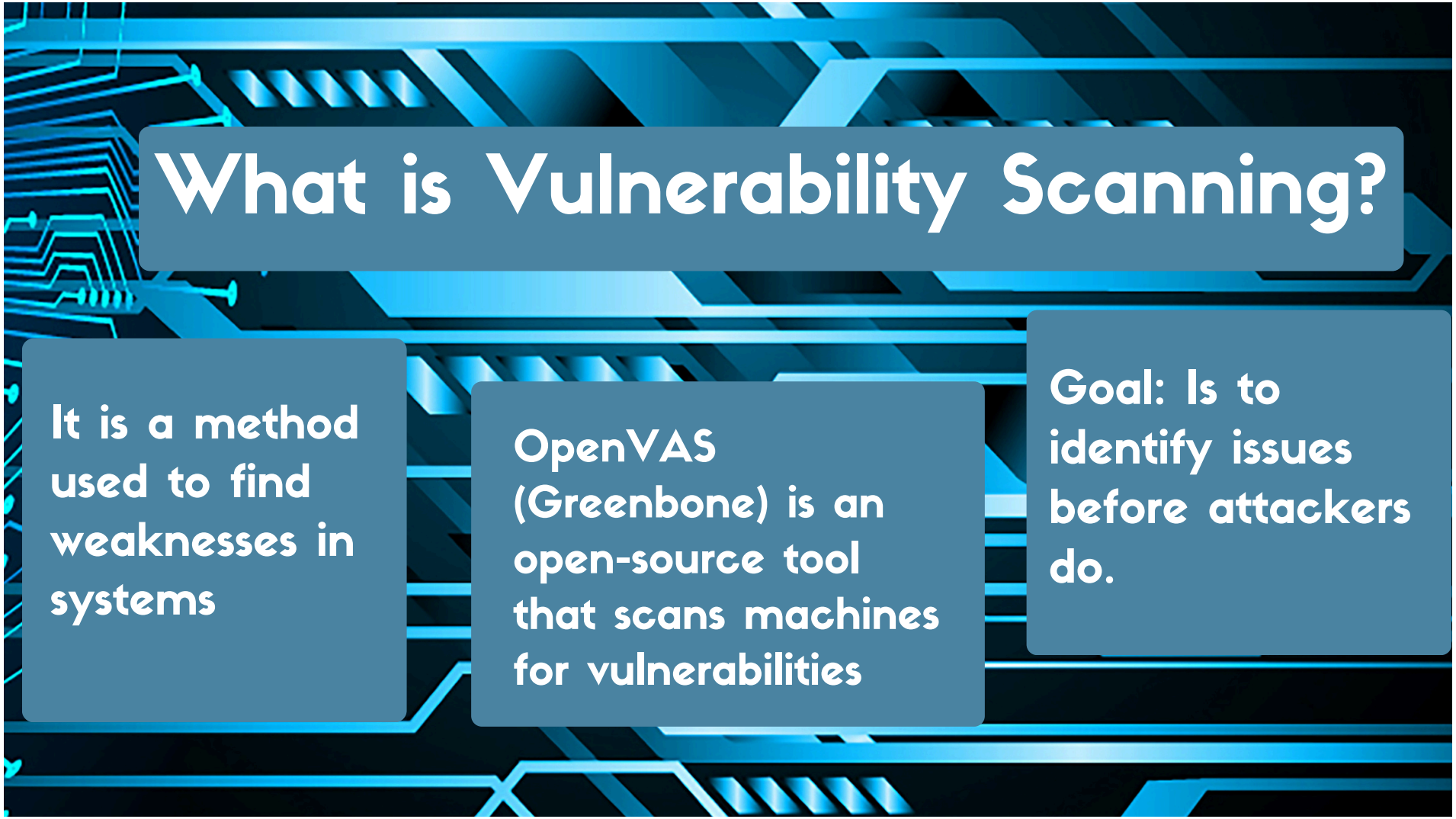
ADVANCED VULNERABILITY MANAGENMENT WORKFLOW :

