# 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

****TASK 1****

#### 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.

****QUESTION 1****

**What does NCATS stand for?**

****ANSWER****

National Cybersecurity Assessments and Technical Services, conduct risk and vulnerability assessments

**QUESTION 2**

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

**ANSWER**

Cyber Hygiene Vulnerability Scanning is a free cybersecurity service, primarily offered by CISA (Cybersecurity and Infrastructure Security Agency), that continuously monitors and assesses internet-accessible network assets to identify and report vulnerabilities and weaknesses before they can be exploited by attackers.

**QUESTION 3**

**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.

**QUESTION 4**

**Who are these services available to?**

**ANSWER**

Federal, state, local, tribal, and territorial governments, and public and private sector critical infrastructure organizations in the USA.

**TASK 2**

**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.

**QUESTION 1**

**What is the goal of the report?**

**ANSWER**

To help organizations strengthen their security posture.

**QUESTION 2**

**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

**QUESTION 3**

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

**ANSWER**

Appendix C

**QUESTION 4**

**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.

## TASK 3

### 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.

**QUESTION 1**

**What percent of the scanned hosts were found to be vulnerable? How does this compare to the previous scan?**

**ANSWER**

32% of hosts vulnerable. Altogether 268 vulnerable hosts. This is 6 hosts fewer than previous scan.

**QUESTION 2**

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

**ANSWER**

Medium level of severity represents the highest number of newly vulnerable hosts with addition of 20 new identified vulnerabilities.

**QUESTION 3**

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

**ANSWER**

Medium severity of vulnerability requires 2748 days to mitigate.

**QUESTION 4**

**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 at the time 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.

**QUESTION 5**

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

**ANSWER**

The Cyber Hygiene assessment includes network mapping and vulnerability scanning for Internet-accessible SAMPLE hosts.

**QUESTION 6**

**How many distinct types of vulnerabilities were identified?**

**ANSWER**

30 distinct types of potential vulnerabilities (0 critical, 2 high, 20 medium, and 8 low) were detected

**QUESTION 7**

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

**ANSWER**

SSL certificate and TLS version 1.1 protocol deprecated

**QUESTION 8**

**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. It is a MikroTik router

**QUESTION 9**

**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)

**QUESTION 10**

**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**

Router OS should be updated to version 6.41.3 or higher, or the Server Message Block (SMB) should be disabled

**QUESTION 11**

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

**ANSWER**

It is a buffer overflow. Remote attackers with access to the service can exploit this vulnerability and gain code execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it.

**QUESTION 12**

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

**ANSWER**

They should have been following product advisories for their network hardware. After they were informed 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 determine the quality of the work that was done. Review the material in that section of the report.

****QUESTION 13****

**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.

IP network is registered to the US Department of Homeland Security.

It is important to tell this to Sample Organization, because the vulnerability assessment process performs deep scanning of the organization network, this could be interpreted as a reconnaissance attack from a threat 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.

****QUESTION 14****

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

****ANSWER****

A computer (or device) is designated as a "host" only if: at least one of the most common 1,000 TCP ports is open and responsive during the scan.

****QUESTION 15****

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

****ANSWER****

Nmap was used for network mapping and Nessus was used for vulnerability scanning.

****QUESTION 16****

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

****ANSWER****

Tenable provides the Nessus product. The free version is limited to scanning only 16 IP addresses and for non-commercial use only.

**QUESTION 17**

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

**ANSWER**

7-9.8 score are considered high severity.

## **TASK 3**

### 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.

**QUESTION 1**

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.

**ANSWER**

Vulnerability: **Sun ONE Application Server Upper Case Request JSP Source Disclosure**

**Synopsis**

The remote web server is affected by an information disclosure vulnerability.

**Description**

It is possible to make the remote web server disclose the source code of its JSP pages by requesting the pages with a different case (ie: filename.JSP instead of filename.jsp).

An attacker may use this flaw to get the source code of your CGIs and possibly obtain passwords and other relevant information about this host.

**Solution**

Upgrade to Sun ONE Application Server 7.0 Update Release 1.

### 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.

**QUESTION 2**

**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**

x.x.58.55 is the IP address. The host requires its software to updated.

**QUESTION 4**

**What should be done to mitigate this vulnerability?**

**ANSWER**

Update the PHP service software to version 5.6.34 or higher.

**QUESTION 5**

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

**ANSWER**

Purchase or generate a proper SSL certificate for this service.

Contact the Certificate Authority to have the SSL certificate reissued.

**TASK 4**

## 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 provides a free service of vulnerability scanning for qualified government and private sector organizations. 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 security issues in the network that require attention. Each vulnerability is rated by severity according to its CVSS score.

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

   **ANSWER**

   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

to CVE specifications for the vulnerability. Tenable provides the CVSS vectors for the vulnerability as well.

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

   ****ANSWER****

   - 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 is found 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 likelihood that critical or high severity vulnerabilities appear on the network.