8/7/2025

Vulnerability Scan

Using Nessus

@SRCybersecurity

Task 3: Perform a Basic Vulnerability Scan.

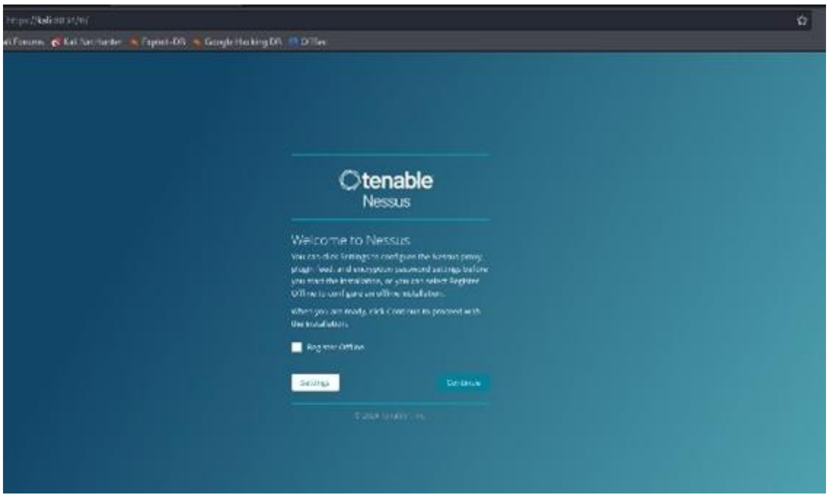
Objective: Identify common vulnerabilities on your computer**.**

Tools: OpenVAS Community Edition or Nessus, Targeted host (BeeBox).

Key Concepts: Vulnerability scanning, risk assessment, CVSS, remediation, security tools**.**

Deliverables: Vulnerability scan report with identified issues.

1.Installation and setting up of Nessus.