Threat Detection, CVSS Prioritization & Remediation Planning Using OpenVAS

BY JACINTA IZUNDU

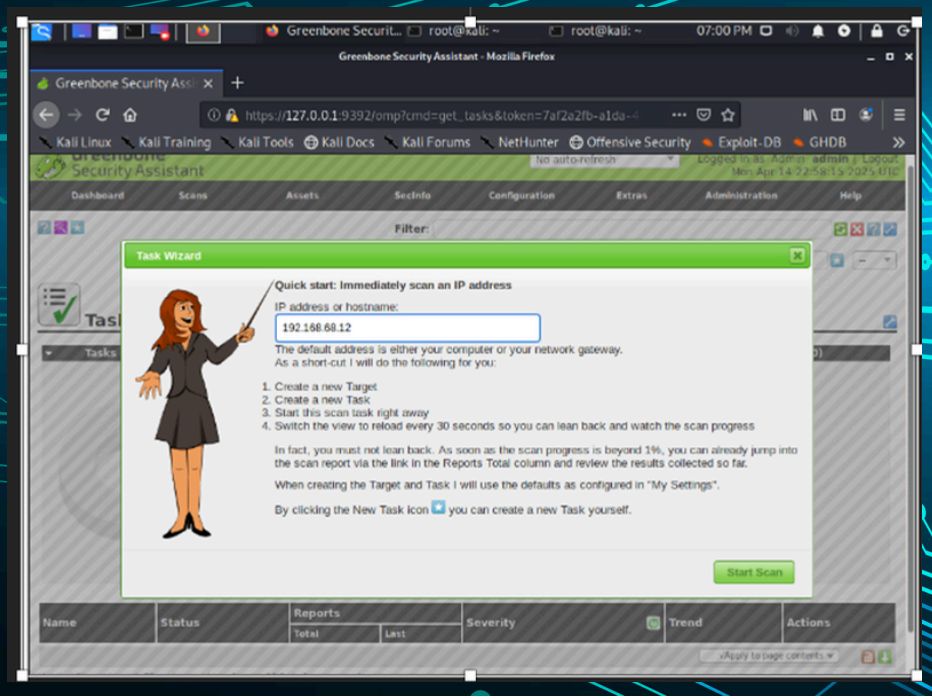

What is Vulnerability Scanning?
It is a method used to find weaknesses in systems
OpenVAS (Greenbone) is an open-source tool that scans machines for vulnerabilities
Goal: Is to identify issues before attackers do.

Lab Enviroment Overview

- I used Kali Linux to run OpenVAS
- I scan the OWASP Broken Web Application server at 192.168.68.12

Starting OpenVAS

- I logged into kali as root
- Started OpenVAS service
- Logged into Greenbone Security Ass

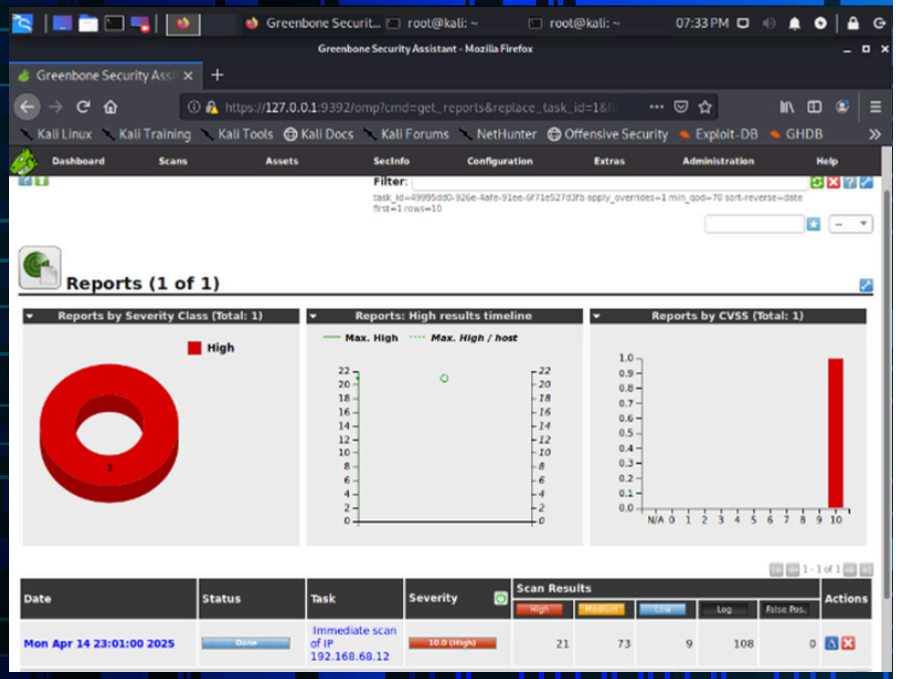


Viewing Security Dashboard

- The dashboard shows vulnerability tests, risk levels and CVEs
- This helps understand what kinds of threats exist.

