Introduction to Vulnerability Analysis Project

Overview

As part of my role as an ethical hacker with the EC-Council, I undertook a comprehensive vulnerability analysis project. This project focused on identifying and analyzing potential security weaknesses within a target network. By leveraging information acquired during the footprinting and scanning phases, I was able to conduct a thorough investigation into the network's vulnerabilities.

Objectives

The main objectives of this project were to extract critical information about the target network, including:

- **Network Vulnerabilities:** Identification of network vulnerabilities, listening IPs, TCP/UDP ports, and services.
- **Application and Service Configuration Errors:** Detection of configuration errors and vulnerabilities within applications and services.
- **Operating System and Applications:** Enumeration of the operating systems and applications in use.
- **Weak Passwords and Permissions:** Identification of weak passwords and improper permissions.
- **Default Services and Applications:** Recognition of default services and applications that may need to be removed or secured.

Tasks and Techniques

To achieve these objectives, a variety of tasks were performed using multiple tools and techniques. These tasks provided practical experience in several enumeration techniques essential for ethical hacking and penetration testing. Key tasks included:

Vulnerability Research: Utilizing vulnerability scoring systems and databases to perform thorough research, including Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE).

Vulnerability Assessment: Conducting vulnerability assessments using tools such as OpenVAS and Nessus, which involved:

- Performing scans to identify vulnerabilities.
- Analyzing scan results to determine the severity of discovered vulnerabilities.

Web Server and Application Scanning: Using tools like CGI Scanner Nikto to identify vulnerabilities in web servers and applications.

Gerren Jerome - Vulnerability Analysis

Tools Utilized

The project involved the use of several key tools to perform vulnerability assessments and analyses:

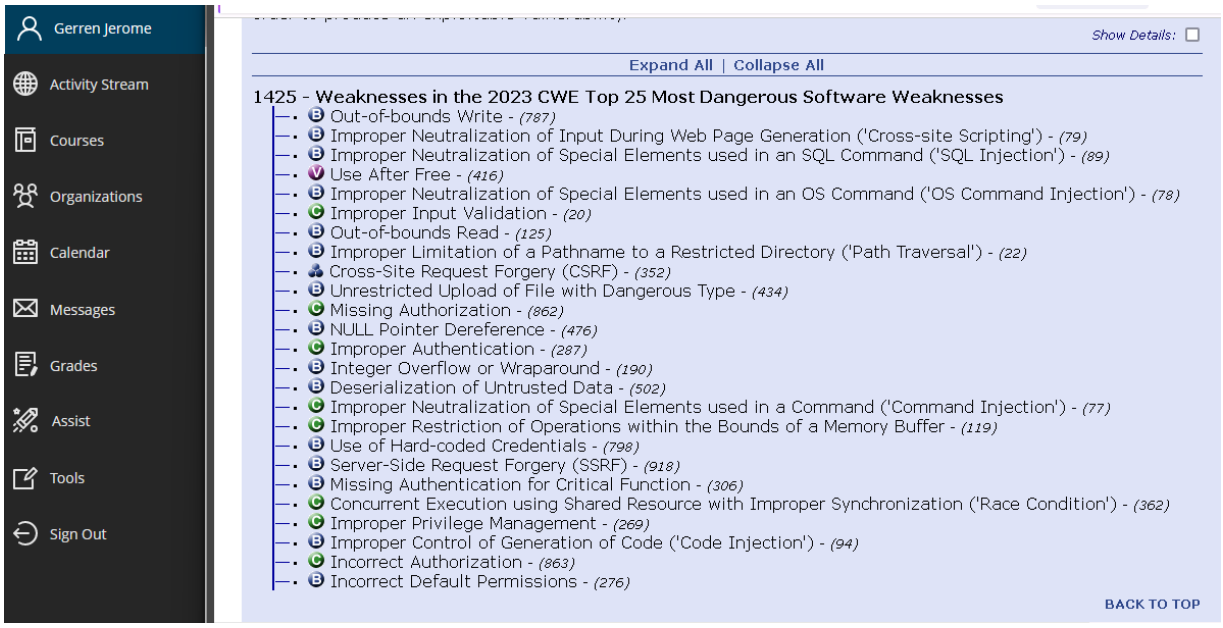
- OpenVAS: For comprehensive vulnerability scanning and analysis.
- Nessus: To conduct detailed vulnerability scans and assess security weaknesses.
- CGI Scanner Nikto: For scanning web servers and applications to detect potential vulnerabilities.

Perform vulnerability research with vulnerability scoring systems and databases.

Perform vulnerability research in Common Weakness Enumeration (CWE)

CWE search results (SMB)

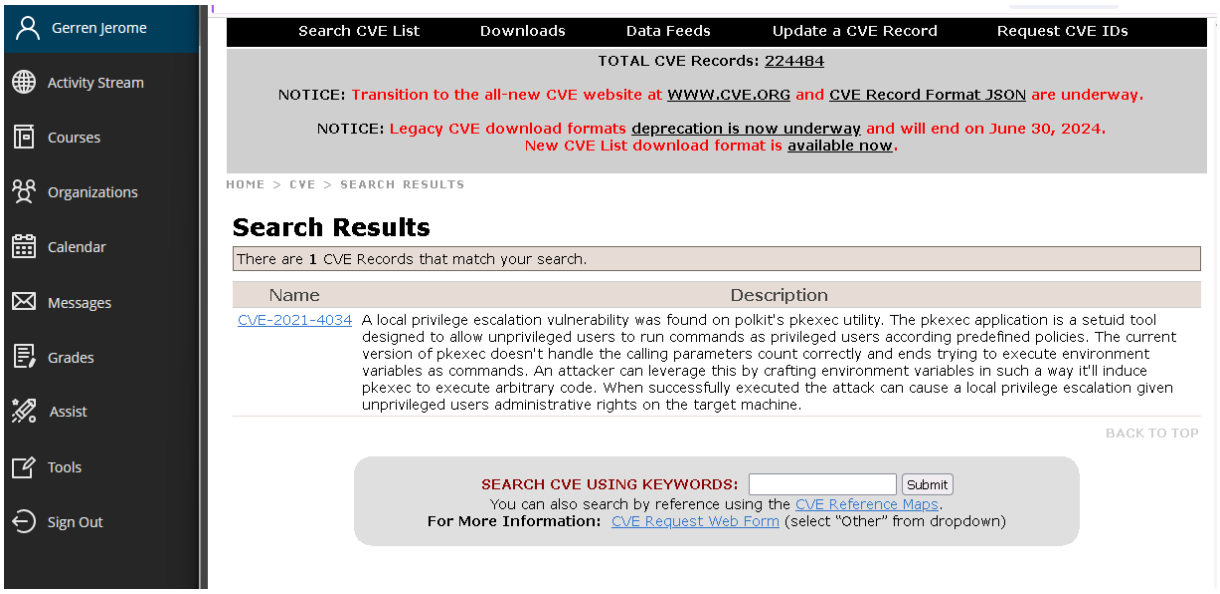
Top 25 Most Dangerous Software Weaknesses (CWE VIEW)



