

Deploy a Vulnerability Management Solution to Organization Infrastructure

Demo organization: testphp.vulnweb.com

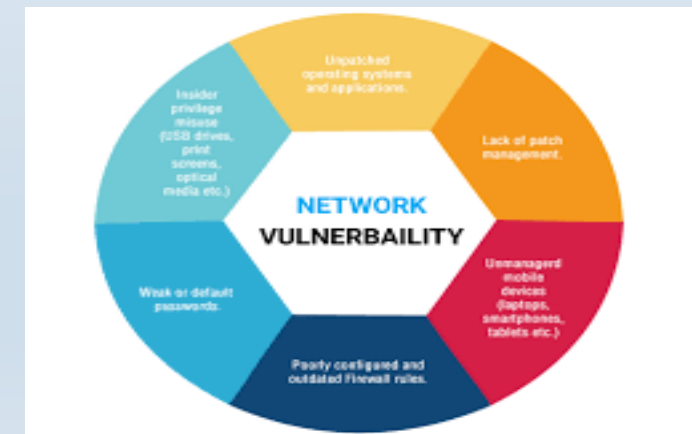
Vulnerability Management | Institute Of Emerging Carrers (IEC)| M. Ansar Raza

Project Outline

- Introduction of Vulnerability Management
- Importance of Vulnerability Management/Assessment
- What is meant by CVE
- Details of Project-Vulnerability Management Solution (Nessus)
- Conclusion
- Q&A

What is Vulnerability & Vulnerability Management

- A vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system.
- Vulnerability management is a continuous, proactive process that keeps your computer systems, networks and enterprise applications safe from cyber attacks and data breaches.



Importance of Vulnerability Management

- Vulnerability management programs give companies a framework for managing risks, detecting vulnerabilities across the entire environment.
- Vulnerability management enhances the overall security posture of your organization by recognizing key assets and where to prioritize efforts in order to reduce risk.



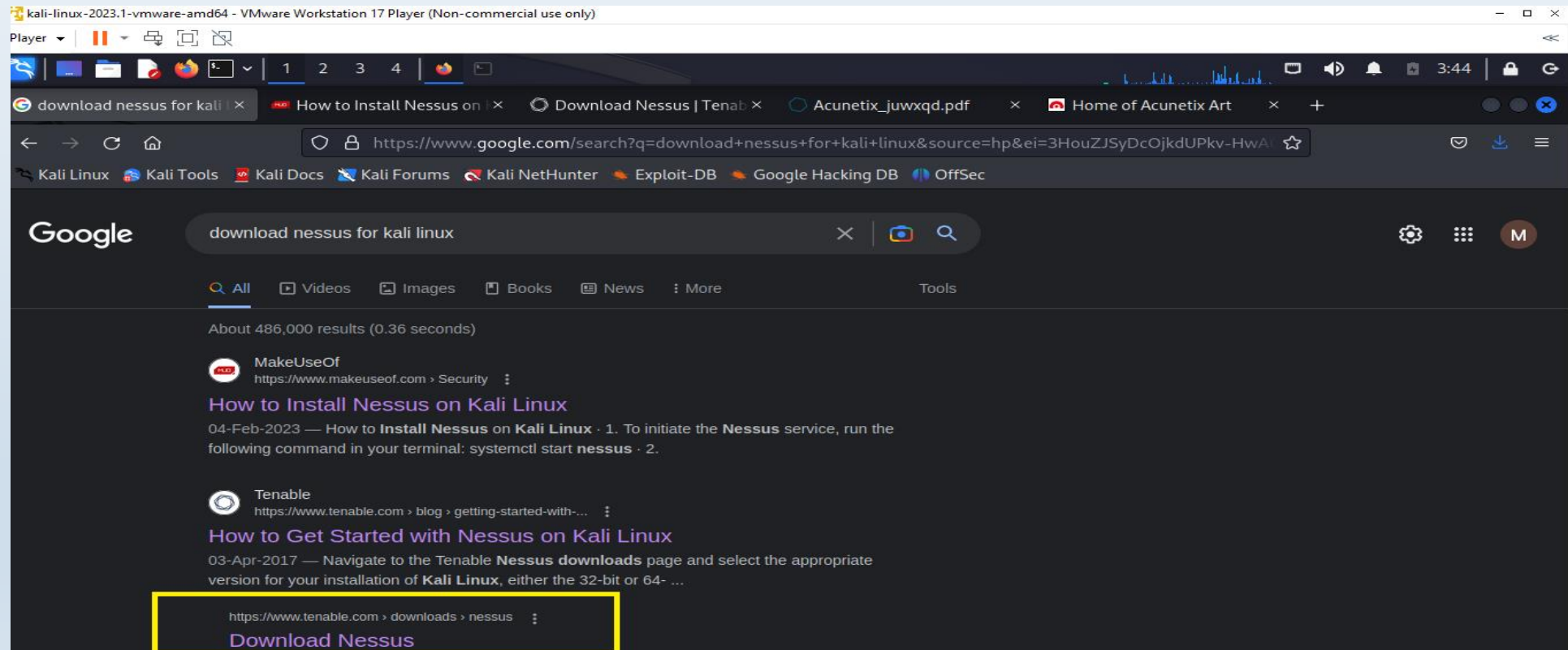
What is meant by CVE?

- CVE Common Vulnerabilities and Exposures is a list of publicly disclosed computer security flaws.