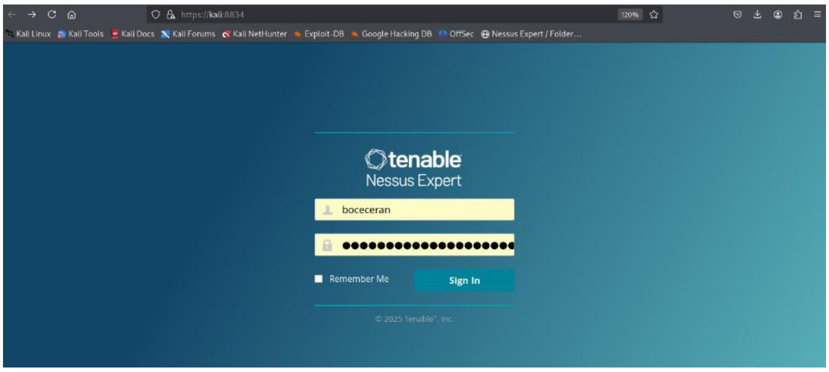


Welcome to Nessus

You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

□ Register Offline

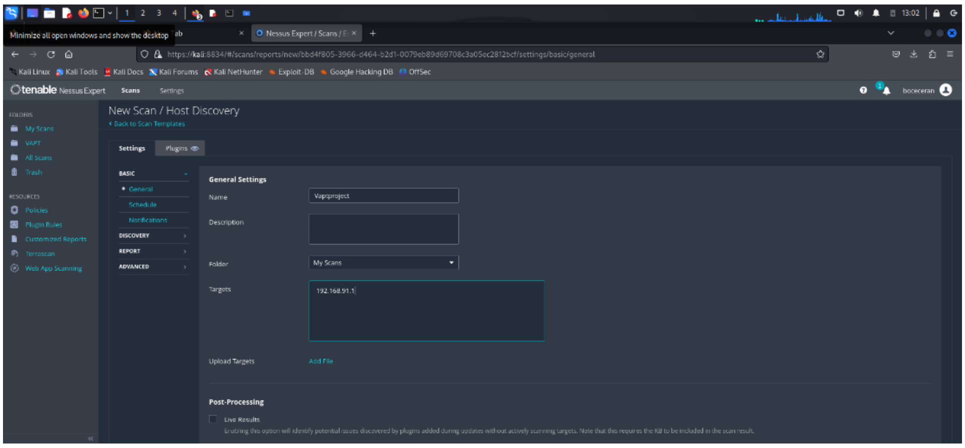


boceceran

●●●●●●●●●●●●●●●●●●●●●

□ Remember Me

2.Set up scan target as your local machine IP or localhost.



https://kali:8834/#/scans/reports/new/bbd4f805-3966-d464-b2d1-0079eb89d69708c3a05ec2812bcf/settings/basic/general

New Scan / Host Discovery

General Settings

Name: Vaptproject

Description:

Folder: My Scans

Targets: 192.168.91.1

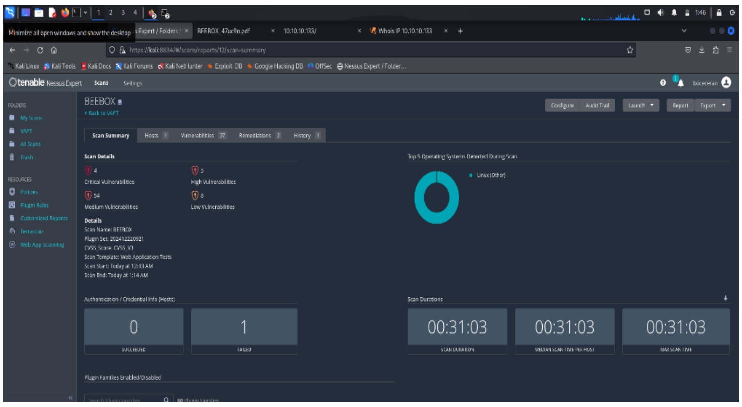
Upload Targets: Add File

Post-Processing

☐ Live Results

Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.

3.Full vulnerability scan result.



https://kali:8834/#/scans/reports/12/scan-summary

BEEBOX

Scan Details

4 Critical Vulnerabilities

5 High Vulnerabilities

54 Medium Vulnerabilities

8 Low Vulnerabilities

Details

Scan Name: BEEBOX

Plugin Set: 202412220921

CVSS_Score: CVSS_V3

Scan Template: Web Application Tests

Scan Start: Today at 12:43 AM

Scan End: Today at 1:14 AM

Authentication / Credential Info (Hosts)

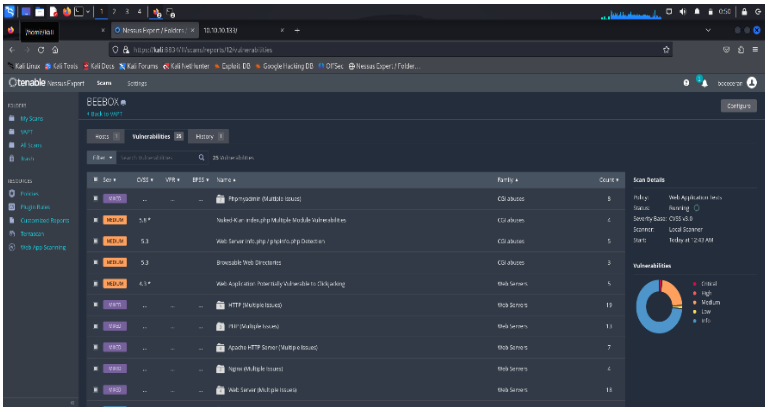
0	1
SUCCEEDED	FAILED

Scan Durations

00:31:03	00:31:03	00:31:03
SCAN DURATION	MEDIAN SCAN TIME PER HOST	MAX SCAN TIME

Top 5 Operating Systems Detected During Scan: Linux (Other)