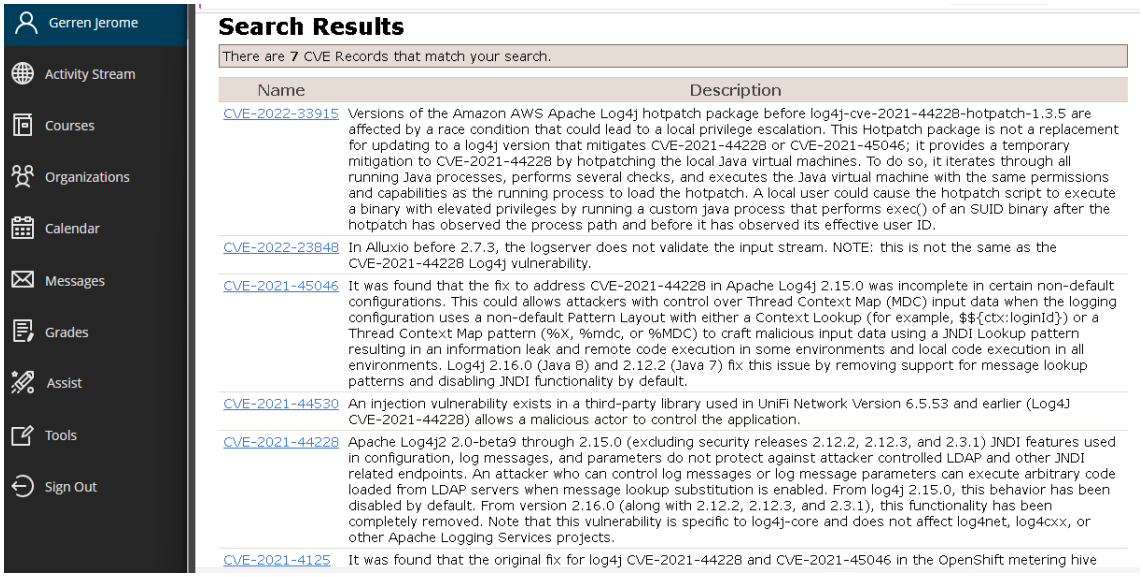
Gerren Jerome - Vulnerability Analysis

Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)

CVE Search (CVE-2021-4034)

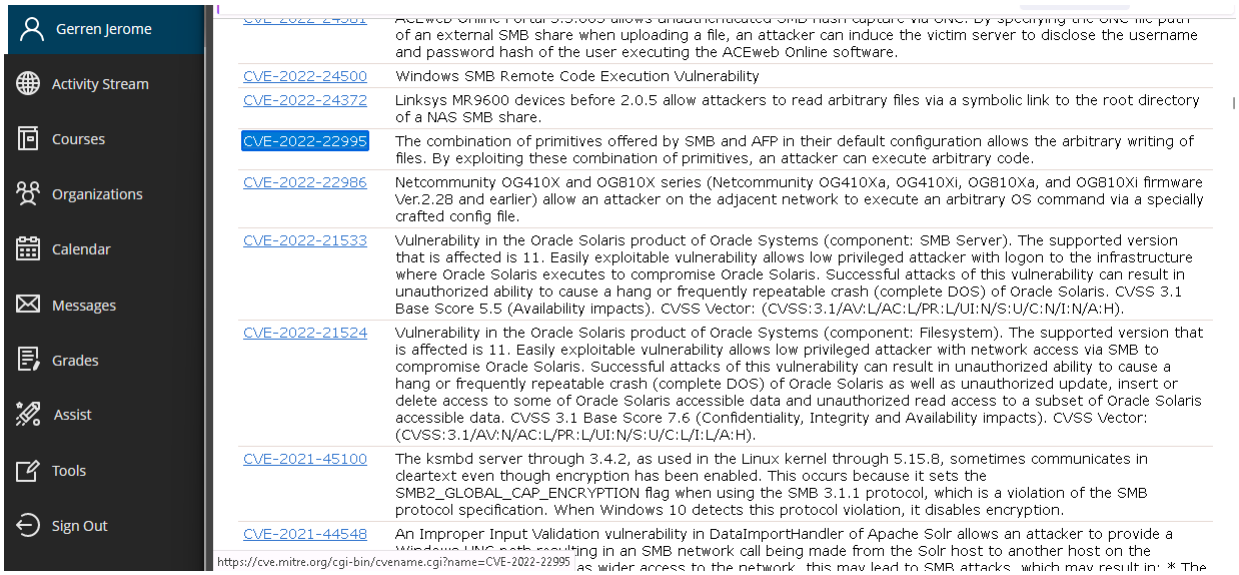


CVE Search (CVE-2021-44228)



