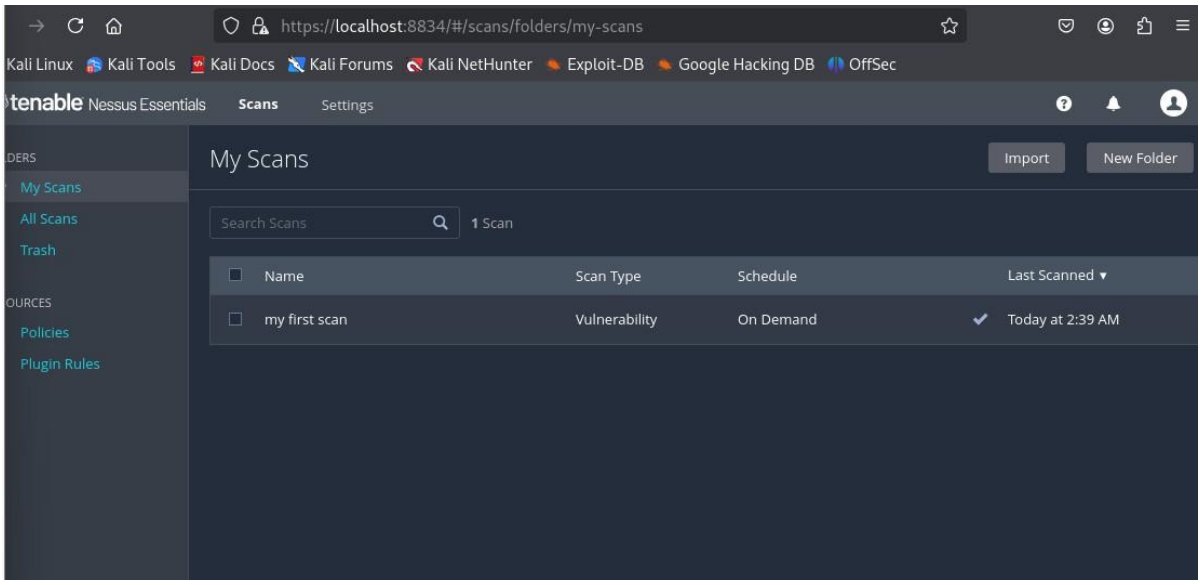
Task 3 – Vulnerability Scan Report (Nessus on Metasploit)

1. Objective

To perform a vulnerability scan on a deliberately vulnerable system (Metasploit 2) using Nessus Essentials and analyze the identified security risks.



