Task-3: Perform a Basic Vulnerability Scan on Your PC

NESSUS VULNERABILITY SCANNING TOOL:

- Nessus is an open source Vulnerability Scanning Tool that helps pen testers to identify the Vulnerabilities and security risks in a system.
- Nessus is available in both a free open-source version and a commercial version with additional features.
- To use Nessus, first install Nessus Essentials (free version) in Kali Linux or in any operating system.

INSTALLATION IN KALI LINUX:

Step 1: Download Nessus Essentials (.deb) file from website.

Step 2: Navigate to Downloads folder from PWD using CD command.

Step 3: Select the downloaded file to install it by using following command:

```
sudo dpkg –i Nessus-10.4.1-ubuntu1404_amd64.deb
```

Step 4: Configure Nessus by activation code and register as an user with credentials.

STARTING NESSUS:

- Start Nessus Service by using following command:

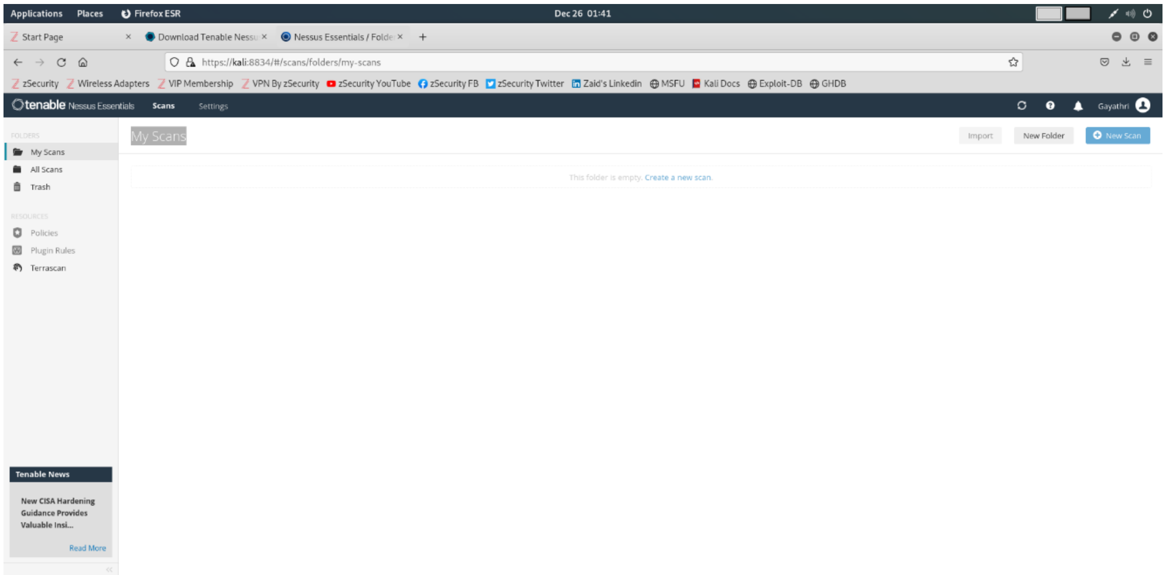
```
/bin/systemctl start nessusd.service
```

Then use the following link to open Nessus: **https://kali:8834/**

SCANNING A TARGET

Step 1: Start & open Nessus by using above command & link.

Step 2: If you are using Nessus for the first time, study about the various components in the Nessus window.



a) **Scan**: Used to scan the target for Vulnerabilities.

b) Policies: We can create our own policy by using new policy tab or we can use the default policies. It determines the type of scan, which plug-ins to use what type of scan should be excluded etc.

c) Plug-ins: Plug-ins defines the type of Vulnerabilities it shall look for. These Plug-ins are coded in "Nessus attack scripting language".

Step 3: Scan a target by clicking on "create a new scan" and select any scan type from the available profiles. Alternatively, we can create our own policies for scanning and these policies will be saved in user defined tab.

Step 4: After entering the target details and address into the scan profile, we can save the profile for future scans or begin the scan by clicking the "Launch" button.

Step 5: After the scan is completed, it will provide detailed information about the vulnerabilities and risks presented in the target.

Step 6: Analyze the results and export the report in HTML, CSV, PDF, or .nessus format.