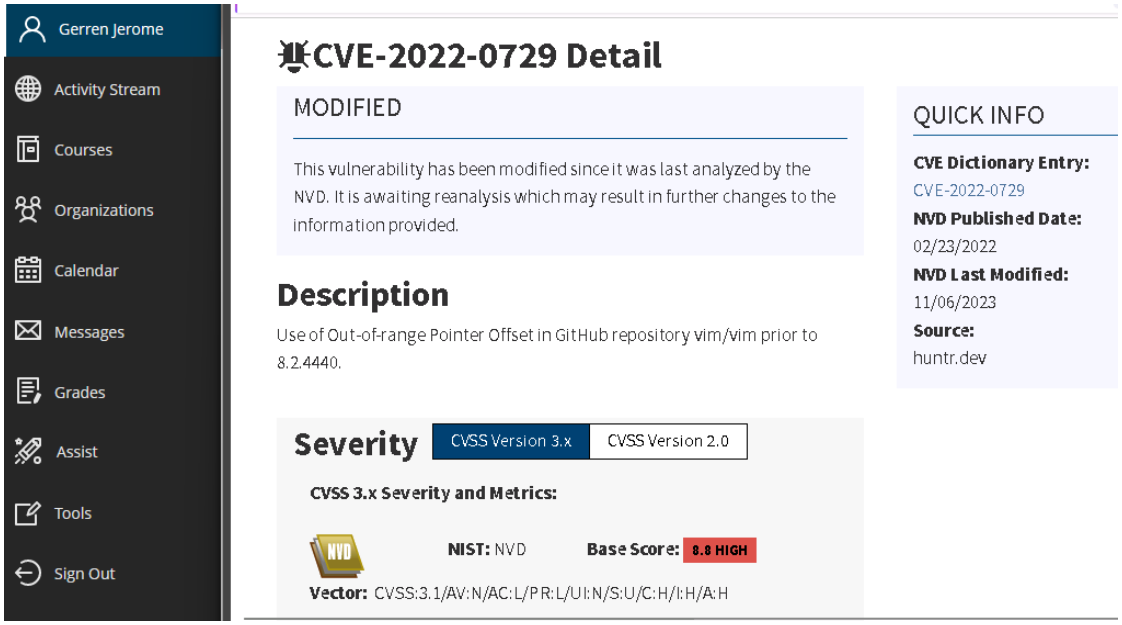
Gerren Jerome - Vulnerability Analysis

CVE Search (CVE-2022-22995



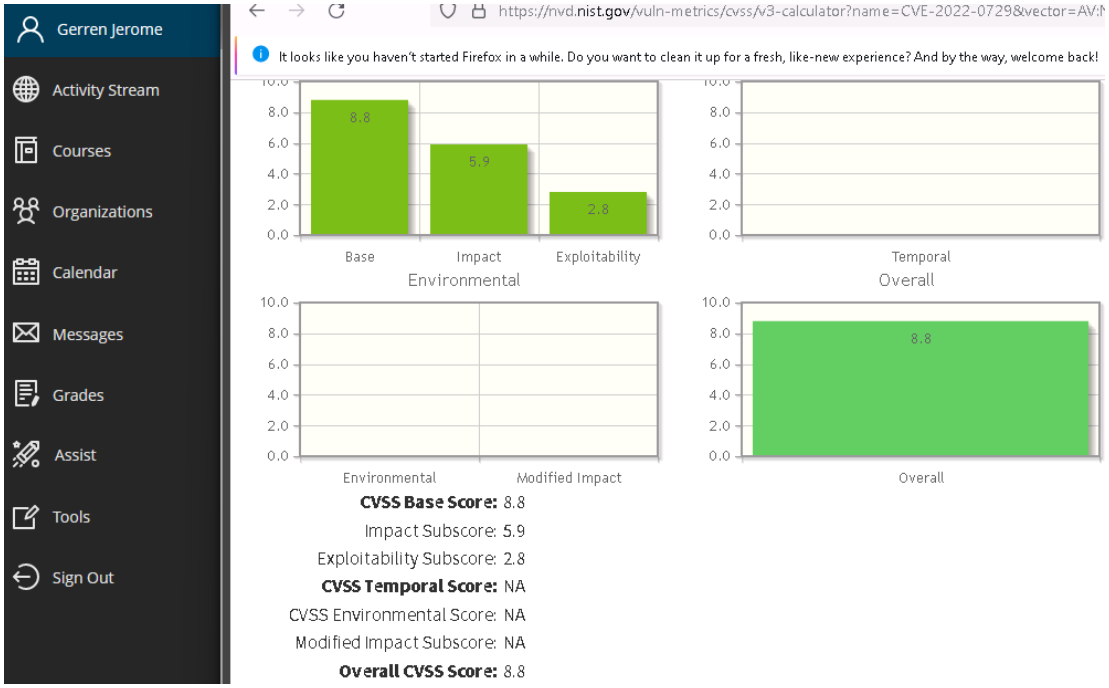
Perform vulnerability research in National Vulnerability Database (NVD)

NVD Search (CVE-2022-0729)

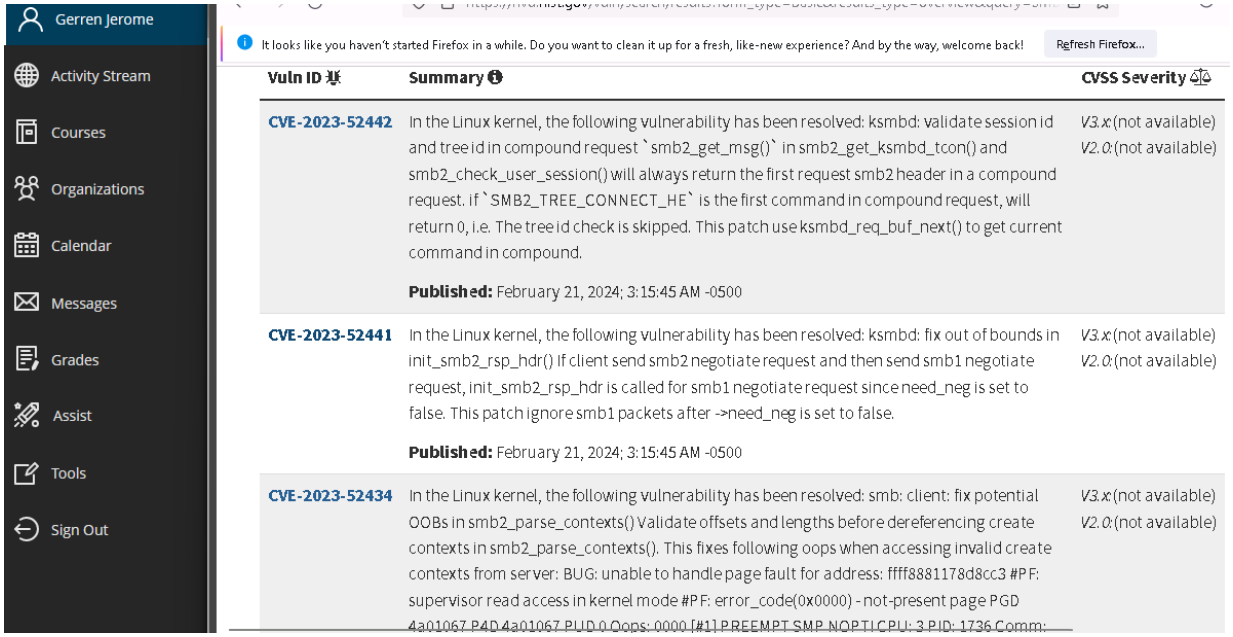


Gerren Jerome - Vulnerability Analysis

Graphical Score Representation (CVE-2022-0729)



NVD Search (SMB)

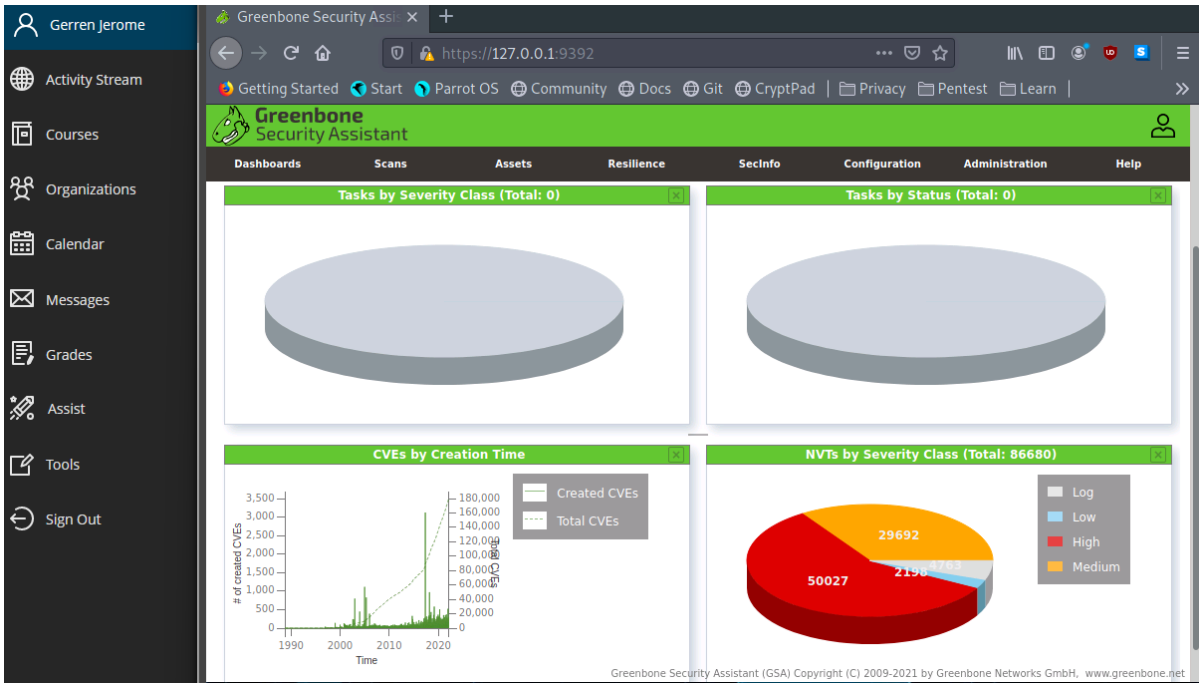


Gerren Jerome - [Vulnerability Analysis]

