

ADVANCED VULNERABILITY MANAGEMENT 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

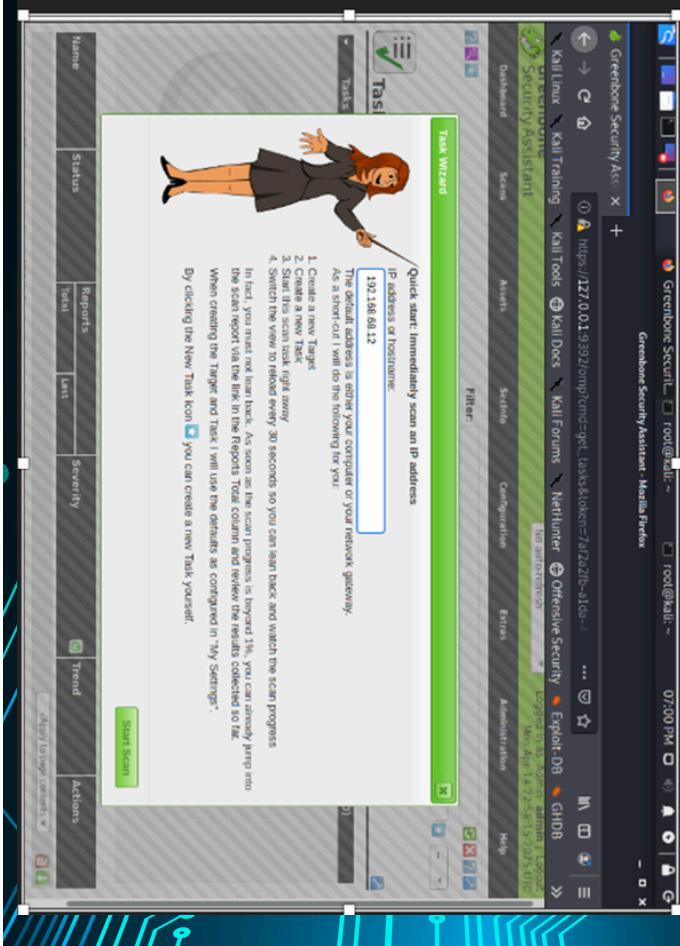
Goal: Is to identify issues before attackers do.

Lab Environment 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 Assistant**
- Greenbone Security Assistant