EXAMPLE:

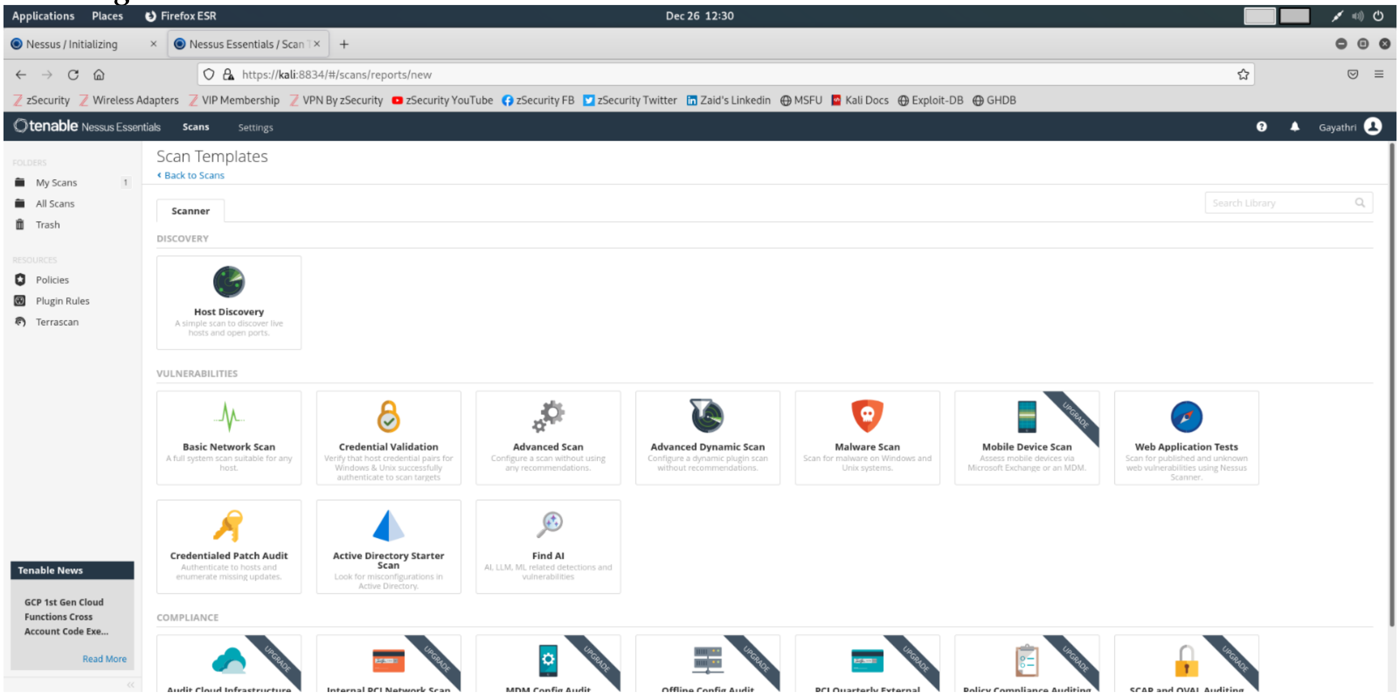
- In this example my target is a Metasploitable machine.

  Target has an IP is **“192.168.226.129”**

- So, we will scan this Metasploitable machine to identify the Vulnerabilities by using Nessus.

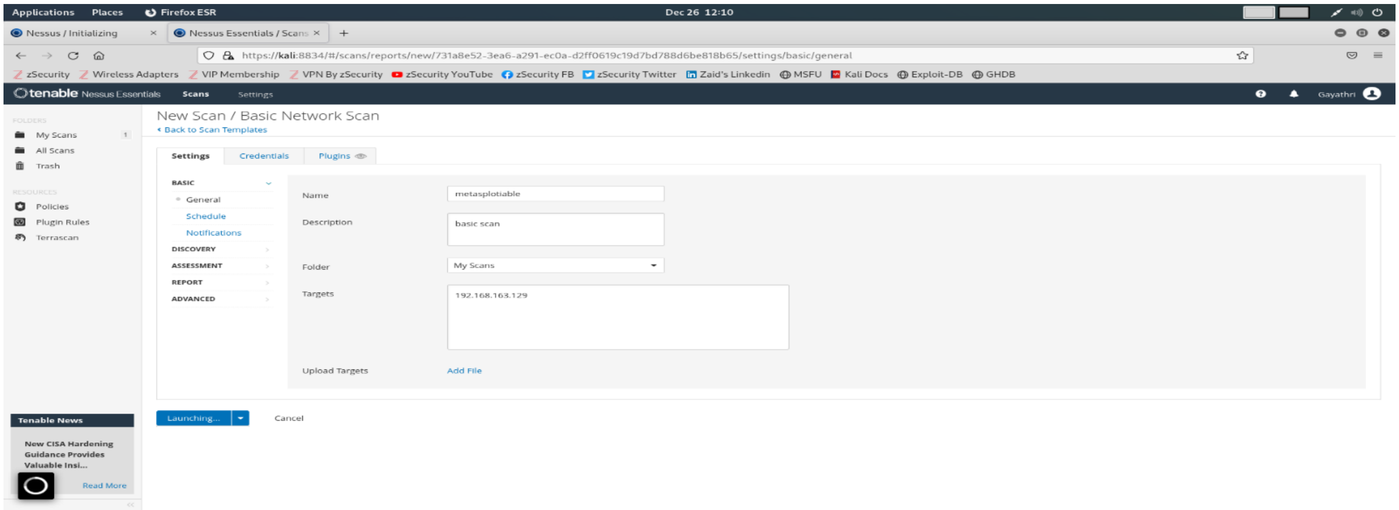
- After completion of scan it will provide the risks and vulnerabilities presented in the Metasploitable machine.