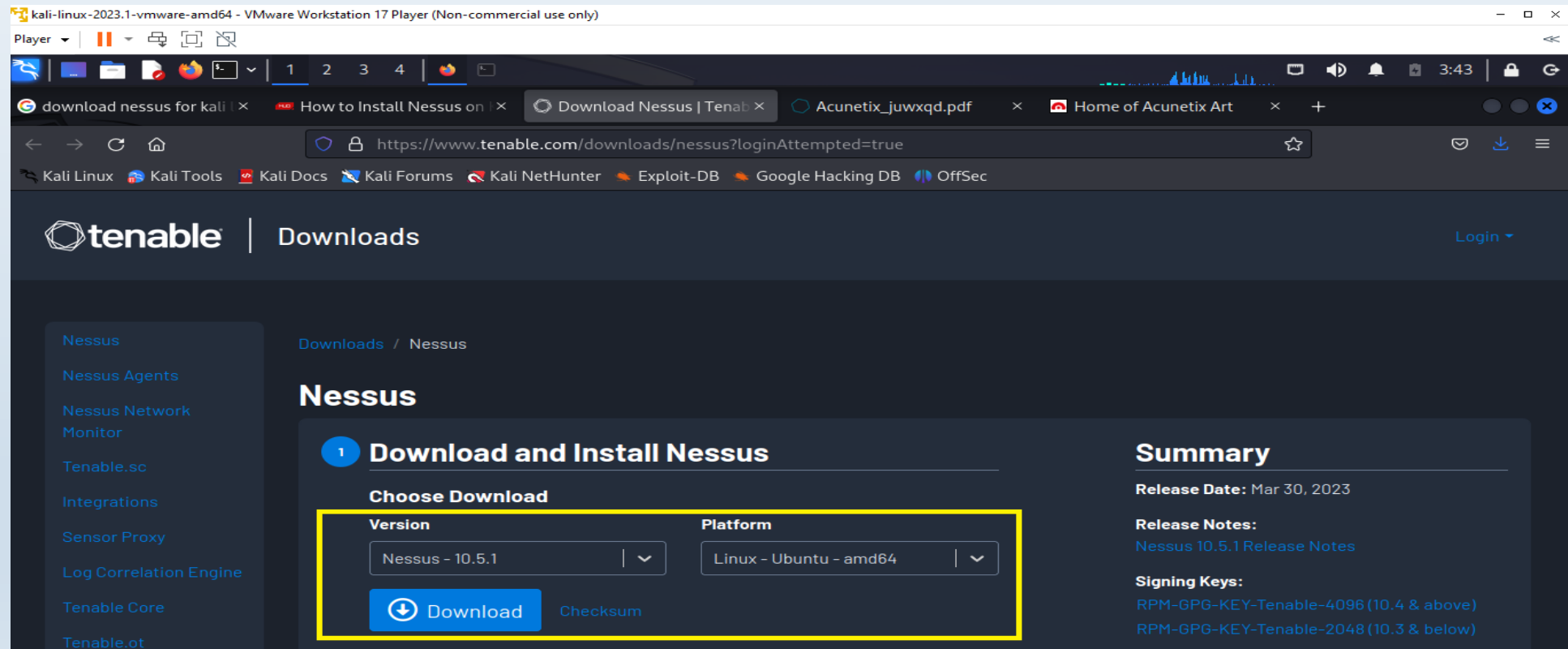


Project Description: Deploy a vulnerability management solution (Nessus) to identify all the vulnerabilities of Organization: testphp.vulnweb.com & develop a report?

- Google (Nessus Download for Kali Linux)