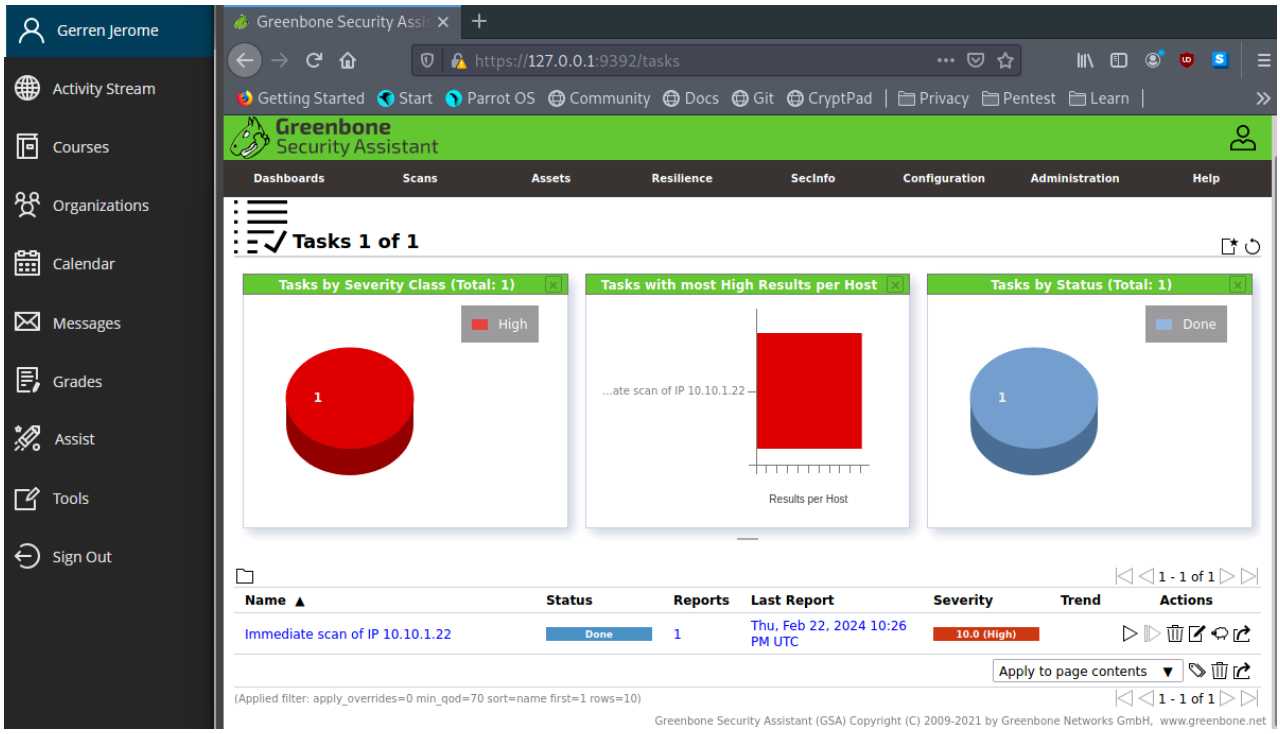
Perform vulnerability assessment using various vulnerability assessment tools.

Perform vulnerability analysis using OpenVAS (5 tasks)

OpenVAS Dashboard post-login

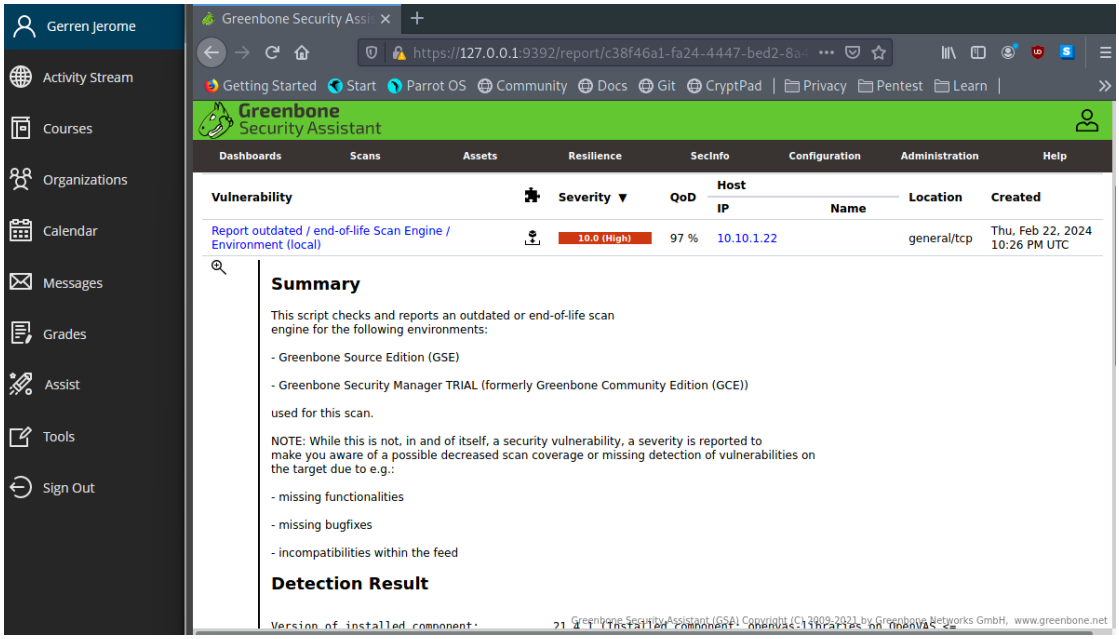


OpenVAS scan completed.

