Nama : Selly Amelia Putri (2141762142)

Class : SIB 4C (16)

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?

National Cybersecurity Assessments and Technical Services

National Cybersecurity Assessments and Technical Services

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

The Cyber Hygiene Vulnerability Scanning Service provided by the Cybersecurity and Infrastructure Security Agency (CISA) is a vulnerability assessment that aims to help organizations identify and remediate security vulnerabilities in their systems. The program is free and available to a variety of entities, including the federal government, private organizations, and local, tribal, and territorial governments.

Through this service, CISA conducts Risk and Vulnerability Assessments (RVA) to determine weaknesses that could be exploited by malicious actors. Once the assessment is complete, CISA provides a customized risk analysis and recommendations to improve the organization's cybersecurity posture(CISA).

CISA also publishes an annual report that summarizes the findings of the RVA conducted during the fiscal year, providing insight into potential attack paths taken by cyber threat actors(CISA). This helps organizations implement better defense strategies and strengthen their security posture.

It is a free vulnerability assessment service that is provided by the Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of Homeland Security.

What other cybersecurity services are available from NCATS?

In addition to the Cyber Hygiene Vulnerability Scanning Service, the National Cybersecurity Assessment and Technical Services (NCATS) offers a variety of other cybersecurity services. Some of these include:

Phishing Campaign Assessment: This service helps organizations identify vulnerabilities related to phishing attacks by simulating phishing campaigns to train staff and increase security awareness.

Risk and Vulnerability Assessment: This service involves a thorough analysis of an organization's systems and infrastructure to identify and assess existing risks and provide recommendations for mitigation.

Validated Architecture Design Review: This service involves evaluating network and system architectures to ensure that they are securely designed and compliant with cybersecurity best practices

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?

The National Cybersecurity Assessment and Technical Services (NCATS) service is available to a variety of entities, including:

Federal Government: This service is for federal agencies that require a cybersecurity assessment.

State and Local Governments: The service also covers state and local governments that want to improve their cybersecurity.

Tribes and Territories: Organizations that operate at the tribal and territorial level can also benefit from this service.

Critical Infrastructure Organizations: This includes the public and private sectors that manage critical infrastructure, such as healthcare, energy, and transportation in the United States.

Federal, state, local, tribal, and territorial governments, and public and private sector critical infrastructure 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-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?

The purpose of a security assessment report is to help organizations strengthen their security posture. The report is designed to provide clear, focused guidance, provide in-depth risk analysis, and implementable recommendations to address identified vulnerabilities. Using the report, organizations can take appropriate steps to improve and enhance the security of their systems and infrastructure.

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 some comparisons of weekly performance?

You can find a high-level overview of the assessment results, including comparisons of weekly performance, in the Cyber Hygiene Report Card section of the report. This section typically summarizes the key findings of the assessment and provides visual representations of the organization's performance over time, making it easier to identify trends and areas for improvement

Cyber Hygiene Report Card

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

You can find a detailed list of findings and recommended mitigations for each vulnerability in Appendix C of the report. This appendix typically provides a comprehensive breakdown of the vulnerabilities identified during the assessment, along with specific recommendations for addressing each one. It serves as a crucial resource for organizations looking to enhance their cybersecurity posture by implementing the suggested mitigations

Appendix C

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

You can easily open the results of the scan into a spreadsheet or other tabular document using the Comma-Separated Values (CSV) files provided in Appendix G of the report. This format allows for easy data manipulation and analysis in various applications, such as Microsoft Excel or Google Sheets

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 with the results of the current scan.

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

n the Cyber Hygiene Report Card, 10% of the scanned hosts, or 393 hosts, were found to be vulnerable. This represents a decrease of 44 hosts compared to the previous scan, indicating an improvement in the organization's security posture over time.

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 newly vulnerable hosts?

The level of severity that represents the highest number of newly vulnerable hosts is medium severity vulnerabilities. In the latest assessment, an additional 108 hosts were newly identified as having medium severity vulnerabilities.

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?

The class of vulnerability that requires the most time for the organization to mitigate is medium level vulnerabilities. It takes the organization a mean time of 158 days to address these vulnerabilities.

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 reason the scan included 293,005 IP addresses but only assessed 3,986 hosts is that the Sample Organization provided access to a large address space, but at the time of the scan, only 3,986 hosts were active and reachable. This disparity is common in large networks, where many IP addresses may be assigned but not all correspond to active devices or services.

Inactive addresses can arise from various factors, including decommissioned devices, misconfigured networks, or simply a lack of active services in certain address ranges. Thus, the scan focused only on the hosts that were available and reachable during that assessment period.

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.

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

The assessment included two major functions: network mapping to identify hosts and gather related information, and vulnerability assessment of the internet-accessible hosts that were found during the mapping process. This approach allows for a comprehensive understanding of the network's structure and the security posture of the identified hosts

The assessment conducted network mapping to identify hosts and other information, and vulnerability assessment of internet-accessible hosts that were found during mapping.

How many distinct types of vulnerabilities were identified?

The assessment identified a total of 63 distinct types of vulnerabilities. This classification helps organizations understand the variety of security weaknesses present in their systems and prioritize remediation efforts effectively

63

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

The common system or protocol that was most often found to be vulnerable among the top five vulnerabilities by occurrence was related to SSL certificates and cipher suites. This indicates that many systems had weaknesses in their secure socket layer (SSL) implementations, which could lead to potential security risks

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?