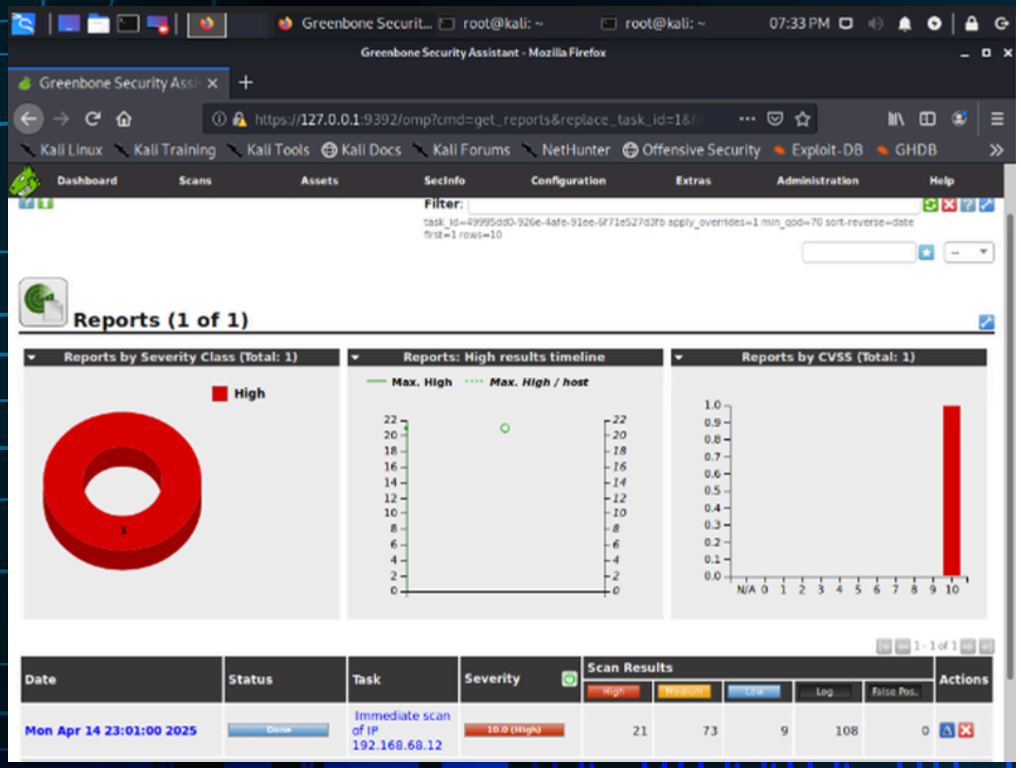
Using The CVSS Calculator

- CVSS scores help rate how serious a vulerability is
- OpenVas includes a built-in calculator.



