Module 05: Vulnerability Analysis LAB REPORT

Lara Alofi

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/40a6ee64-ea63-4341-8db1-db5d184651eb?rc=10
2. https://labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20ecf15d185?rc=10
3. https://labclient.labondemand.com/LabClient/ad668ffb-e1a9-4f7d-9f44-d93fae32efcb?rc=10

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab1:

Task 1: Exploring Vulnerabilities with CWE

Common Weakness Enumeration (CWE) is a structured framework for categorizing software vulnerabilities. By logging into the Windows 11 machine and accessing the CWE website via Mozilla Firefox, users can search for vulnerabilities related to specific services, such as SMB.

Through CWE, users can view detailed information about vulnerabilities and explore the CWE Top 25 (2021) list of the most dangerous software weaknesses. This information enables security professionals to identify potential risks and take proactive measures to mitigate them.

By documenting acquired information, users can effectively analyze vulnerabilities and strengthen the security of software systems.

Task 2: Exploring Vulnerabilities with CVE

Common Vulnerabilities and Exposures (CVE) provides a centralized database of standardized identifiers for software vulnerabilities and exposures. Users can access the CVE website through any browser and search for the latest vulnerabilities.

Upon accessing the CVE website, users can find the newest CVE records displayed in the right pane. By searching for specific vulnerabilities using their CVE IDs or names, users can view detailed information about each vulnerability, including its description and references.

In addition to searching by CVE ID or name, users can search for vulnerabilities related to specific services, such as SMB. This allows users to identify vulnerabilities present in target systems and plan mitigation strategies accordingly.

By documenting acquired information, users can effectively analyze vulnerabilities and take proactive measures to enhance system security.

Task 3: Exploring Vulnerabilities with NVD

The National Vulnerability Database (NVD) is the go-to repository for standardized vulnerability data in the U.S. government's arsenal. It automates vulnerability management and aids in security compliance through the Security Content Automation Protocol (SCAP). With NVD, you can search for vulnerabilities by entering https://nvd.nist.gov/ in your browser.

Once on the site, check out the latest vulnerabilities and click on specific CVE-ID links like CVE-2024-1109 to get detailed information. Dive deep into vulnerability assessment using the Common Vulnerability Scoring System (CVSS) calculator to understand severity and impact metrics.

Use the keyword search to find vulnerabilities related to specific services like SMB. This helps you understand underlying vulnerabilities and take proactive security measures. In essence, NVD empowers security professionals to stay ahead of potential threats and strengthen system defenses.

Lab2:

Task 1: Perform Vulnerability Analysis using OpenVAS

OpenVAS is a robust framework offering powerful vulnerability scanning and management solutions. It includes various testing capabilities and a vast database of Network Vulnerability Tests (NVTs), making it a go-to tool for security professionals.

To start, launch OpenVAS on Parrot Security (10.10.1.13) and target Windows Server 2022 (10.10.1.22). Log in to OpenVAS using admin/password credentials and initiate a scan on the target system.

Once the scan is complete, review the results to identify vulnerabilities and their severity. Investigate high-risk vulnerabilities manually for verification.

To test the effectiveness of Windows Firewall, enable it on Windows Server 2022 and rerun the scan. Despite the firewall, vulnerabilities are still detected, highlighting system weaknesses.

Conclude by documenting findings and closing all windows. Ensure the thoroughness of the vulnerability analysis process to fortify system defenses effectively.

Task2: Nessus Vulnerability Scanning:

Nessus is a tool for identifying vulnerabilities, config issues, and malware.

Create a new scanning policy to define how the scan should run.

Set up a scan with the policy, specifying the target's IP address.

then, Launch the scan and wait for it to finish

after that, Review the results to see vulnerabilities categorized by severity.then, sign out of Nessus to wrap up the assessment.

I learned how to use Nessus for comprehensive vulnerability scanning, from setting up policies to analyzing scan results and generating reports for further analysis and action.

Task3: Performing Web Servers and Applications Vulnerability Scanning using Nikto:

Nikto is an open-source web server scanner used for comprehensive tests against web servers.

Open Nikto in the Terminal window on the Parrot Security machine.

Type the command to initiate Nikto scanning options and view available commands.

Use the Tuning option for a deeper and more comprehensive scan on the target web server.

Initiate Nikto scan with tuning options enabled for the target website (e.g., https://www.certifiedhacker.com).

Check for CGI directories using the-Cgidirs option, specifying specific directories or scanning all available directories.

Save the scan results in a text file on the Desktop for further analysis.

Open the created file in a text editor window to review the scanned results.

Nikto provides valuable insights into vulnerabilities in web servers and applications, aiding in enhancing security measures.

I learned how to use Nikto for conducting vulnerability scans on web servers and applications, including initiating scans, analyzing results, and saving reports for further review and documentation.