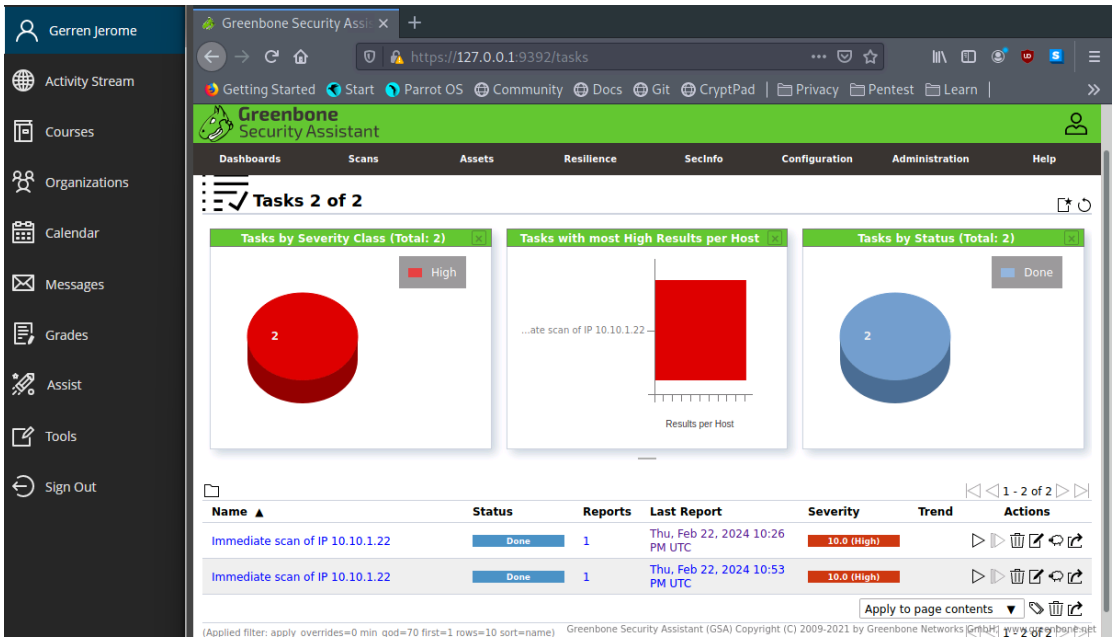


Gerren Jerome - [Vulnerability Analysis]

Detailed results re: vulnerability under “Report outdated/end of life/scan engine/Environment (local)”

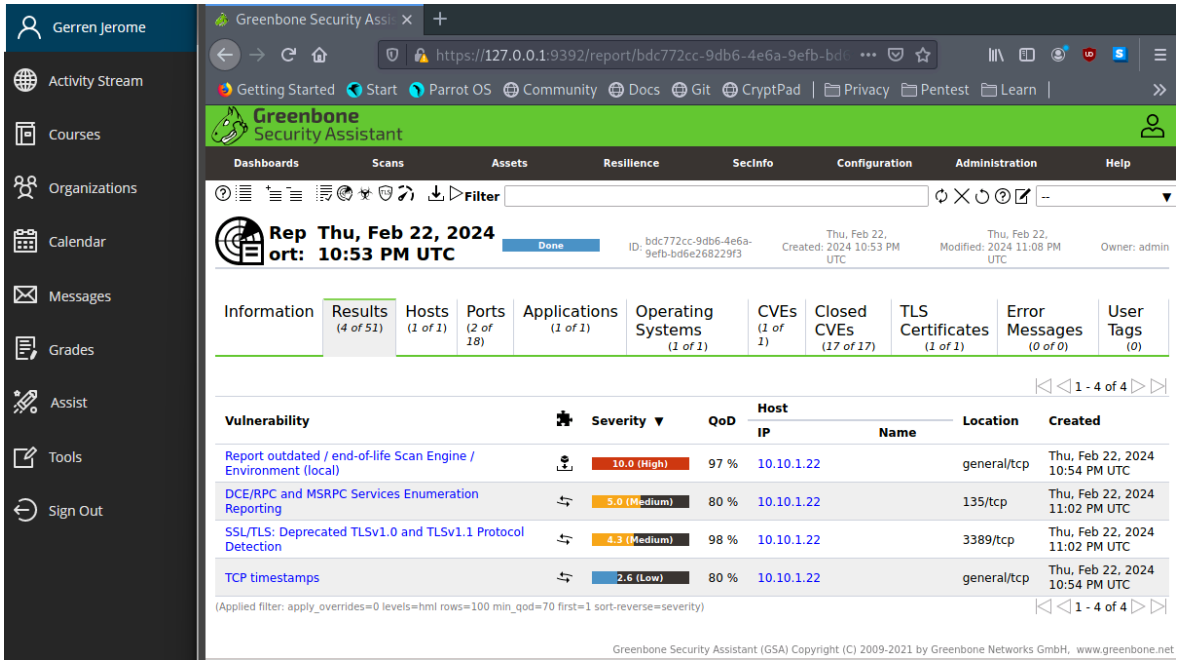


New task in OpenVAS’ Tasks section



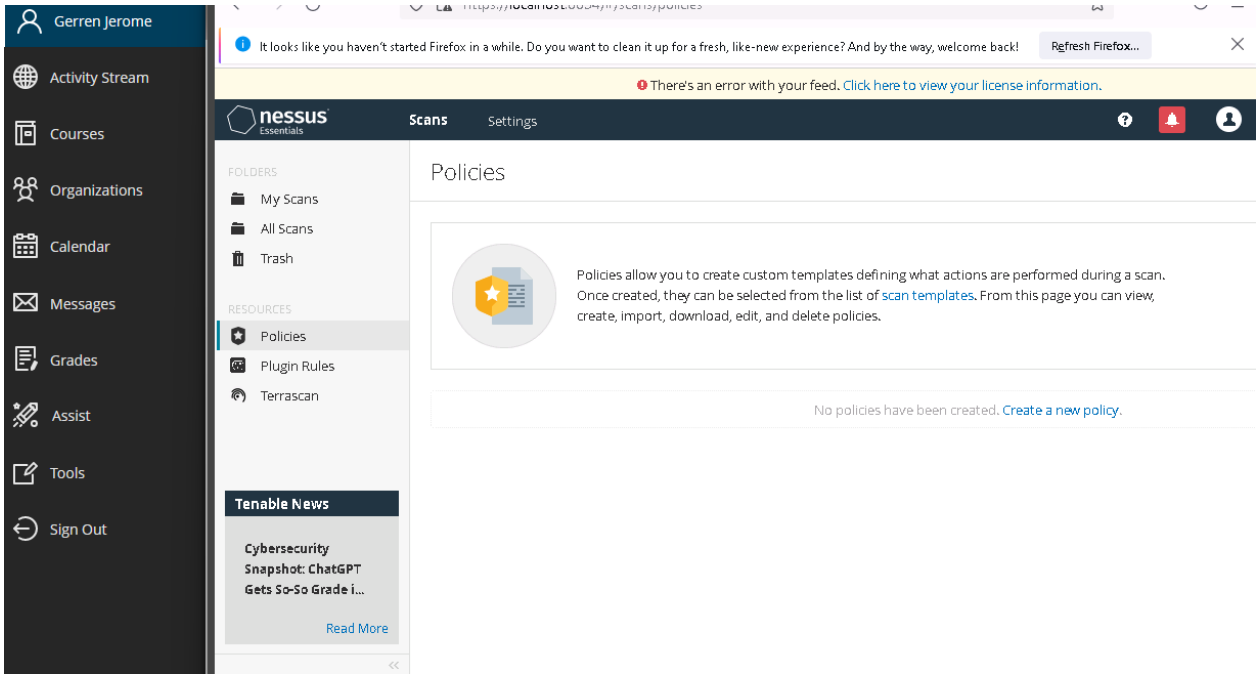
Gerren Jerome - [Vulnerability Analysis]

Report results (Severity of vulnerabilities)