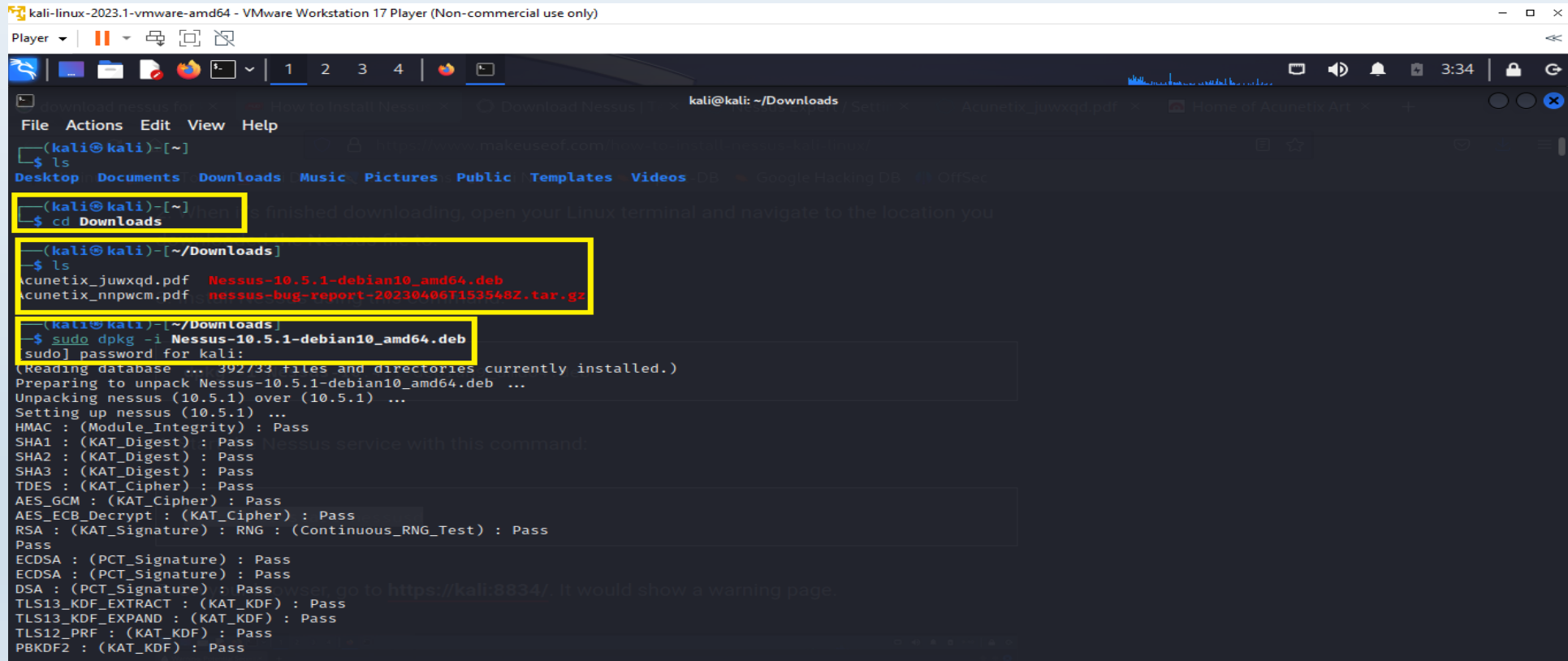


- Nessus 10.5.1 for Linux-Ubuntu-amd64



Installation of Nessus 10.5.1

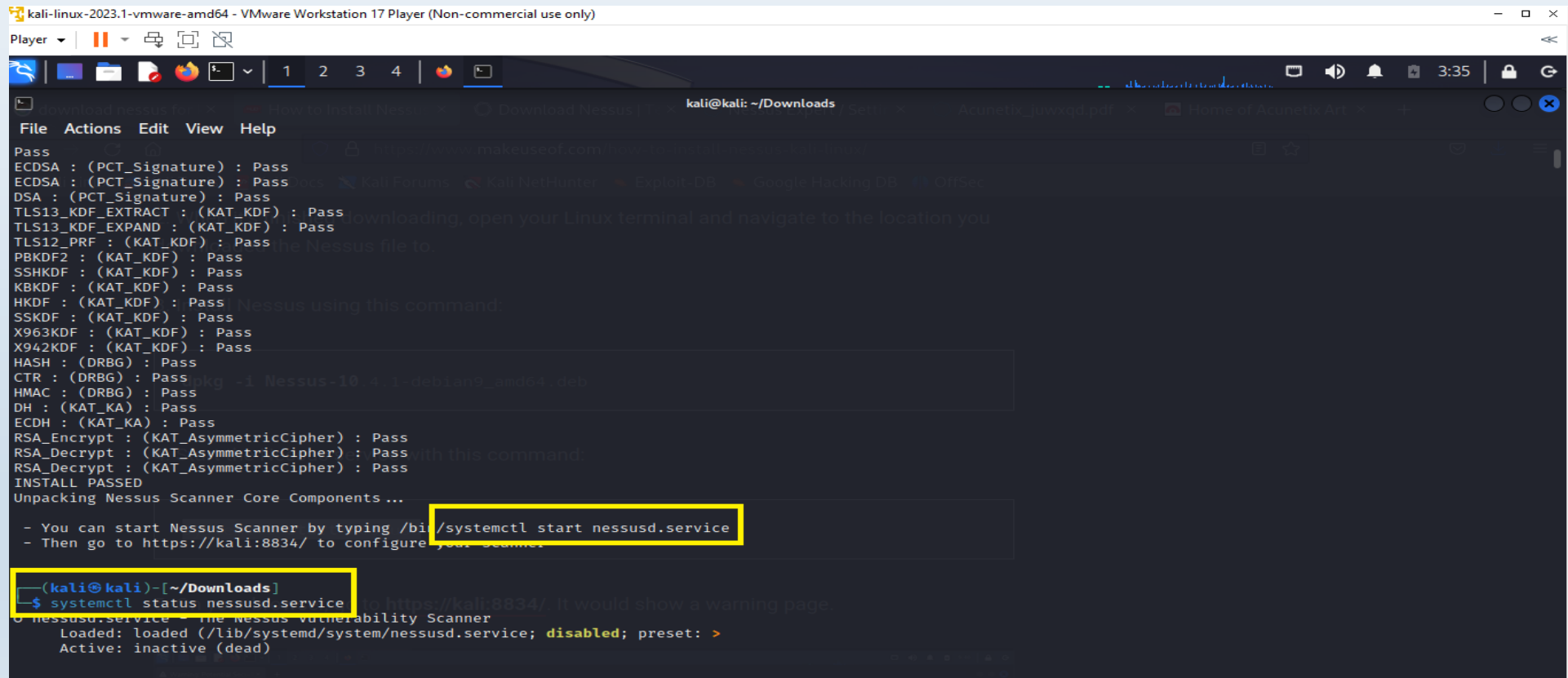
- Open terminal of kali Linux



```
kali-linux-2023.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
(kali@kali)-[~]
$ ls
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
acunetix_juwxqd.pdf  Nessus-10.5.1-debian10_amd64.deb
acunetix_nnpwcm.pdf  nessus-bug-report-20230406f153548Z.tar.gz
(kali@kali)-[~/Downloads]
$ sudo dpkg -i Nessus-10.5.1-debian10_amd64.deb
[sudo] password for kali:
(Reading database ... 392733 files and directories currently installed.)
Preparing to unpack Nessus-10.5.1-debian10_amd64.deb ...
Unpacking nessus (10.5.1) over (10.5.1) ...
Setting up nessus (10.5.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
```