Viewing Security Dashboard

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

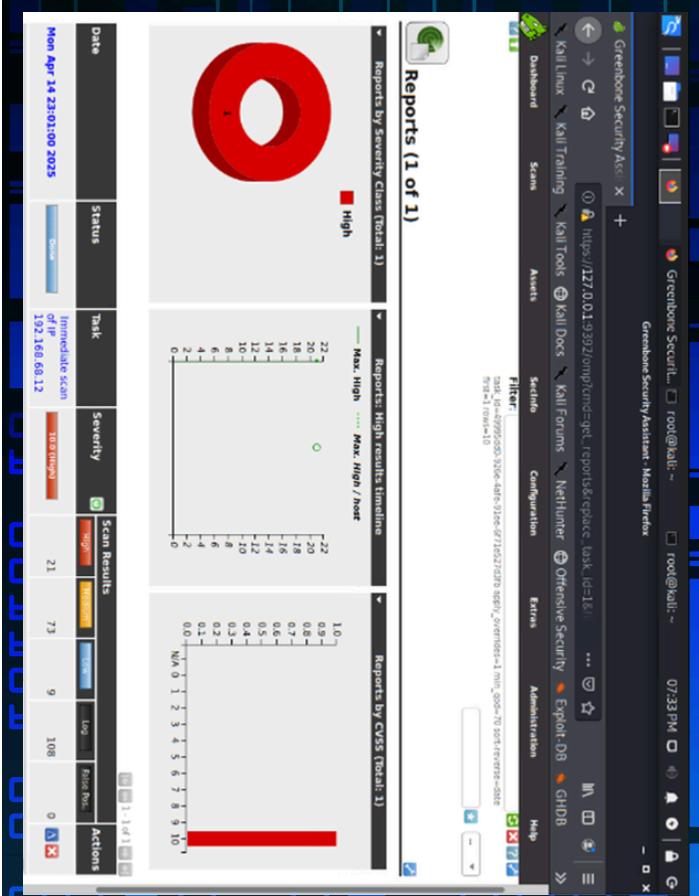
Using The CVSS Calculator

- CVSS scores help rate how

serious a vulnerability is

- OpenVas includes a built-in

calculator.

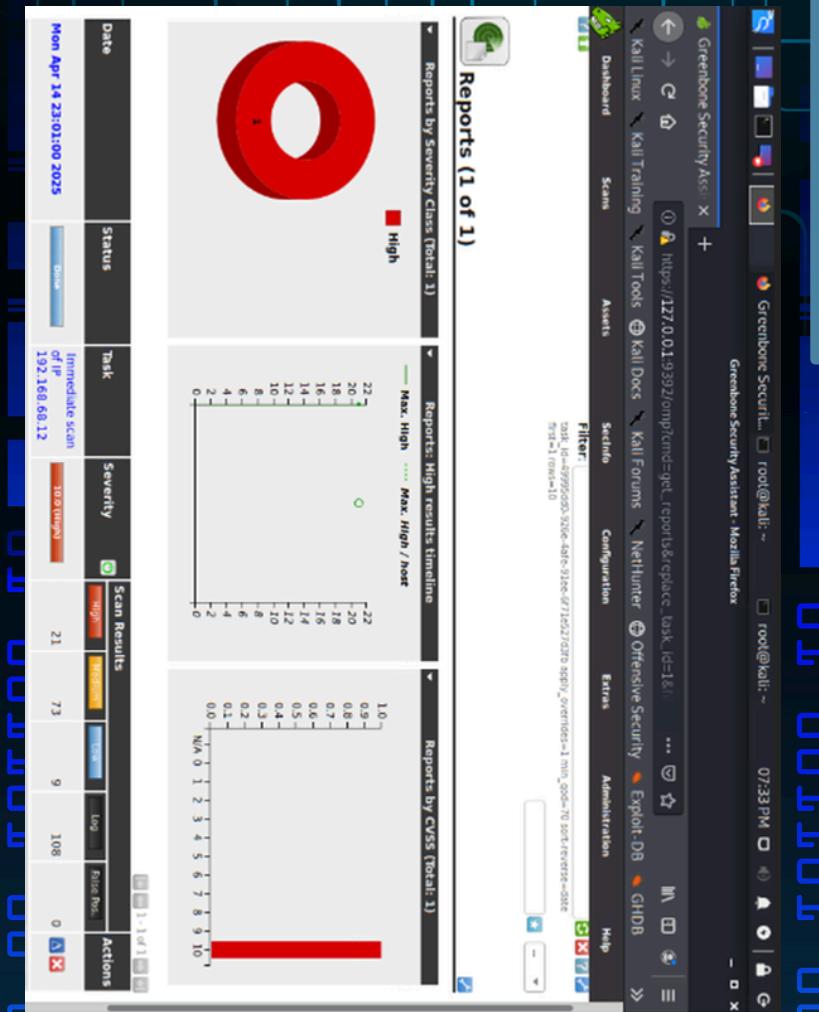


Creating a Quick Scan

- 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

Report: Results (103 of 699)

