cisco Networking Academy

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?

National Cybersecurity Assessments and Technical Services

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

It is a free service from the Cybersecurity and Infrastructure Security Agency (CISA) under the US Department of Homeland Security that checks for security weaknesses.

What other cybersecurity services are available from NCATS?

Besides Cyber Hygiene vulnerability scanning, NCATS also provides Phishing Campaign Assessment, Risk and Vulnerability Assessment, and Validated Architecture Design Review.

Who are these services available to?

They are available to U.S. federal, state, local, tribal, and territorial governments, as well as critical infrastructure organizations in both the public and private sectors.

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?

To help organizations improve their security defenses.

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

Appendix G provides Comma-Separated Values files, which make it easy to open the scan results in a spreadsheet or similar table-based document.

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?

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

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

The highest number of newly vulnerable hosts were in the medium severity category, with 108 hosts added.

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

The organization takes about 158 days to fix a medium-level vulnerability on average.

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

The Sample Organization gave access to 239 005 IP addresses, but during the scan, only 3 986 were active and could be reached.

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?

The assessment included network mapping to find hosts and gather information, as well as a vulnerability check of the internet-accessible hosts discovered.

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 to be vulnerable?

Cipher suites and SSL certificates

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?

The vulnerabilities linked to a specific piece of network hardware are 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?

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?

The full disclosure report is on the Seclists.org website. Item 5 recommends updating RouterOS to version 6.41.3 or later, or turning off the Server Message Block.

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

It is a buffer overflow flaw that lets attackers run code on the system without needing to log in.

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

They should have kept up with product advisories for their network hardware. Once the vulnerability was reported, they should have updated RouterOS right away.

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?

The IP range 64.69.57.0/24 is listed by several lookup sites as belonging to the U.S. Department of Homeland Security. Because the scan digs deep into the network, traffic from these IPs might look like a reconnaissance attack. The organization could mistakenly block those addresses at the network edge. Also, for the scan to work, firewall rules might need to let connections from that range through even though they come from outside.

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

A host is any device with an address that has at least one active or listening service running.

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

Nmap was used to map the network and Nessus was used to scan for vulnerabilities.

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

Nessus is made by Tenable and its free version can only scan up to 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 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?

The host at x.x.124.231 needs a software update. It seems that patch management and update services are not being used for this host.

What should be done to mitigate this vulnerability?

The host x.x.124.231 requires a software update and it appears that patch management or update services are not in place for it.

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

The report recommends requiring SSL for certain protocols, using valid certificates, replacing expired certificates, configuring applications to use strong ciphers, and upgrading 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.

NCCIC offers a free vulnerability scanning service for eligible government and private sector organizations. The scans are done remotely and on a regular basis, with results provided in reports. These reports help identify vulnerabilities, track weekly trends, and guide mitigation efforts. NCCIC uses Nmap to map the network and identify hosts, and Nessus to scan those hosts for vulnerabilities. The reports include detailed information, tables, and graphs to show security issues that need attention, and each vulnerability is rated by severity based on its CVSS score.

How are the Vulnerability names useful for further investigation?

The vulnerability names match a reference maintained by Tenable, the company that makes Nessus. This reference gives more details about each vulnerability and often includes links to other sources for further information. It also provides links to the CVE specifications and shows the CVSS vectors for the vulnerability.

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

   Based on a Cyber Hygiene report, you could identify and immediately fix critical vulnerabilities, address hosts with multiple vulnerabilities by applying the necessary fixes, and recommend centralized solutions such as patch management systems to reduce the chances of critical or high-severity vulnerabilities appearing on the network.

REFLECTION QUESTIONS

1. Think about your own experiences with technology — why do you think it's important for organizations to regularly assess vulnerabilities, and how might that relate to keeping your personal devices secure? ***It's important for organizations to regularly assess vulnerabilities because it helps them find and fix security weaknesses before attackers can exploit them. This is like keeping my personal devices secure, since I also need to install updates, use strong passwords, and check for risks to prevent hackers from gaining access to my data. Regular assessments, whether for big organizations or for my own devices, are a way to stay one step ahead of threats.***
2. Out of the mitigation strategies you read about in the lab, which do you believe would be the most challenging for an organization (or even yourself) to apply, and what factors make it difficult? ***The most challenging mitigation strategy to apply would be setting up and maintaining a proper patch management system. For an organization, it can be hard because there may be hundreds or even thousands of devices to update, and some updates might break existing software or require downtime. For me personally, it can be difficult because updates sometimes take a lot of time, use up storage, or cause apps to stop working the way they used to. These factors make people or organizations delay updates, which increases the risk of vulnerabilities.***
3. Reflect on the tools and standards used in the lab (like Nmap, Nessus, and CVSS scoring). How do you think using common tools and frameworks changes the way people understand and act on security issues? ***Using common tools and standards like Nmap, Nessus, and CVSS scoring makes security issues easier to understand and act on because everyone is working from the same reference point. For example, CVSS scores give a clear way to measure how serious a vulnerability is, so organizations can agree on what to fix first. Tools like Nmap and Nessus provide consistent results that can be shared and compared across teams. This shared language and consistency help reduce confusion, improve communication, and make it easier to take the right steps to improve security.***