Of the top five categories by degree of risk, the vulnerabilities related to a specific piece of network hardware are associated with MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary. The device in question is a MikroTik router. These vulnerabilities indicate potential security issues that could affect the router's functionality and expose the network to various threats

MikroTik Router OS 6.41.3 SMB and MikroTik RouterOS HTTP Server Arbitrary. It 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?

The CVSS base score for the vulnerability related to MikroTik Router OS 6.41.3, specifically for CVE-2018-7445, is 9.8, which is rated as critical. This vulnerability involves a buffer overflow in the SMB service of MikroTik RouterOS, allowing unauthenticated remote attackers to execute arbitrary code before authentication occurs

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 for CVE-2018-7445, found on Seclists.org, outlines two main mitigation strategies:

1. Update RouterOS to version 6.41.3 or higher.
2. Disable the Server Message Block (SMB) service.

These measures can help address the vulnerabilities associated with MikroTik Router OS

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 should be disabled.

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

The vulnerability associated with CVE-2018-7445 is a buffer overflow. When exploited, an attacker can execute arbitrary code on the system without requiring user authentication, potentially gaining control over the affected device. This makes it particularly dangerous, as it allows unauthorized access to sensitive functions or data on the MikroTik router

It is a buffer overflow. Attackers could easily execute code of the system because the user does not need to be authenticated to exploit it.

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

To prevent the critical vulnerability CVE-2018-7445 from affecting their network, the Sample Organization should have actively monitored and followed product advisories for their network hardware. Upon being notified of the vulnerability, they should have prioritized updating the RouterOS version promptly to mitigate the risk.

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.

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 network mentioned in the report is 64.69.57.0/24, which is registered to the US Department of Homeland Security. This information is important for the Sample Organization because the deep scanning conducted during the vulnerability assessment could be misinterpreted as a reconnaissance attack by a threat actor. If the organization blocks these IP addresses at their network edge, it could hinder legitimate assessment efforts. Additionally, the organization may need to adjust firewall settings to allow connections from this network for a successful scan.

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 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.

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

A computer is designated as a host for the purposes of this report if it has an address and is running at least one open or listening service. This definition is crucial for identifying which devices are actively participating in network communications and can be assessed for vulnerabilities.

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

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

The scan utilized Nmap for network mapping and Nessus for vulnerability assessment. These tools are widely recognized for their effectiveness in identifying hosts and evaluating potential vulnerabilities within a network.

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 is the provider of the Nessus product. The limitation of the freely downloadable version of Nessus is that it can only scan 16 IP addresses at a time. For larger networks, a paid version would be necessary to conduct more extensive scans.

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 are labeled as "High" severity if they have a CVSS base score ranging from 7.0 to 10.0. This classification indicates a significant potential impact on the system's security.

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.

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 IP address of the host running a vulnerable PHP service is x.x.124.231. This vulnerability likely exists because the host does not have a proper patch management system in place, leading to outdated software that is susceptible to exploitation

x.x.124.231. The host requires its software to updated. Apparently patch management and update services are not used for the host.

What should be done to mitigate this vulnerability?

To mitigate this vulnerability, the PHP service software should be updated to version 5.6.34 or higher. Regular updates and patch management practices are essential to protect against known vulnerabilities and maintain the security of the host.

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 are recommended in the report?

Some recommended mitigation measures for SSL issues include:

- Enforcing the use of SSL for certain protocols.
- Purchasing or generating valid certificates for services.
- Replacing expired certificates.
- Configuring applications to use strong cipher suites.
- Upgrading from SSL 2.0 or 3.0 to TLS 1.1 or higher.

Implementing these measures can significantly enhance the security of SSL implementations and protect against vulnerabilities.

- **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, the tools used and a brief description of the results.

   The NCCIC conducts vulnerability assessments for eligible government and private sector organizations through remote and periodic scans. They use Nmap for network mapping to identify hosts and Nessus for vulnerability scanning. Reports generated provide insights into vulnerabilities, weekly trends, and mitigation guidance, featuring details, tables, and graphs. Each identified vulnerability is rated by severity using CVSS scores, helping organizations prioritize security issues needing attention. This free service supports organizations in enhancing their network security posture.

   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.

   How are the Vulnerability names useful for further investigation?

   The vulnerability names in the reports are beneficial for further investigation as they correspond to references maintained by Tenable, the company behind Nessus. These references offer detailed information on each vulnerability and often include links to additional resources and CVE specifications. They also provide CVSS vectors, allowing organizations to understand the severity and implications of the vulnerabilities more effectively. This information aids in prioritizing mitigation efforts and understanding the context of the vulnerabilities.

   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.

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

   Based on the information provided in a Cyber Hygiene report, three actions you could take include:

   1. Address Critical Vulnerabilities: Use the report to pinpoint critical vulnerabilities that need immediate remediation.
   2. Mitigation Measures for Affected Hosts: Identify hosts with multiple vulnerabilities and implement necessary mitigation measures for those systems.
   3. Centralized Solutions: Recommend the implementation of centralized solutions, like patch management systems, to reduce the likelihood of critical or high-severity vulnerabilities emerging in the network.

   These actions can significantly enhance the overall security posture of the organization.

Answers will vary. Some examples are:
• 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.