Vulnerability	Severity	QID	Host	Location	Actions		
Tiki Wiki CMS Groupware End of Life Detection	Info (Info)	97%	192.168.68.12	general/tcp			
Tiki Wiki CMS Groupware End of Life Detection	Info (Info)	80%	192.168.68.12	443/tcp			
OS End of Life Detection	Info (Info)	80%	192.168.68.12	80/tcp			
Apache Tomcat Manager Web Application Vulnerability	Info (Info)	80%	192.168.68.12	general/tcp			
Apache Tomcat Manager Web Application Vulnerability	Info (Info)	98%	192.168.68.12	80/tcp			
Apache Tomcat Manager Web Application Vulnerability	Info (Info)	100%	192.168.68.12	443/tcp			
Apache Nginx Web Server Range Header Denial of Service Vulnerability	Info (Info)	80%	192.168.68.12	443/tcp			
Apache Nginx Web Server Range Header Denial of Service Vulnerability	Info (Info)	100%	192.168.68.12	80/tcp			
Journalist Prior to 1.6.1 Multiple Security Vulnerabilities	Info (Info)	80%	192.168.68.12	80/tcp			
Journalist Prior to 1.6.1 Multiple Security Vulnerabilities	Info (Info)	80%	192.168.68.12	443/tcp			
Journalist < 3.9.5 Multiple Vulnerabilities	Info (Info)	80%	192.168.68.12	80/tcp			
Journalist < 3.9.5 Multiple Vulnerabilities	Info (Info)	80%	192.168.68.12	443/tcp			

After scan completes, I clicked viewed report discovered report link

The screenshot shows the Greenbone Security Assistant (GSA) interface. The title bar reads "Greenbone Security Assistant - Mozilla Firefox". The main content area is titled "Report: Results (4 of 29)". The table displays the following data:

Vulnerability	Severity	QoD	Host	Location	Actions
Report outdated / end-of-life Scan Engine / Environment (local)	20.8 (High)	97%	192.168.9.1	general (tcp)	
Insufficient Admin Credentials	10.0 (High)	100%	192.168.9.1	80/tcp	
ClearText Transmission of Sensitive Information via HTTP	4.3 (Medium)	80%	192.168.9.1	80/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.9.1	general (tcp)	

At the bottom of the table, a note states: "(Applied filters: and=0 apply_overrides=1 negate=1 override=1 result_noze_only=1 first=1 max=100 sort=-severity level=0 min_qod=70)"

On the left side of the interface, there is a sidebar with icons for "Anonymous XML", "Scans", "Assets", "Scoring", "Configuration", "Extra", and "Administration". The "Scans" tab is currently selected. The "Scans" tab has a sub-menu with "Dashboard", "Scans", "Assets", "Scoring", "Configuration", "Extra", and "Administration". The "Scans" sub-menu is also selected.

The status bar at the bottom left shows "Backend operation: 0.41s".

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.

Result: Report outdated / end-of-life scan Engine / Environment (local)

Vulnerability	Severity	QoD	Host	Location	Actions
Report Outdated / end-of-life Scan Engine / Environment (local)	12.8 High	97%	192.168.60.12	general:tcp	

summary
This script checks and reports an outdated or end-of-life scan engine for the following environments:

Greenbone Source Edition (GSE)
Greenbone Community Edition (GCE)

used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.: missing functionalities, missing bugfixes, incompatibilities within the feed.

vulnerability detection result

installed GSN Libraries (gnl-lib) version: 9.0.3
latest available GSN Libraries (gnl-lib) version: 10.0.1
reference URL(s) for the latest available version: <https://community.greenbone.net/t/gnl-11-stable-initial-release-2019-10-14/2874/>

solution vendor fix

note to the user: available stable release for your scan environment. Please check the references for more information. If you're using packages provided by our Linux distribution please contact the maintainer of the user distribution / repository and request updated packages.