2. Target Information

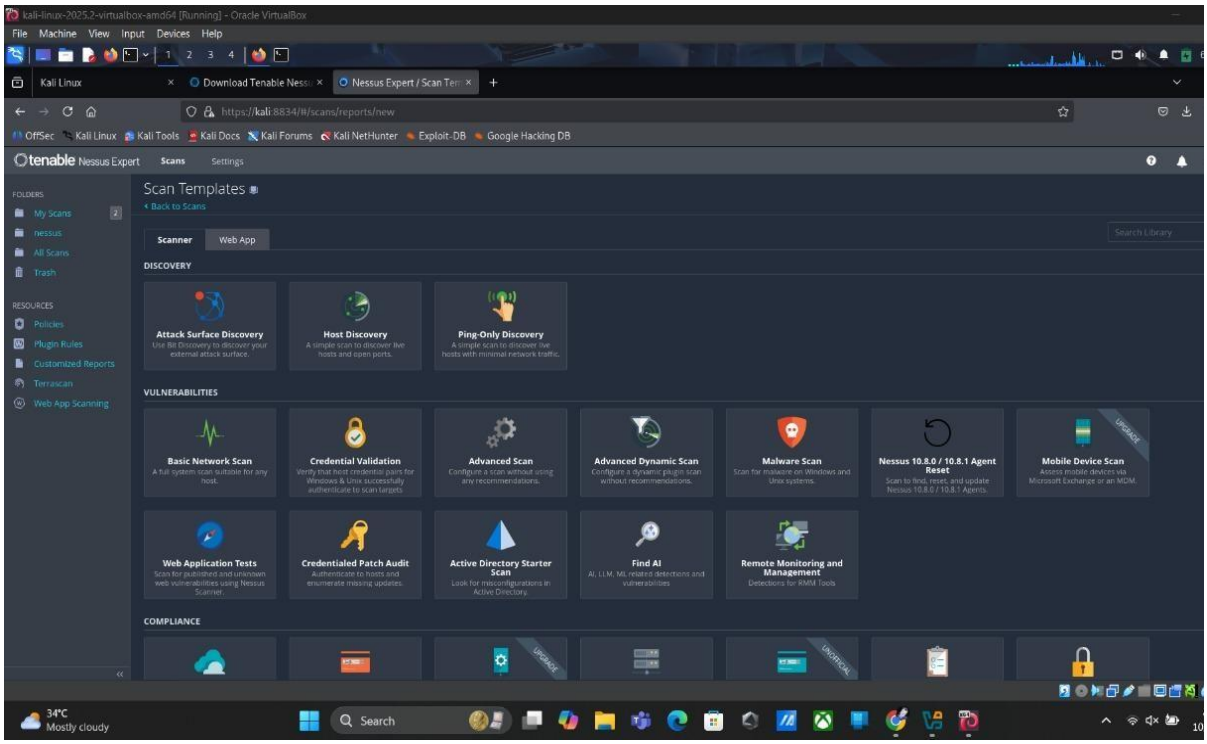
- **Target Machine:** Metasploit 2
- **IP Address:** 192.168.56.101
- **Operating System:** Kali Linux
- **Scan Type:** Basic Network Scan
- **Tool Used:** Nessus Essentials

3. Open Ports Detected

Nessus identified multiple open ports:

- 21 – FTP (vsftpd 2.3.4)
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 – DNS

- 80 – HTTP (Apache)
- 139 – NetBIOS
- 445 – SMB
- 3306 – MySQL
- 5432 – PostgreSQL



4. Critical Vulnerabilities Identified

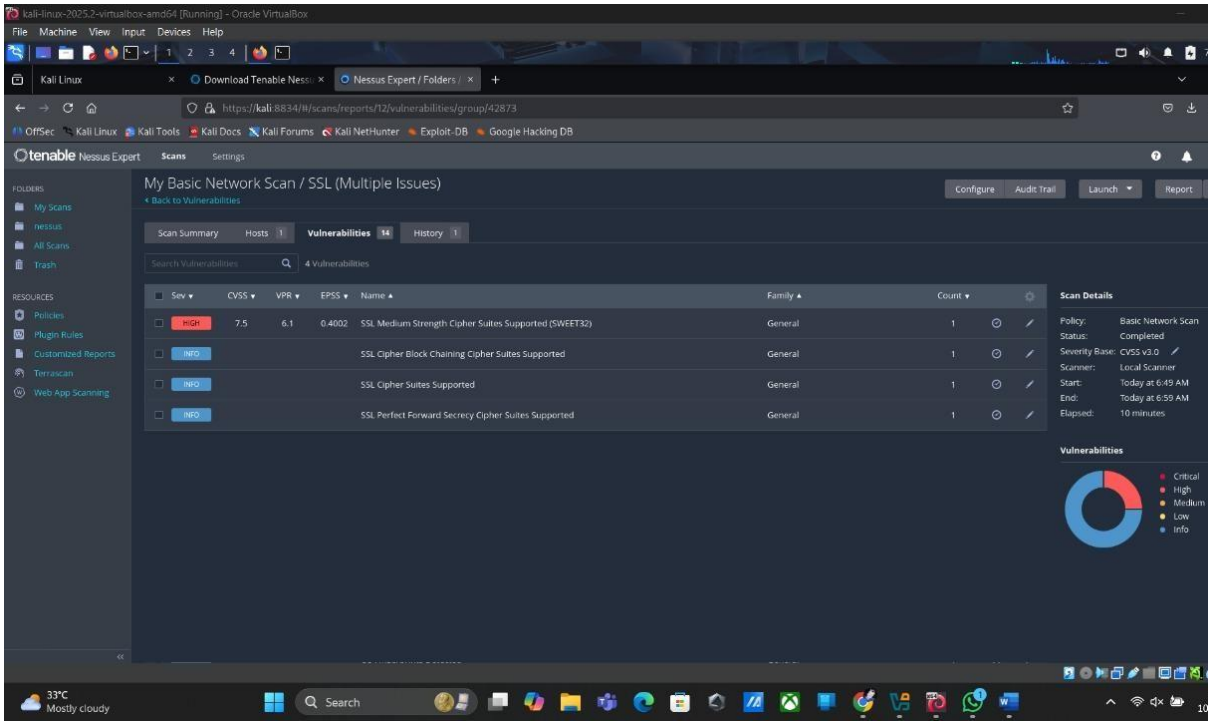
4.1 vsFTPd 2.3.4 Backdoor (Critical)