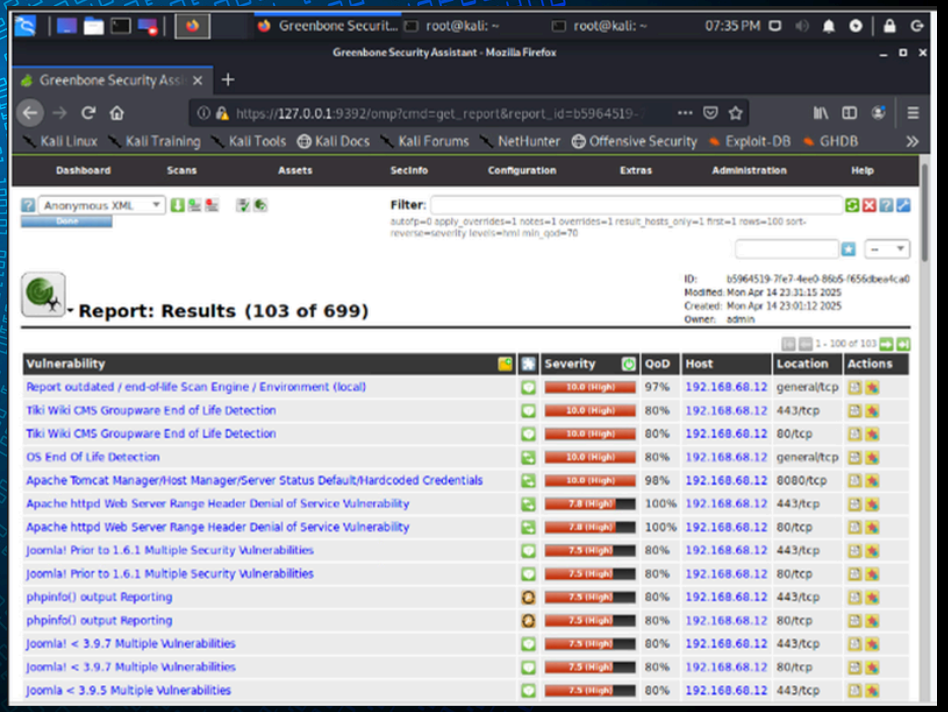
Creating a Quick Scan

- Opened Scans → Tasks
- Used the purple wizard to start a quick scan
- Entered the target IP: 192.168.68.12