- ***Selecting the Basic Scan in Nessus***


Applications
Places
Firefox ESR
Dec 26 12:30
Nessus / Initializing
Nessus Essentials / Scan
https://kali:8834/#/scans/reports/new
zSecurity
Wireless Adapters
VIP Membership
VPN By zSecurity
zSecurity YouTube
zSecurity FB
zSecurity Twitter
Zaid's Linkedin
MSFU
Kali Docs
Exploit-DB
GHDB
tenable Nessus Essentials
Scans
Settings
Gayathri
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
GCP 1st Gen Cloud Functions Cross Account Code Exe...
Read More
Scan Templates
‹ Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Find AI
AI, LLM, ML related detections and vulnerabilities
COMPLIANCE
Audit Cloud Infrastructure
Internal PCI Network Scan
MDM Config Audit
Offline Config Audit
PCI Quarterly External
Policy Compliance Auditing
SCAP and OVAL Auditing
UPGRADE

-

- ***Launching the Scan after giving target details***



Name: metasplotiable

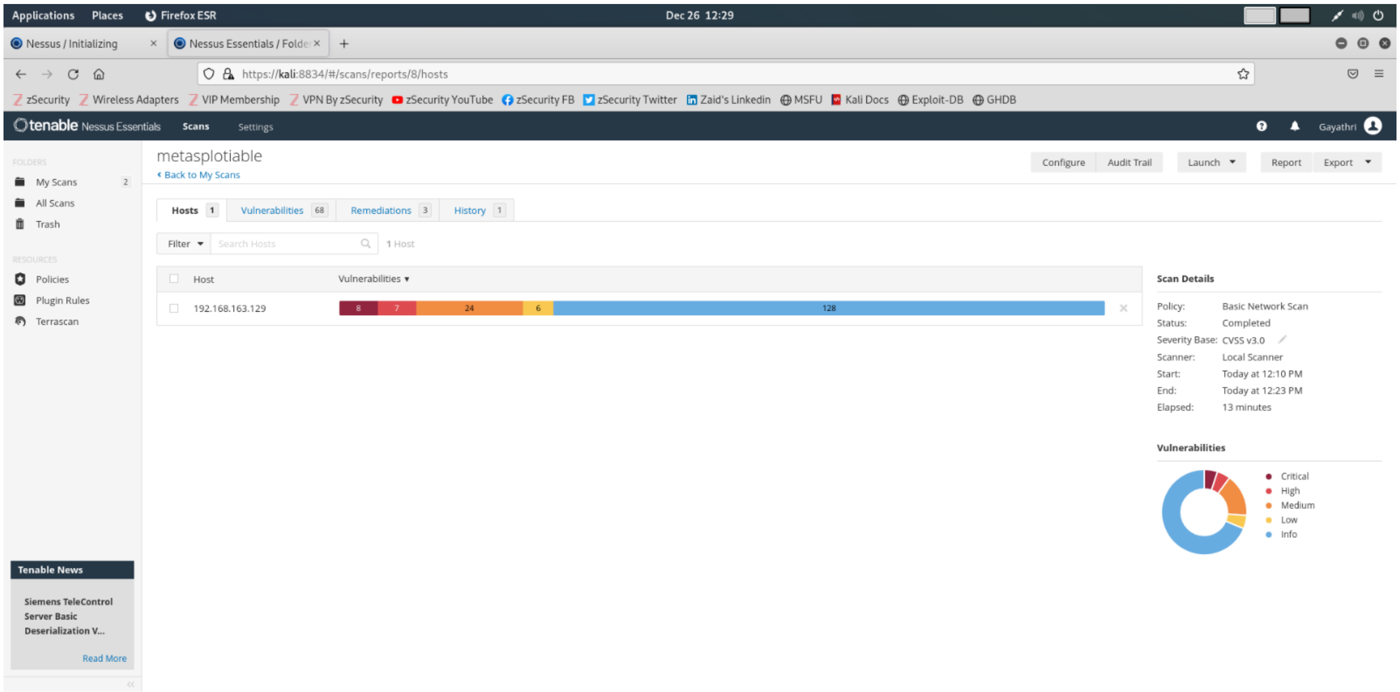
Description: basic scan

Folder: My Scans

Targets: 192.168.163.129

Upload Targets: Add File

- *Analyzing the Result*



metasplotiable

‹ Back to My Scans

Hosts 1 | Vulnerabilities 68 | Remediations 3 | History 1

Filter ▾ | Search Hosts | 1 Host