Installation of Nessus 10.5.1

- Run command *systemctl start nessusd.service*



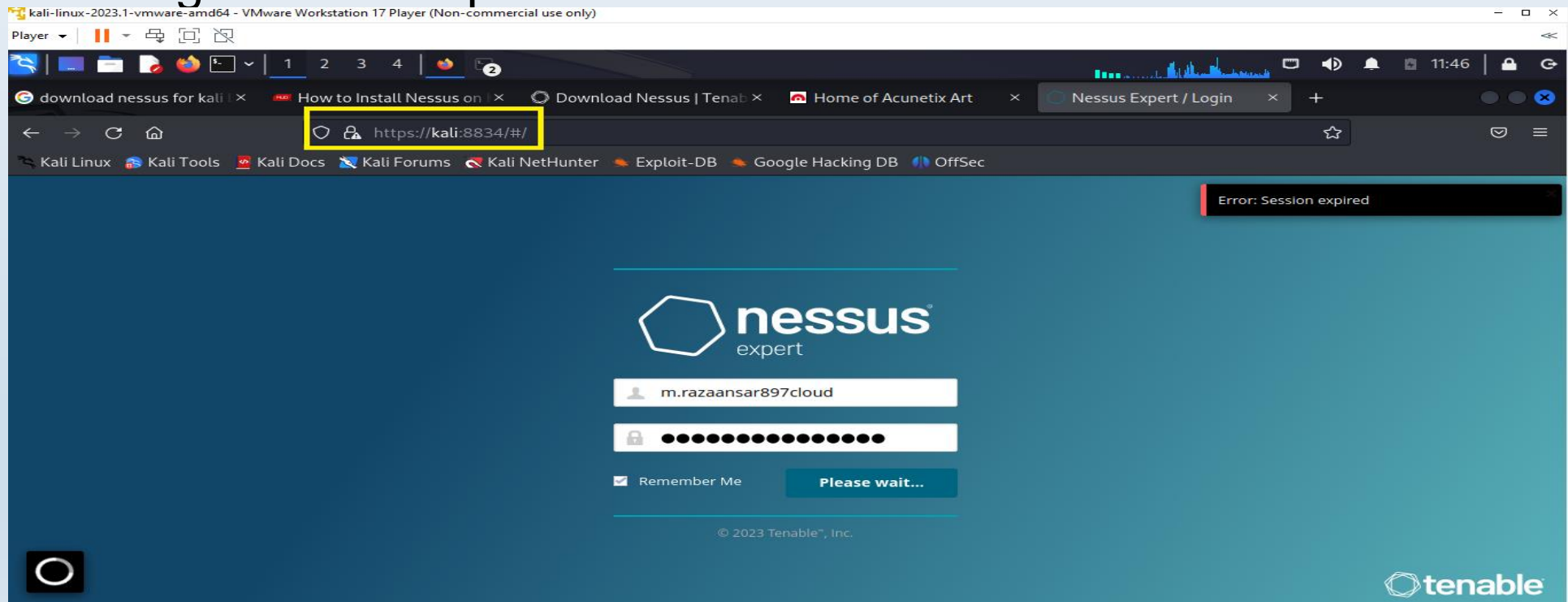
```
kali@kali: ~/Downloads
File Actions Edit View Help
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner.

(kali@kali)-[~/Downloads]
$ systemctl status nessusd.service
● nessusd.service - The Nessus vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: >
   Active: inactive (dead)
```