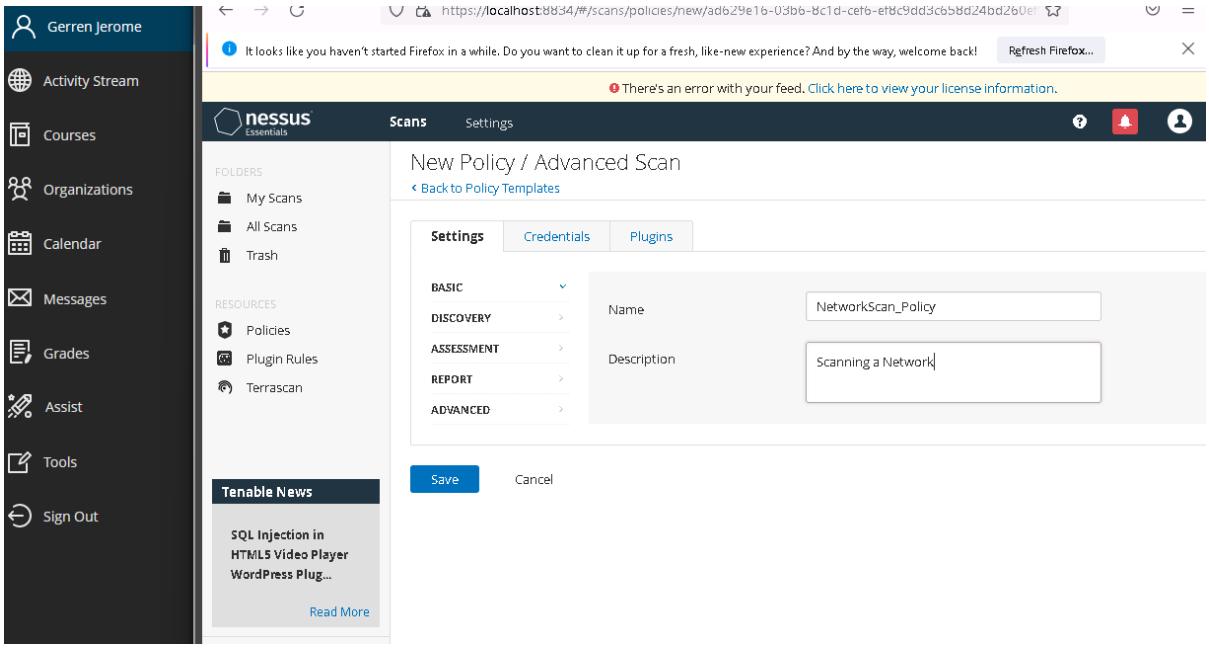
Perform vulnerability scanning using Nessus.

Nessus Dashboard post-login

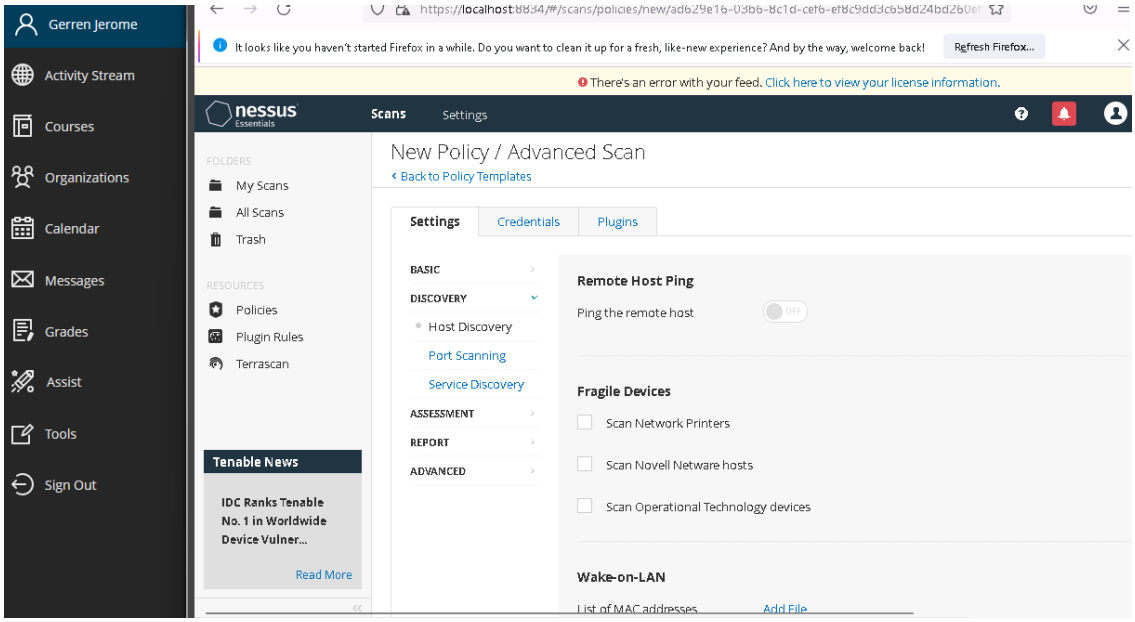


Gerren Jerome - [Vulnerability Analysis]

