.

Show Answer

End of document

Show All Answers Clear My Responses