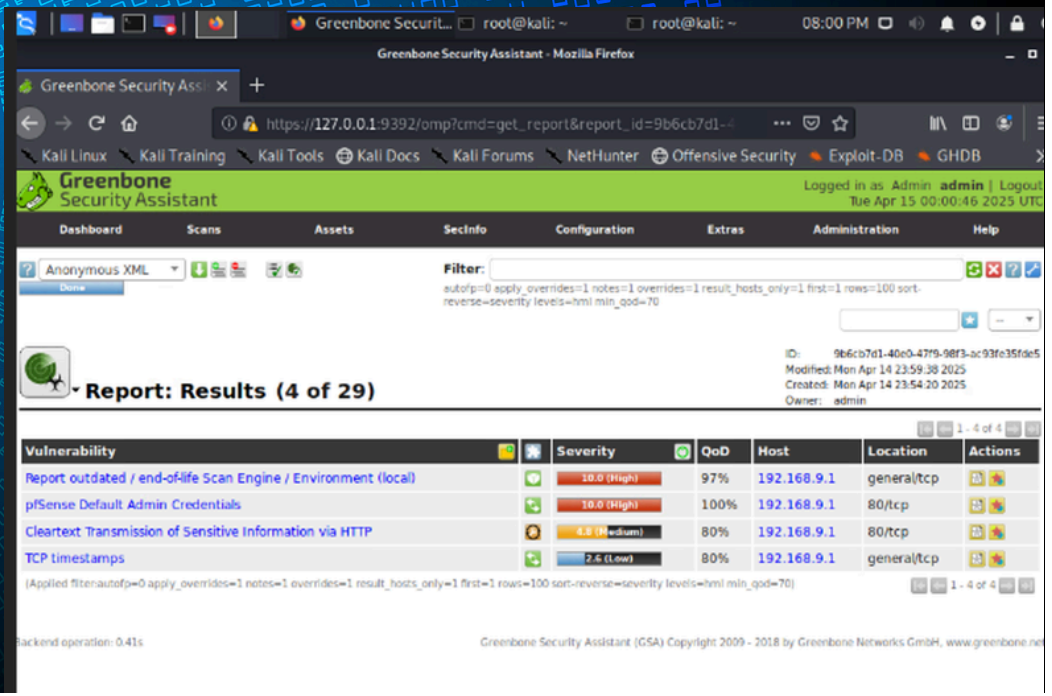
Running The Quick Scan

- The scan runs for 10-20 minutes
- OpenVas checks for known vulnerabilities



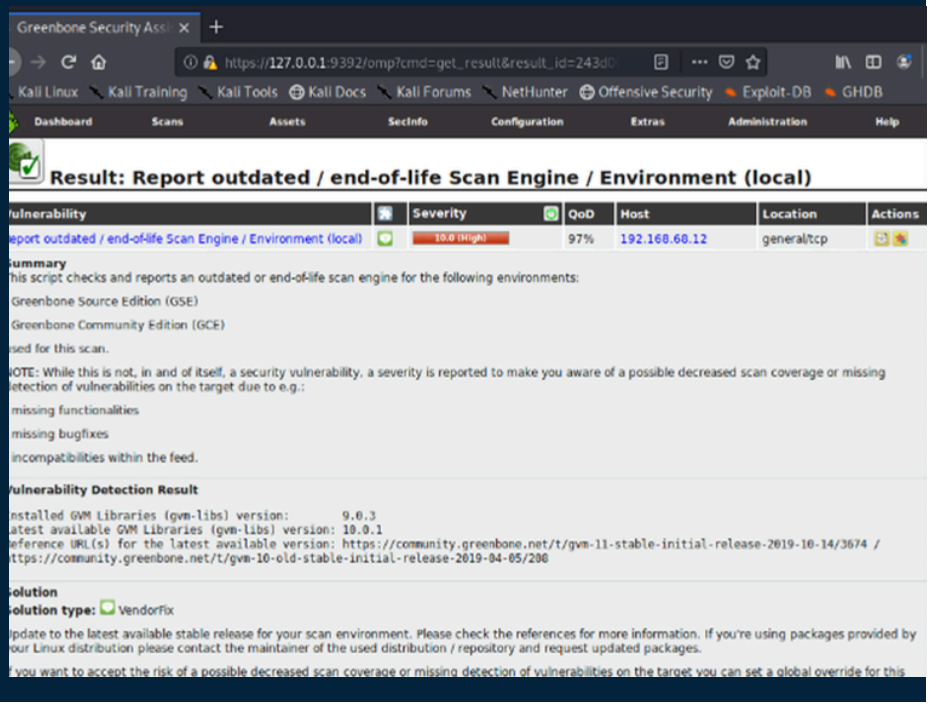
Viewing Quick Scan Report

- After scan completes, I clicked report link
- Viewed report discovered vulnerabilites



Quick Scan Summary Report

This report tells a penetration tester that the organization's security tools are outdated. That's like a guard looking over your house with old blueprints; they won't see new backdoors. It's a chance for the tester to exploit what the scan can't see or advise the company to update their tools.

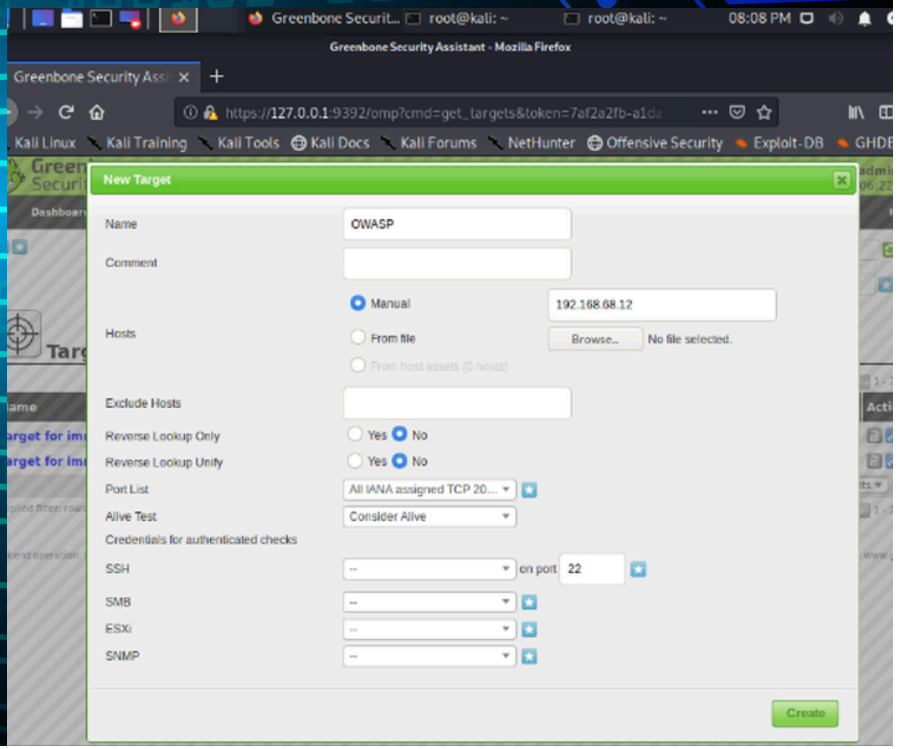


Creating a Custom Scan Config

- Went to Configuration → Scan Configs
- Selected Full and Very Deep Ultimate
- This scan is more detailed than the quick scan