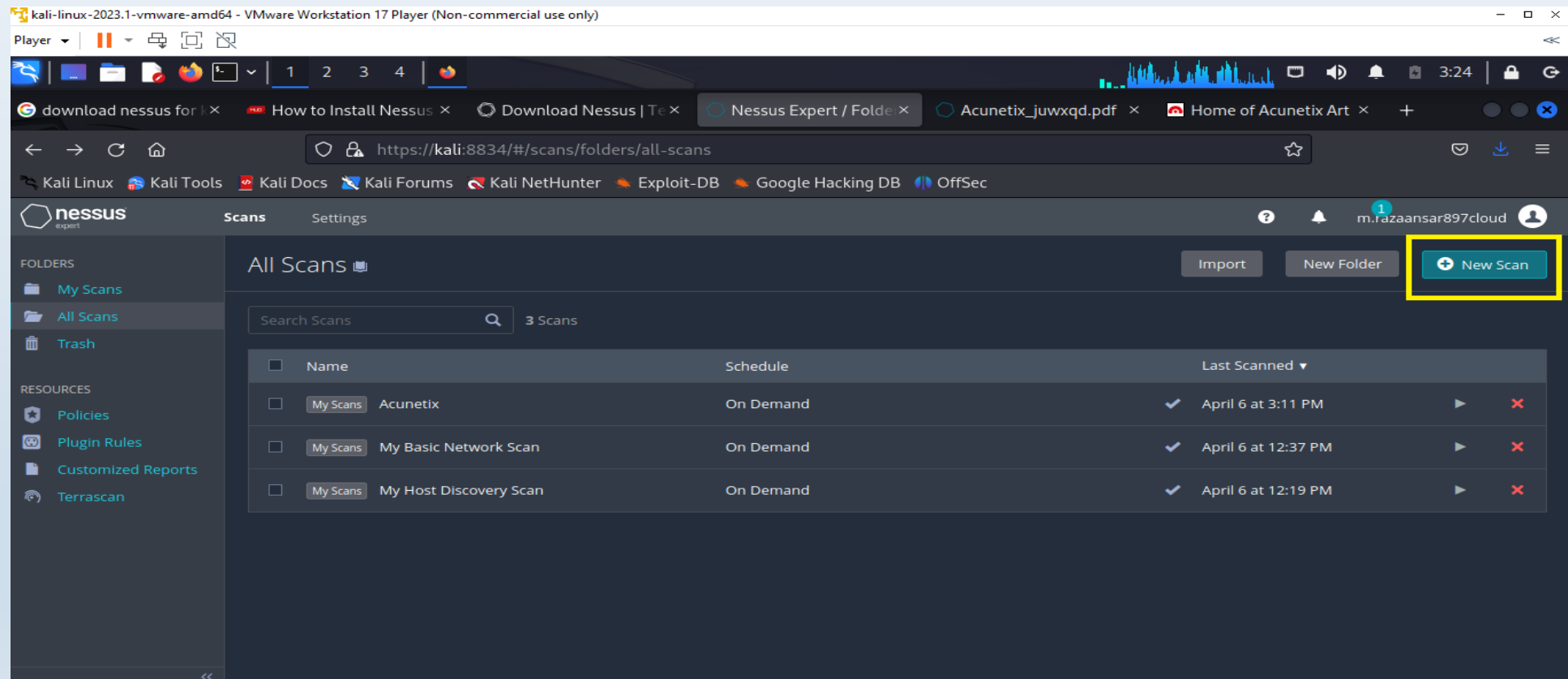
Open Nessus Browser

- `https://localhost:8834/#/`
- Using Nessus Expert activate the account



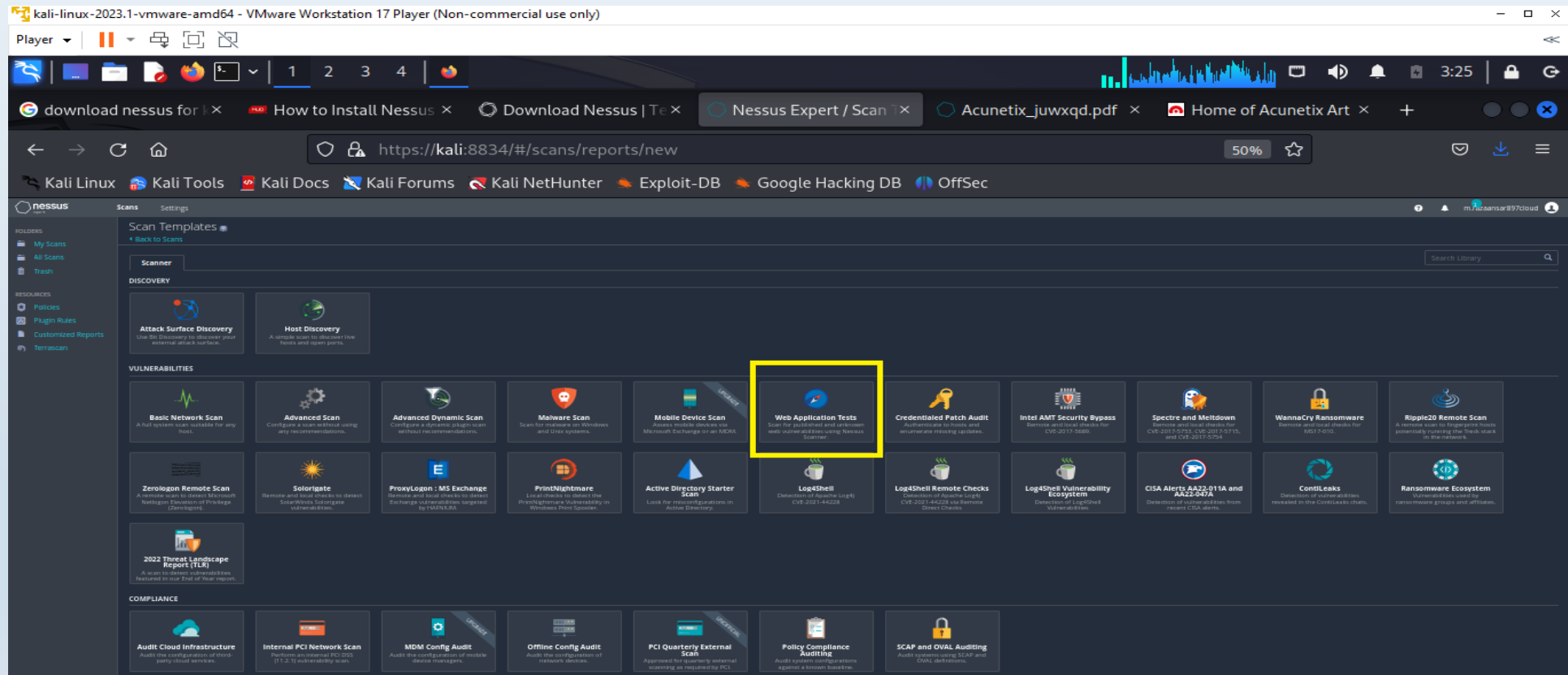
Using Nessus Tool

- Click on New Scan



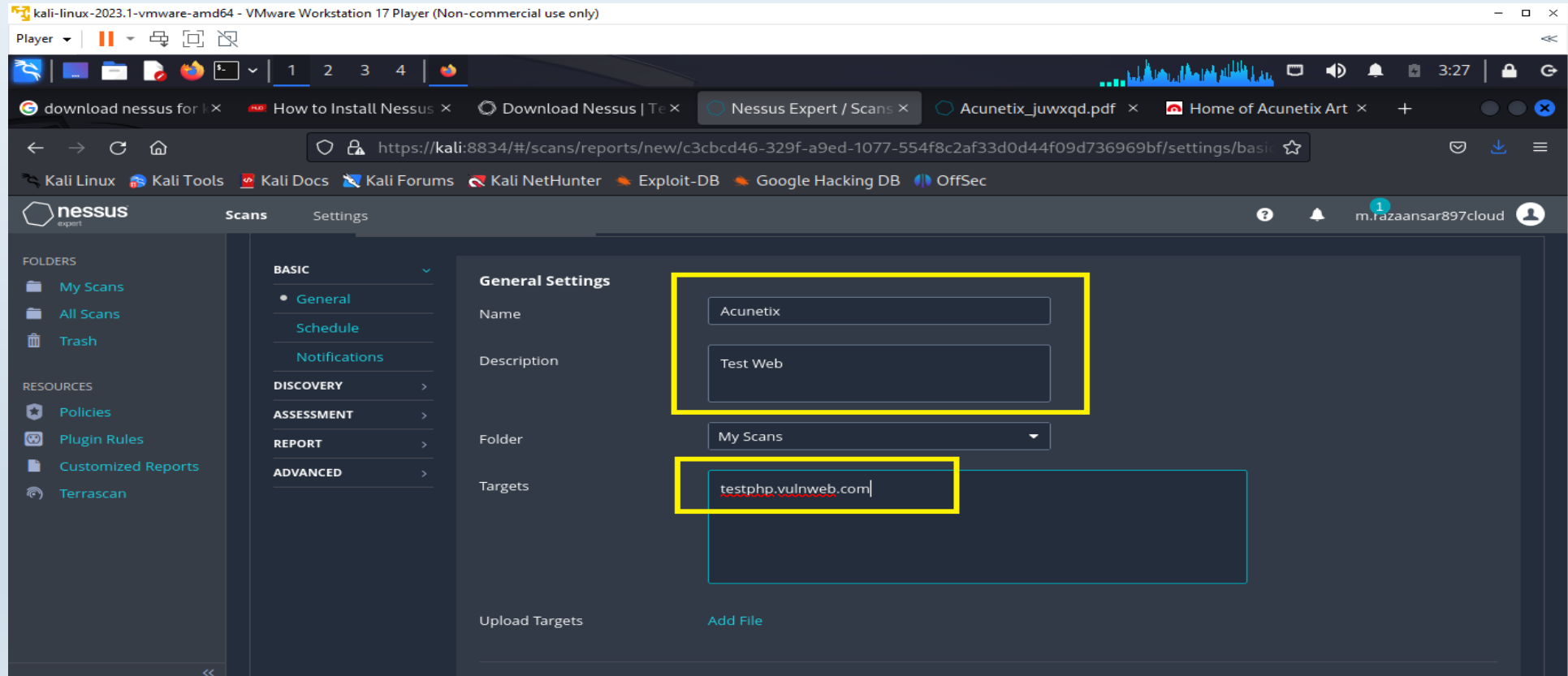
Using Nessus Tool

- Click on Web Application Test



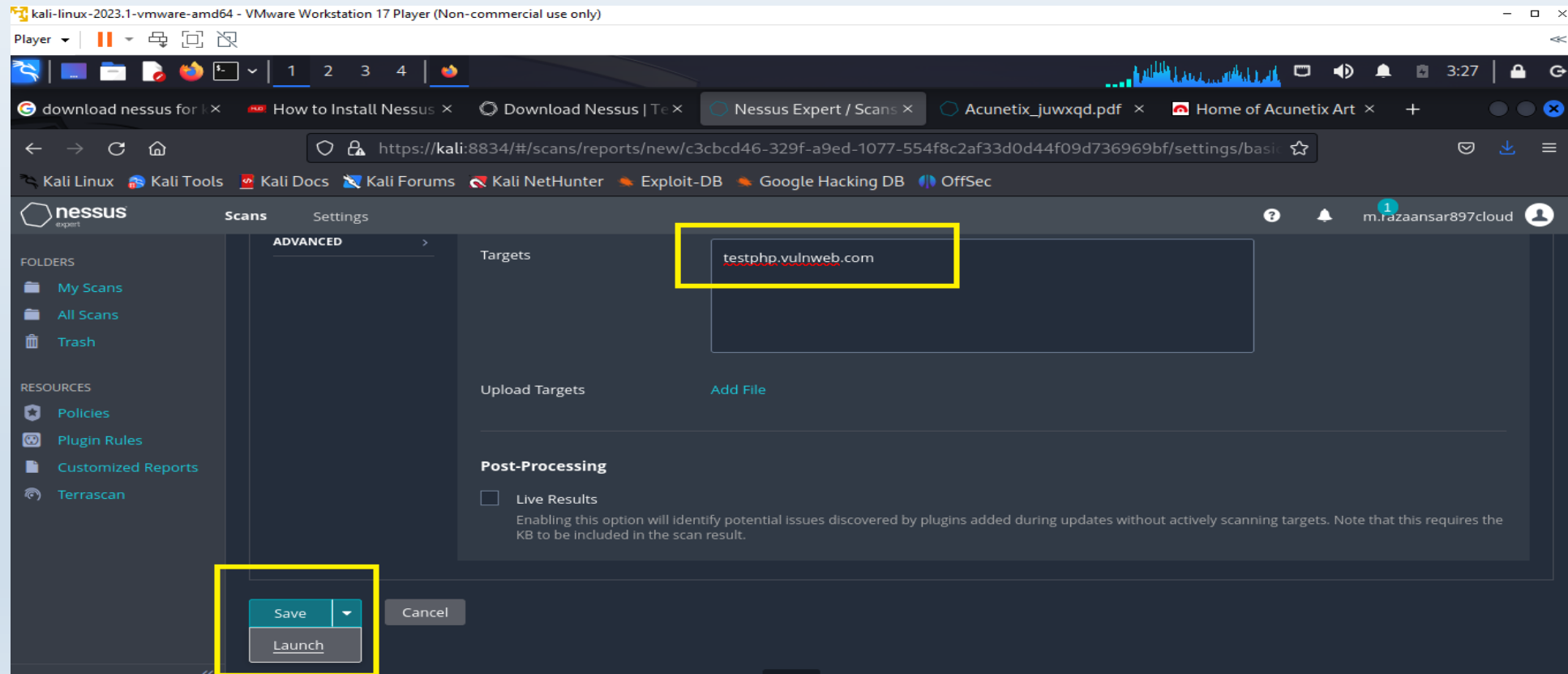
Using Nessus Tool

- Enter Parameter testphp.vulnweb.com



Using Nessus Tool

- Scan launch



Nessus Scanning Results

- Scan Summary

The screenshot displays the Nessus Expert web interface within a VMware Workstation 17 Player. The browser window shows the URL `https://kali:8834/#/scans/reports/23/scan-summary`. The interface is divided into a sidebar and a main content area. The sidebar contains sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area features the 'Acunetix' logo and a 'Scan Summary' tab. Below the tab, a 'Scan Details' section provides a breakdown of vulnerabilities: 2 Critical, 13 High, 16 Medium, and 2 Low. A 'Details' section below that lists scan metadata: Scan Name (Acunetix), Plugin Set (202304052204), CVSS Score (CVSS_V3), Scan Template (Web Application Tests), Scan Start (April 6 at 1:16 PM), and Scan End (April 6 at 3:11 PM). The interface also includes navigation buttons like 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'.

Scan Summary

Hosts 1 Vulnerabilities 26 Remediations 1 History 1

Scan Details

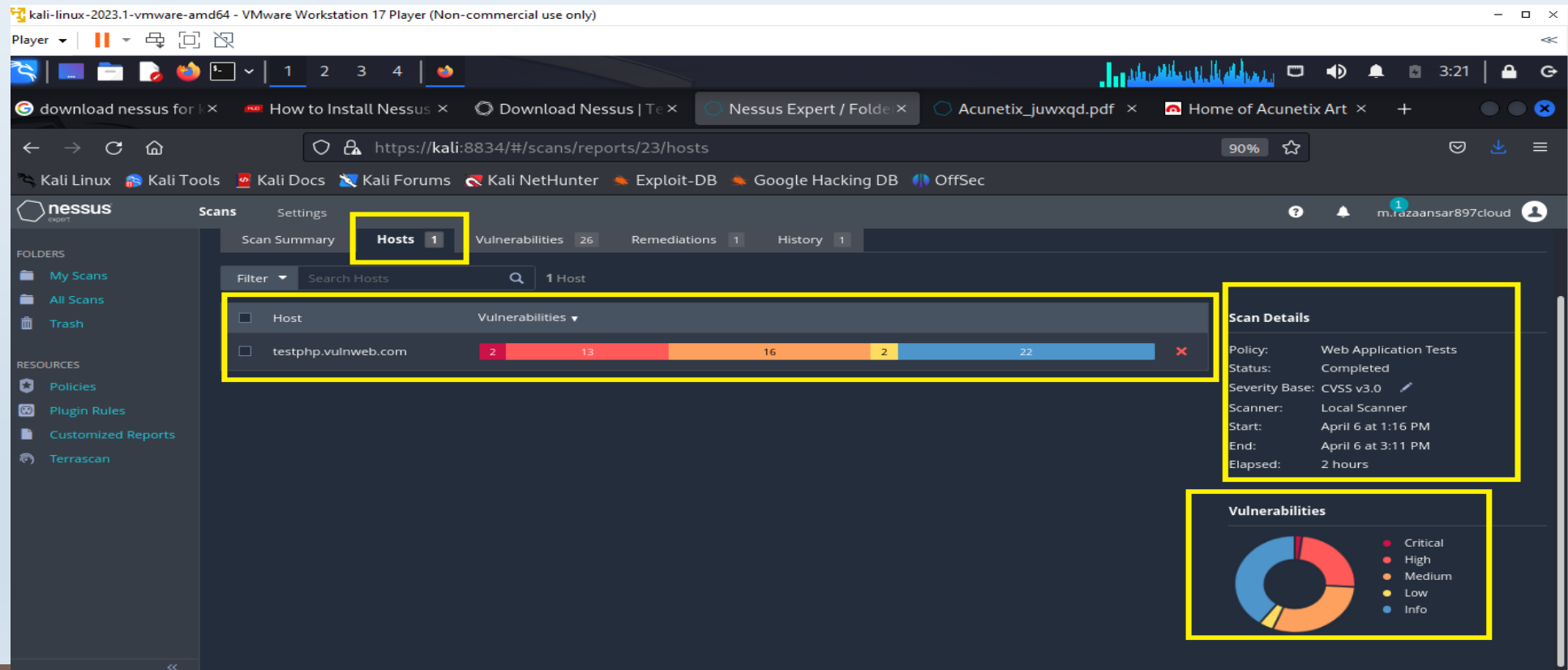
2 Critical Vulnerabilities	13 High Vulnerabilities
16 Medium Vulnerabilities	2 Low Vulnerabilities

Details

Scan Name: Acunetix
Plugin Set: 202304052204
CVSS Score: CVSS_V3
Scan Template: Web Application Tests
Scan Start: April 6 at 1:16 PM
Scan End: April 6 at 3:11 PM

Nessus Scanning Results

- Host vulnerabilities



Nessus Scanning Results

- Detail of vulnerabilities

kali-linux-2023.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | [Icons] | 1 2 3 4 | [Icons]

download nessus for | x How to Install Nessus x Download Nessus | Te x Nessus Expert / Folde x Acunetix_juwxqd.pdf x Home of Acunetix Art x +

https://kali:8834/#/scans/reports/23/vulnerabilities 90% ☆ [Icons]

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

nessus expert Scans Settings [Icons] m.tazaansar897cloud [Avatar]