- **Port:** 21
- **Issue:** Backdoored FTP service
- **Risk:** Allows remote command execution
- **CVSS Score:** 10.0
- **Impact:** Full system compromise possible

4.2 Samba Remote Code Execution (High/Critical)

- **Port:** 445
- **Issue:** Outdated Samba version vulnerable to remote code execution
- **Risk:** Unauthorized access and data theft

- **CVSS Score:** ~9.3



4.3 UnrealIRCd Backdoor (Critical)

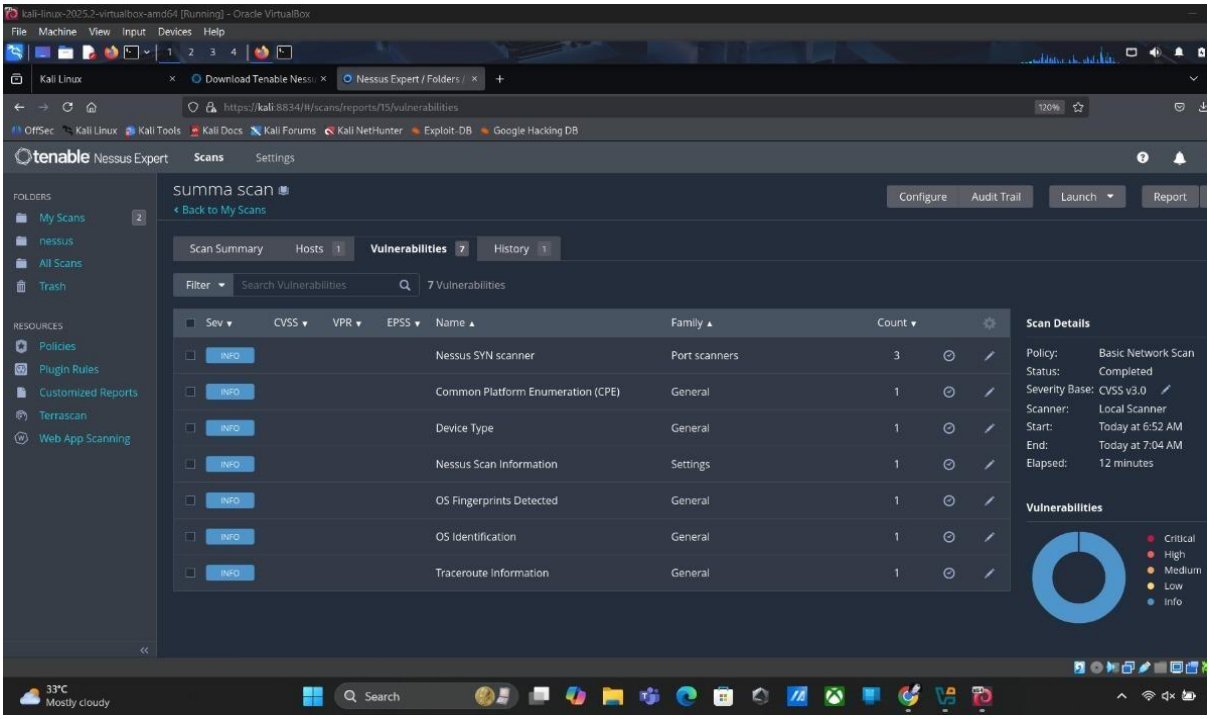
- **Port:** 6667
- **Issue:** Malicious backdoor in IRC daemon
- **Impact:** Remote command execution
- **CVSS Score:** 10.0