Nessus Advanced Scan settings – BASIC

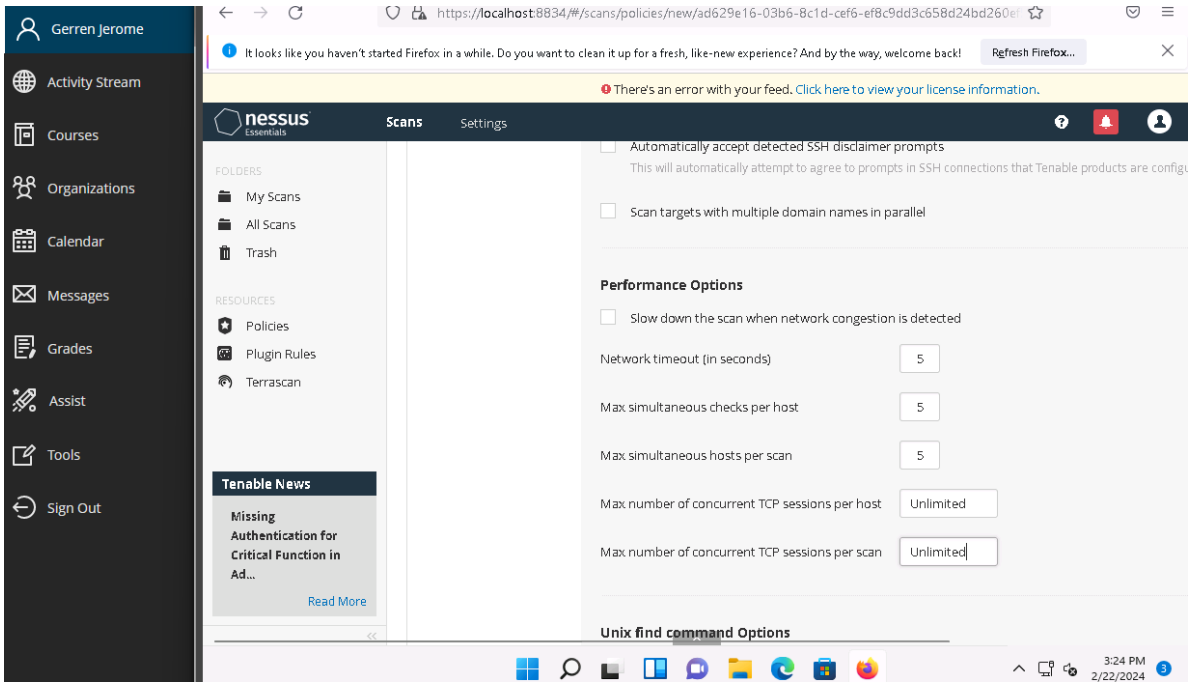


Nessus Advanced Scan settings – DISCOVERY

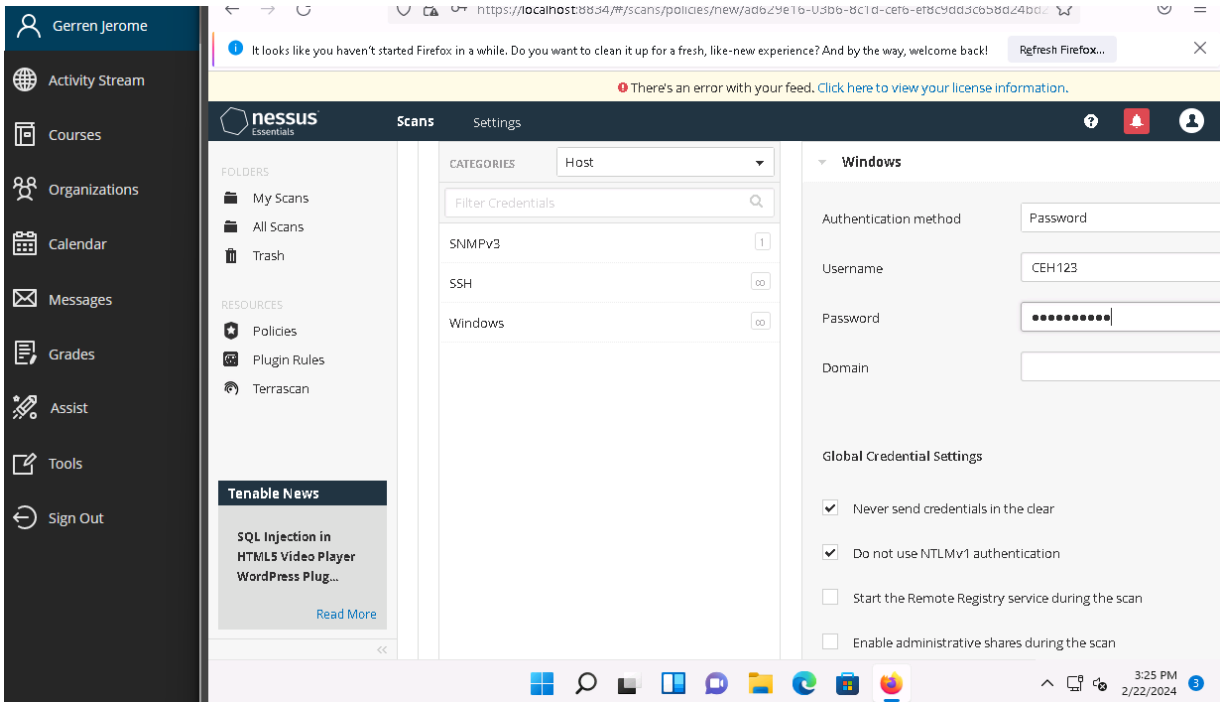


Gerren Jerome - Vulnerability Analysis

Nessus Advanced Scan settings – ADVANCED

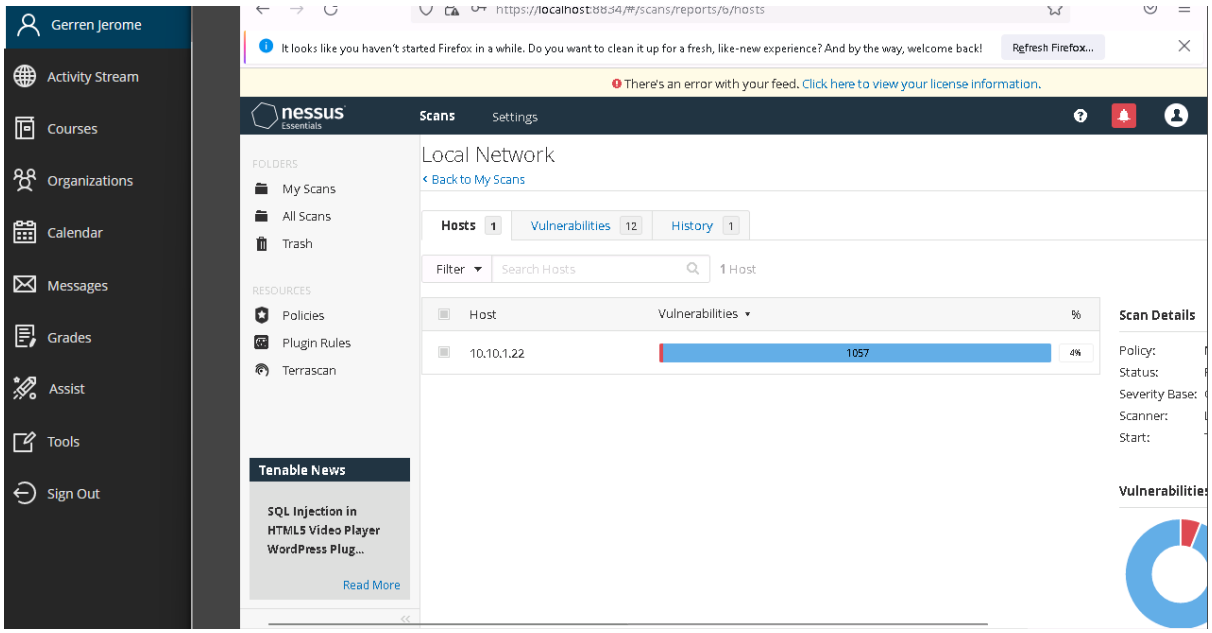


Specify username and password for Windows credentials.