Plugin Families Enabled/Disabled



https://kali:8834/#/scans/reports/12/vulnerabilities

BEEBOX

25 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	8
MEDIUM	5.8 *			Nuked-Klan index.php Multiple Module Vulnerabilities	CGI abuses	4
MEDIUM	5.3			Web Server info.php / phpinfo.php Detection	CGI abuses	5
MEDIUM	5.3			Browsable Web Directories	CGI abuses	3
MEDIUM	4.3 *			Web Application Potentially Vulnerable to Clickjacking	Web Servers	5
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	19
MIXED	...	...	...	PHP (Multiple Issues)	Web Servers	13
MIXED	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	7
MIXED	...	...	...	Nginx (Multiple Issues)	Web Servers	4
MIXED	...	...	...	Web Server (Multiple Issues)	Web Servers	18

Scan Details

Policy: Web Application Tests

Status: Running

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 12:43 AM

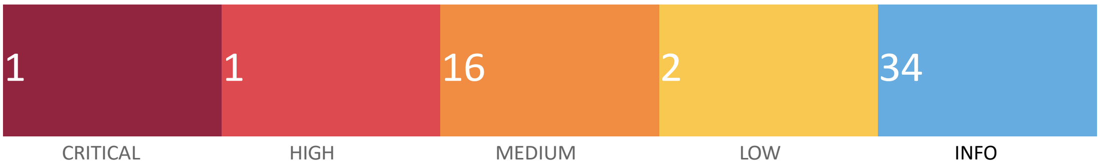
Vulnerabilities

4.Wait for scan to complete (may take 30-60 mins).

- It takes about 40-60 mins or more.

5. Vulnerabilities and severity Report.

Targeted Host BEEBOX (10.10.10.133) Scan results.



Total Vulnerabilities: 54

SEVERITY	CVSS V3.0	VPR SCO	RE EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	0.0081	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
HIGH	7.5*	7.4	0.9723	78515	Drupal Database Abstraction API SQLi
MEDIUM	5.3	1.4	0.001	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	0.0225	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.3	2.2	0.0027	134220	nginx < 1.17.7 Information Disclosure
MEDIUM	4.3*	-	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	4.3*	-	-	51972	CGI Generic XSS (Parameters Names)
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	5.1*	6.7	0.1328	24726	SQLiteManager SQLiteManager_currentTheme Cookie Travers
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	0.2301	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

LOW	N/A	- -	42057	Web Server Allows Password Auto-Completion
LOWlo	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	18638	Drupal Software Detection
INFO	N/A	-	49704	External URLs
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A		43111	HTTP Methods Allowed (per directory)

6.Simple fixes or mitigations for found vulnerabilities.

CRITICAL Severity

Summary of the Vulnerability:

- Vulnerability: SQL Injection in phpMyAdmin prior to version 4.8.6
- CVE ID: CVE-2019-12922
- Patch Info: Fixed in phpMyAdmin 4.8.6
- Public Exploits: Yes, proof-of-concept (PoC) and exploit scripts are publicly available.

- Mitigation Steps

Upgrade phpMyAdmin

This is the most direct and strongly recommended fix.

- Current Version: Prior to 4.8.6
- Secure Version: 4.8.6 or later

HIGH Severity

Drupal Database Abstraction API SQLi

Risk: SQL injection through unsafe queries.
CVE: CVE-2014-3704
Affected: Drupal 7.x before 7.32

Mitigation:

- Update Drupal immediately to latest 7.x or 9.x/10.x if still on 7.

MEDIUM Severity

2. Apache ETag Header Information Disclosure

Risk: ETag reveals inode info, which may assist in host fingerprinting.

Mitigation (Apache):

In httpd.conf or .htaccess:

LOW severity

HTTP TRACE / TRACK Methods Allowed

Risk: Cross-site tracing (XST) vulnerability.

Mitigation:

Disable TRACE method (Apache):

TraceEnable Off

THANK YOU

END