You want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this

Creating a Custom Scan Config

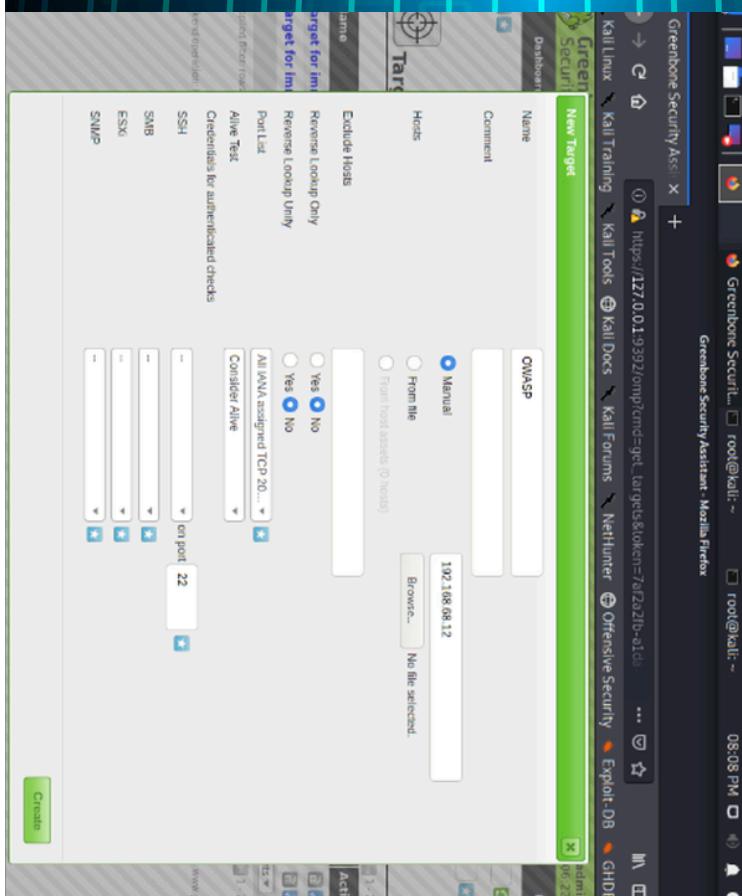
- Went to Configuration → Scan Configs
- Selected Full and Very Deep Ultimate
- This scan is more detailed than the quick scan