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Terrascan

Scan Summary Hosts 1 **Vulnerabilities 26** Remediations 1 History 1

Filter Search Vulnerabilities 26 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	[Icons]
MIXED	PHP (Multiple Issues)	CGI abuses	23	[Icons]
HIGH	7.5 *		CGI Generic SQL Injection (2nd pass)	CGI abuses	1	[Icons]
HIGH	7.5 *		CGI Generic SQL Injection (blind, time bas...	CGI abuses	1	[Icons]
MEDIUM	5.3		Browsable Web Directories	CGI abuses	1	[Icons]
MEDIUM	5.0 *		Web Application SQL Backend Identification	CGI abuses	1	[Icons]
MEDIUM	4.3 *		CGI Generic Cookie Injection Scripting	CGI abuses	1	[Icons]
MEDIUM	4.3 *		CGI Generic HTML Injections (quick test)	CGI abuses : XSS	1	[Icons]
MEDIUM	4.3 *		CGI Generic XSS (quick test)	CGI abuses : XSS	1	[Icons]

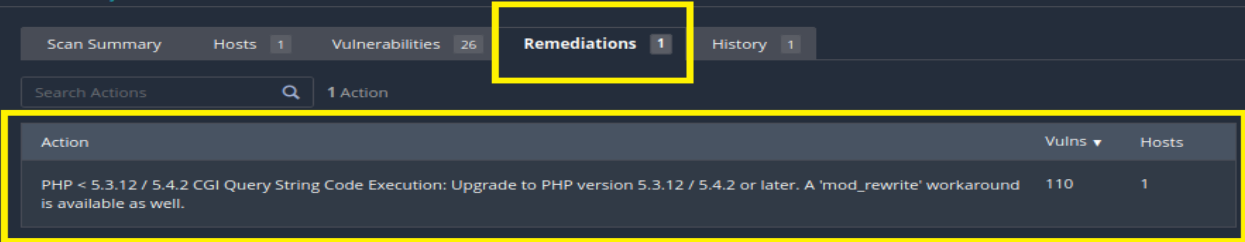
Scan Details

Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: April 6 at 1:16 PM
End: April 6 at 3:11 PM
Elapsed: 2 hours

Vulnerabilities

Legend: Critical, High, Medium, Low, Info

- Remediations



Nessus Report

- Nessus generate report in PDF format

The screenshot displays the Nessus web interface within a Kali Linux virtual machine. The 'Generate Report' dialog box is open, showing the 'Report Format' set to PDF and the 'Detailed Vulnerabilities By Host' template selected. The background interface shows a list of vulnerabilities and scan details.

Generate Report Dialog:

- Report Format:** ☐ HTML ☒ PDF ☐ CSV
- Select a Report Template:**
 - ☐ Hide system templates
 - SYSTEM**
 - Complete List of Vulnerabilities by Host
 - Compliance
 - Detailed Vulnerabilities By Host**
 - Detailed Vulnerabilities by Host with Compliance/Remediations
 - Detailed Vulnerabilities By Plugin
 - Detailed Vulnerabilities By Plugin with Compliance/Remediations
 - Remediations
 - Summary of Exploitable Vulnerabilities
 - Summary of Hosts with Vulnerabilities
 - Summary of Known/Default Accounts
 - Summary of Operating Systems
 - Summary of Unsupported Software
 - Summary of Vulnerabilities Older Than One Year
 - Top 10 Vulnerabilities
 - Vulnerability Operations
- Template Description:** This report provides a summary list of vulnerabilities for each host detected in the scan.
- Filters Applied:** None
- Formatting Options:** ☒ Include page breaks between vulnerability results
- Buttons:** Generate Report, Cancel, Save as default

Background Interface:

- Scans:** Acunetix
- Vulnerabilities Table:**

Sev	CVSS	VPR	Name
Mixed	PHP
HIGH	7.5 *	...	CGI Gene
HIGH	7.5 *	...	CGI Gene
MEDIUM	5.3	...	Browsabl
MEDIUM	5.0 *	...	Web App
MEDIUM	4.3 *	...	CGI Gene
MEDIUM	4.3 *	...	CGI Gene
MEDIUM	4.3 *	...	CGI Gene
MEDIUM	4.3 *	...	Web App
Mixed	Web
INFO	HTTP (Multiple Issues)
- Scan Details:**
 - Policy: Web Application Tests
 - Status: Completed
 - Severity Base: CVSS v3.0
 - Scanner: Local Scanner
 - Start: April 6 at 1:16 PM
 - End: April 6 at 3:11 PM
 - Elapsed: 2 hours
- Vulnerabilities:** A donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Nessus Report

- Nessus PDF Report

Acunetix_b9m2h5.pdf - Adobe Reader

File Edit View Window Help

Open [Icons] 4 (4 of 101) 114% [Icons]

Tools Fill & Sign Comment

testphp.vulnweb.com

2	13	16	2	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Apr 6 13:16:56 2023
End time: Thu Apr 6 15:11:27 2023

Host Information

DNS Name: testphp.vulnweb.com
IP: 44.228.249.3

Vulnerabilities

58987 - PHP Unsupported Version Detection

Synopsis

Sign In

Export PDF

Adobe ExportPDF
Convert PDF files to Word or Excel online.

Select PDF File:
Acunetix_b9m2h5.pdf
1 file / 411 KB

Convert To:
Microsoft Word (*.docx)

Recognize Text in English(U.S.)
[Change](#)

Convert

Create PDF
Edit PDF
Send Files
Store Files

Conclusion

- Nessus is a vulnerability scanning tool
- Vulnerability scanning tool is inspected the potential points of exploit on a computer or network to identify security holes.
- A vulnerability scanner detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Your Questions Answered