Host	Vulnerabilities ▾
192.168.163.129	8 7 24 6 128

Scan Details

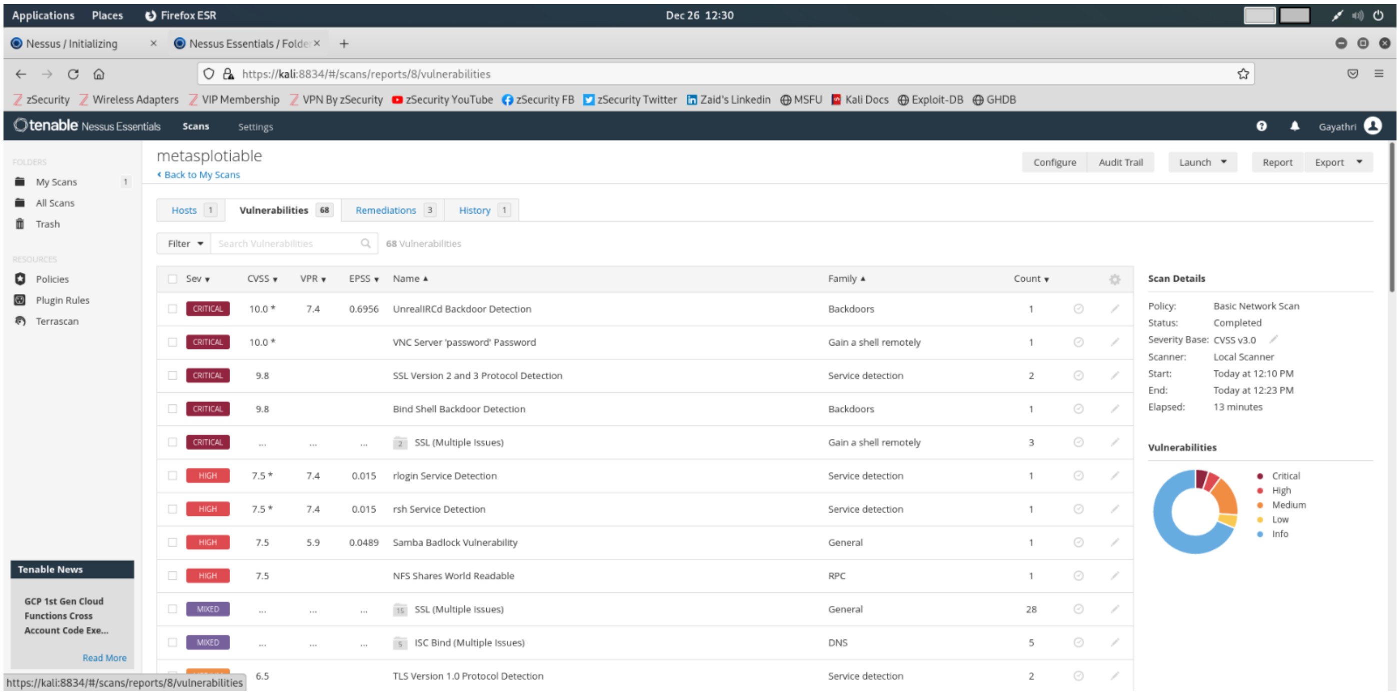
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:10 PM
End: Today at 12:23 PM
Elapsed: 13 minutes

Vulnerabilities

-

CONCLUSION:

So, Nessus is an excellent vulnerability assessment tool that includes a variety of scans and user-defined policies. So, by exploiting the discovered vulnerabilities, we can progress to the next stage of exploitation.



metasplotiable

‹ Back to My Scans

Hosts 1 | Vulnerabilities 68 | Remediations 3 | History 1

Filter ▾ | Search Vulnerabilities | 68 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
CRITICAL	10.0 *	7.4	0.6956	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	7.4	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5 *	7.4	0.015	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.0489	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	15 SSL (Multiple Issues)	General	28
MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5
	6.5			TLS Version 1.0 Protocol Detection	Service detection	2

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:10 PM
End: Today at 12:23 PM
Elapsed: 13 minutes

Vulnerabilities