Creating a New Target

- Created a new scan target named OWASP

Set host to: 192.168.68.12

Selected Consider Alive

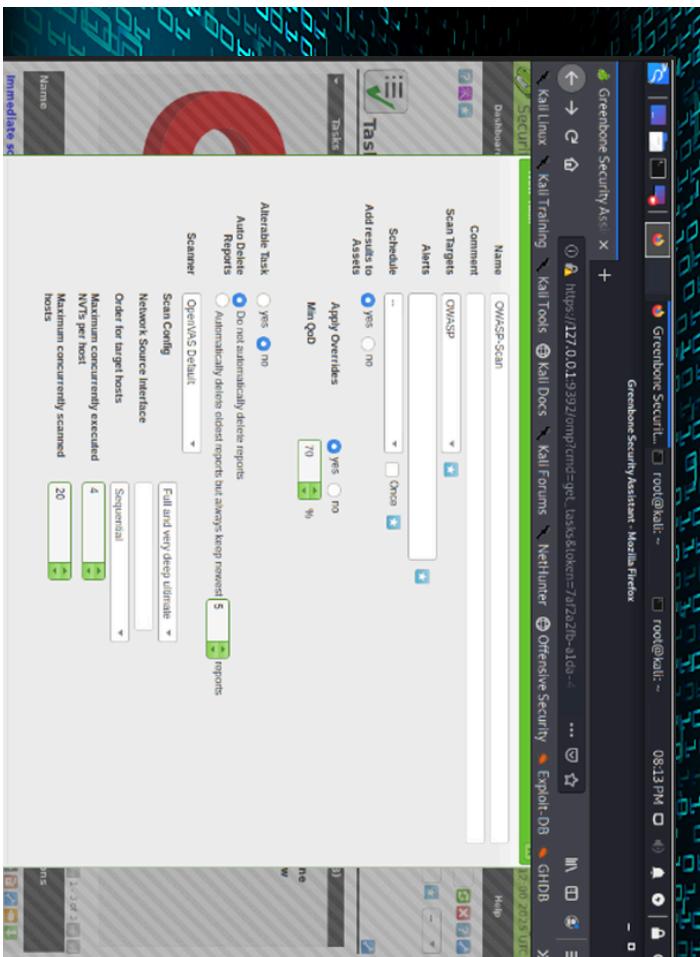


Creating the Custom Scan Task

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

The screenshot shows the Greenbone Security Assistant interface with a custom scan results page. The top navigation bar includes 'Dashboard', 'Scans', 'Assets', 'Sectigo', 'Configuration', 'Extres', and 'Administration'. The main content area displays a 'Results (231 of 728)' section with a donut chart showing the distribution of vulnerabilities by severity: High (21), Medium (74), Low (124), and Log (19). Below the chart is a 'Results by Severity Class (Total: 231)' table with columns for Severity, QID, Host, Location, and Created. A 'Results by CVSS (Total: 231)' chart shows the distribution of vulnerabilities by CVSS score. The bottom of the page includes a 'Vulnerability' section with a table and a 'CPE Inventory' section.

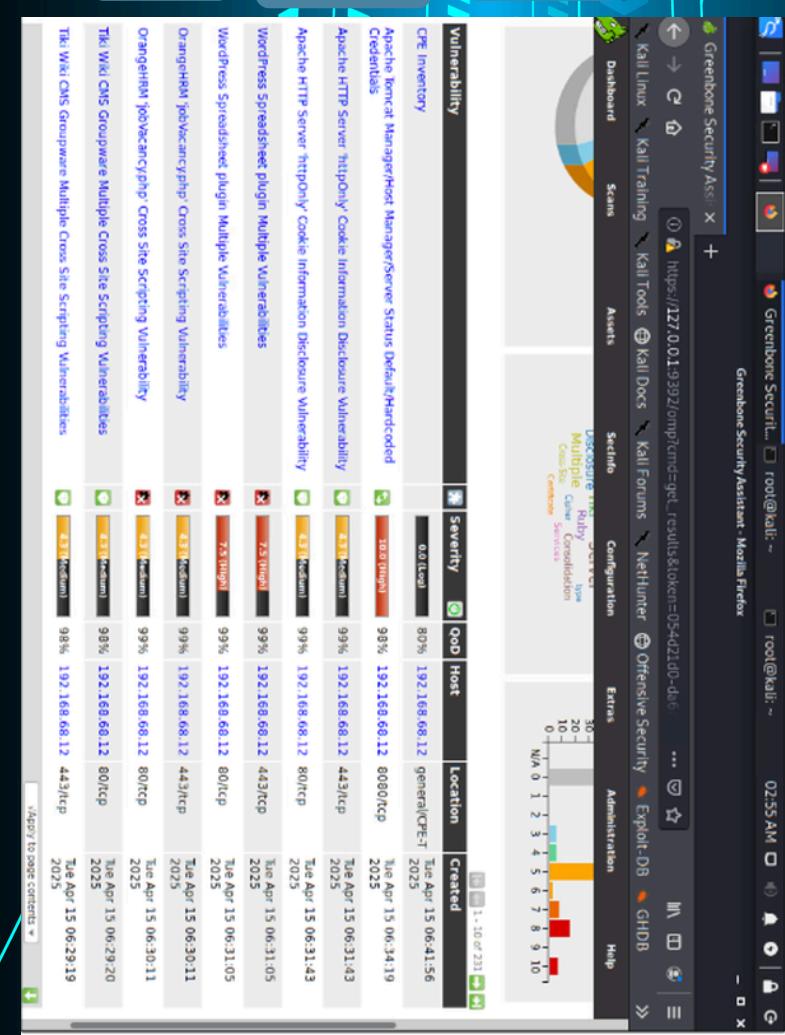
Viewing Scan Results

7

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 = Detailed 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



<http://linkedin.com/in/jacinta-izundub36a20233>

