IK-RARS'JATI PRAMESTI
2141762003
SIB-4C

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 ReportPart 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 personnelabout 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?
National Cybersecurity Assessments and Technical Services

What is the Cyber Hygiene Vulnerability Scanning Service? Search the web for details.
It is a free vulnerability assessment service that is provided by the Cybersecurity and InfrastructureSecurity Agency (CISA) of the US Department of Homeland Security.

What other cybersecurity services are available from NCATS?
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?
Federal, state, local, tribal, and territorial governments, and public and private sector criticalinfrastructure 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-likeoverview 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 provideuseful 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 asSample Organization (Sample).

Review section one of the report and answer the following questions.

What is the goal of the report?
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 somecomparisons of weekly performance?
Cyber Hygiene Report Card

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

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

What percent of the scanned hosts were found to be vulnerable? How does this compare to the previousscan?
10%, or 393, hosts were found to be vulnerable. This is 44 hosts fewer than the previous scan.

Vulnerabilities are classified by severity. Which level of severity represents the highest number of newlyvulnerable hosts?
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?
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?
The Sample Organization provided access to an address space of 293,005 addresses, but at thetime of the scan, only 3,986 were active and reachable for 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?
The assessment conducted network mapping to identify hosts and other information, andvulnerability assessment of internet-accessible hosts that were found during mapping.

How many distinct types of vulnerabilities were identified?
63

Of the top five vulnerabilities by occurrence, what was common system or protocol was most often found tobe vulnerable?
SSL certificates and cipher suites.

Of the top five categories by degree of risk, which vulnerabilities appear to be related to a specific piece ofnetwork hardware? What is the device?
MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary. It is a MikroTikrouter.

Search the web on "MikroTik Router OS 6.41.3 SMB." Locate the CVE entry for this vulnerability on theNational Vulnerability Database (NVD) website. What is the CVSS base score and severity rating?
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 fulldisclosure report, what are two ways of mitigating the vulnerability?
The full disclosure report is found on the Seclists.org website. Item 5 says that the RouterOS should be updated to version 6.41.3 or higher, or the Server Message Block (SMB) service shouldbe disabled.

What type of vulnerability is this, and what can an attacker do when it is exploited?
It is a buffer overflow. Attackers could easily execute code of the system because the user does notneed to be authenticated to exploit it.

What should the Sample Organization have done to prevent this critical vulnerability from appearing ontheir network?
They should have been following product advisories for their network hardware. After they wereinformed of the vulnerability, they should have updated the RouterOS version as quickly as possible.

Step 4: Review assessment methodology and process.

It is important to evaluate the methodology that was used to create a vulnerability assessment to determinethe 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 theIP network, and to whom is it registered? Why is important to tell this to Sample Organization?
64.69.57.0/24. Various IP address lookup sites report that this IP network is registered to the US Department of Homeland Security. Because the vulnerability assessment process performs deep scanning of the organization network, this could be interpreted as a reconnaissance attack from athreat actor. The organization could accidentally attempt to mitigate the threat by blocking the IP addresses in that network at the network edge. In addition, for the scan to be successful, addresses from this network may need to be allowed access through a firewall for connections originating from outside the network.

What qualifies a computer to be designated as a host for the purposes of this report?
A host is defined as a device with an address that has at least one open or listening servicerunning.

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?
Tenable provides the Nessus product. 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?
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 ofthem. 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 byTenable. 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 thevulnerability, 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 thisvulnerability exists on this host?
x.x.124.231. The host requires its software to updated. Apparently patch management and updateservices are not used for the host.

What should be done to mitigate this vulnerability?
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 arerecommended in the report?
- **Force the use of SSL for some protocols.**
- **Purchase or generate proper certificates for services.**
- **Replace expired certificates.**
- **Configure applications to use appropriate strength cyphers.**
- **Replace SSL 2.0 or 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, thetools used and a brief description of the results.
NCCIC provides a free service of vulnerability scanning for qualified government and private sectororganizations. Scanning is done remotely, and periodically. Reports of the results are available to beneficiaries. The reports can be used to discover vulnerabilities, prepare weekly trends and updates, and guide in mitigation of vulnerabilities. NCCIC uses Nmap to create a network map in which hosts are identified, and Nessus to scan the identified hosts for vulnerabilities. The reports include numerous details, tables, and graphs to help communicate to the beneficiaries the securityissues in the network that require attention. Each vulnerability is rated by severity according to its CVSS score.

   How are the Vulnerability names useful for further investigation?
The vulnerability names match a reference that is maintained by the Tenable, the company that offers Nessus. The Tenable reference provides further details on the vulnerabilities and often provides links to other sources for more information. The Tenable reference also provides links toCVE specifications for the vulnerability. Tenable provides the CVSS vectors for the vulnerability aswell.

2. Provide three actions you could take based on the information provided in a Cyber Hygiene report.
   - **Use the report to identify critical vulnerabilities that should be addressed immediately.**
   - **Identify hosts that require mitigation measures to address vulnerabilities, especially if the host isfound to have multiple vulnerabilities.**
   - **Identify vulnerabilities that are shared by many hosts on the network.**
   - **Recommend centralized solutions, such as patch management systems to lower the likelihoodthat critical or high severity vulnerabilities appear on the network.**