Creating a New Target

- Created a new scan target named OWASP
- Set host to: 192.168.68.12
- Selected Consider Alive

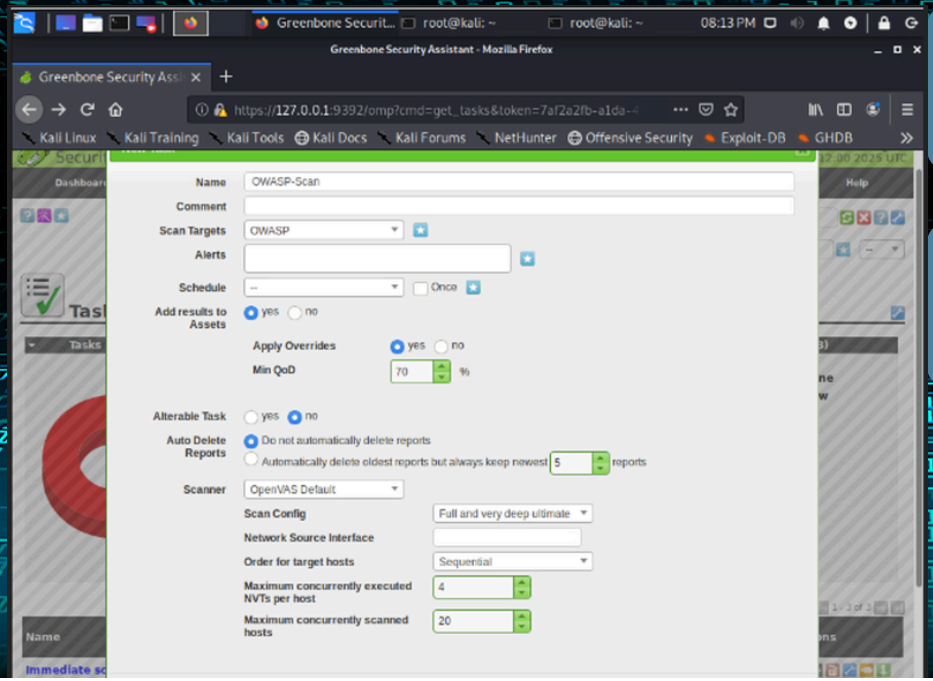


Creating the Custom Scan Task

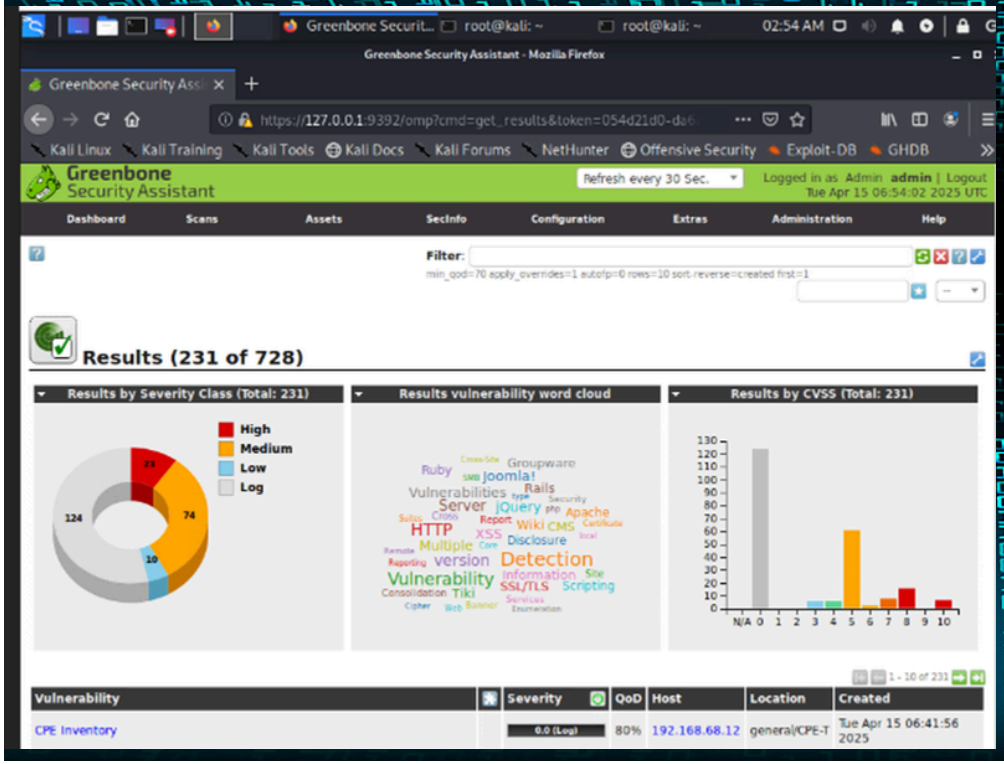
I created a new task named OWASP-SCAN

Used the previously created target

Selected Full and Very Deep Ultimate scan config



Running the Custom Scan



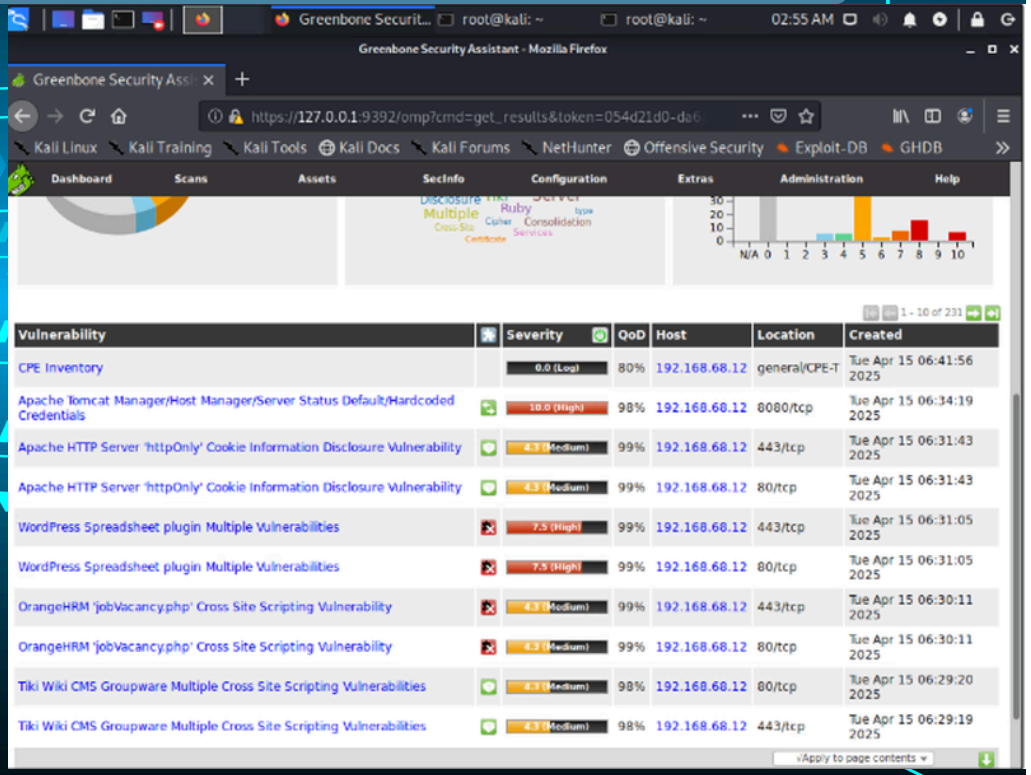
Started the Scan

This takes longer because it checks more vulnerabilities

Can stop early if needed

Viewing Scan Results

- Checked results for vulnerabilities
- Noted severity levels (Low, Medium, High, Critical)
- These results guide remediation



Key Lessons Learned

- Vulnerability scanning helps identify risks early
- Quick Scans = Fast overview
- Deep Scans = Detalied findings
- OpenVAS is powerful free tool for real-world security assessments

THANK YOU

Thank you for being part of the secure digital journey.
Together, we create a safer internet for everyone.

+1-217-670-4436

clemsjacy@gmail.com

LinkedIn http://linkedin.com/in/jacinta-izundu-b36a20233