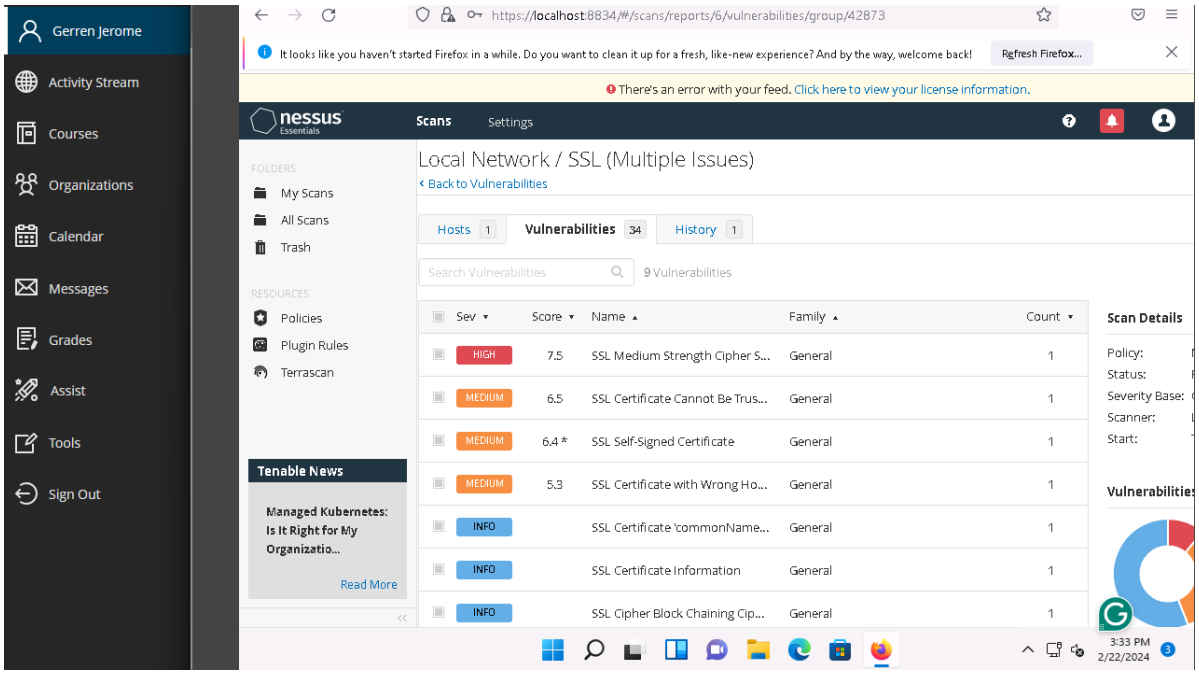


Gerren Jerome - Vulnerability Analysis

Confirm scan is saved and launched successfully.



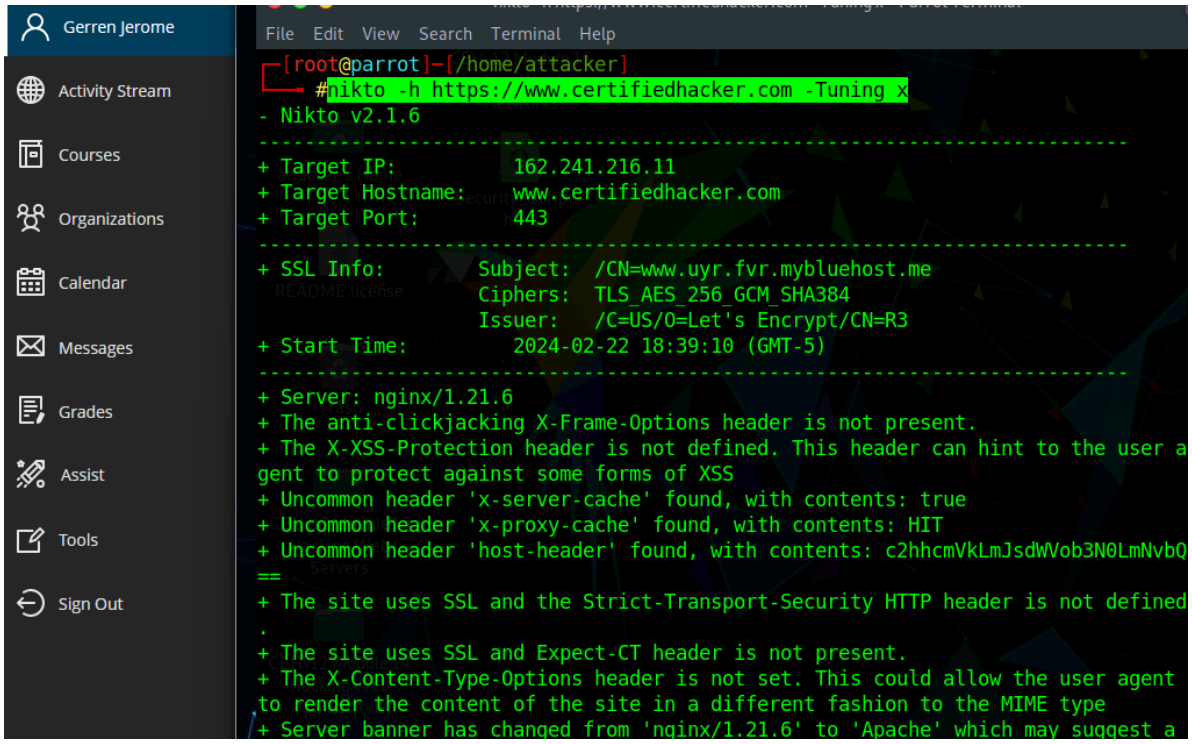
Results of Nessus vulnerability scan (SSL)



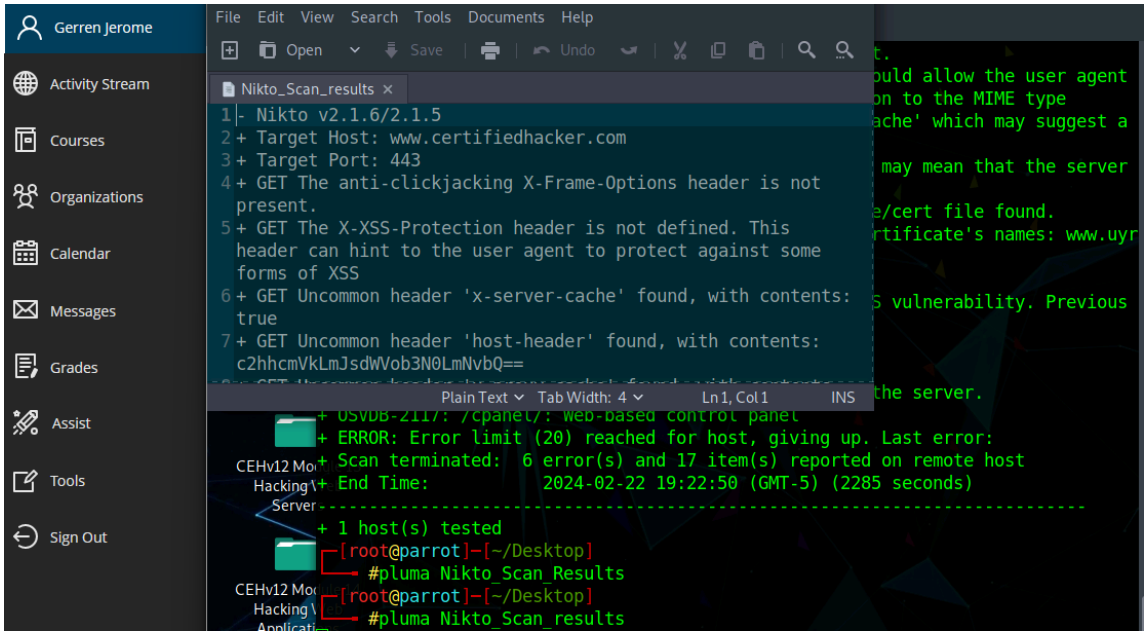
Gerren Jerome - Vulnerability Analysis

Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

Results (Nikto -h TARGET -Tuning x)



Open Nikto scan results in Pluma to audit scan results.



Reflection

This project provided hands-on experience with various enumeration techniques and tools critical for effective ethical hacking and penetration testing. Through this project, I developed a deeper understanding of how to identify, analyze, and mitigate potential security threats within a network.