4.4 Weak SSH Configuration (Medium)

- **Port:** 22
- **Issue:** Supports weak encryption algorithms
- **Risk:** Man-in-the-middle attacks

4.5 Telnet Service Enabled (High)

- **Port:** 23
- **Issue:** Unencrypted login service
- **Risk:** Credentials transmitted in plaintext



5. Risk Analysis

The system is highly vulnerable because:

- Multiple services are outdated
- Remote code execution vulnerabilities exist
- Unencrypted services (Telnet, FTP) are active
- No proper service hardening

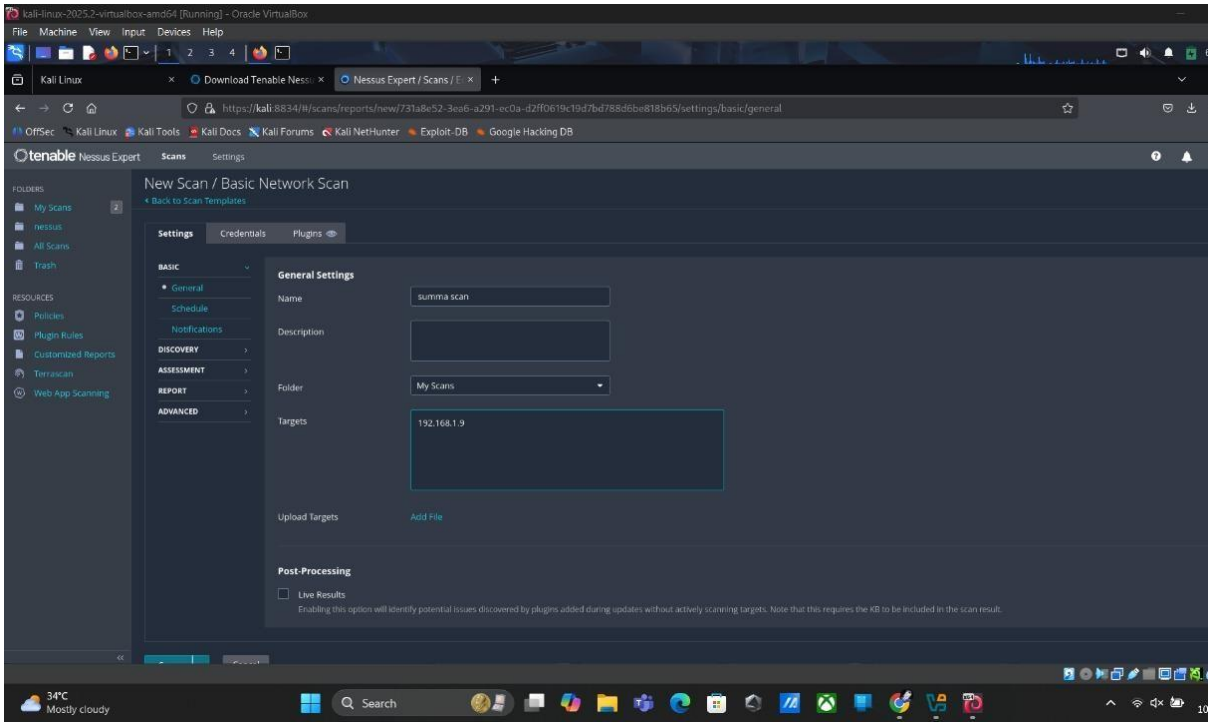
6. Remediation Recommendations

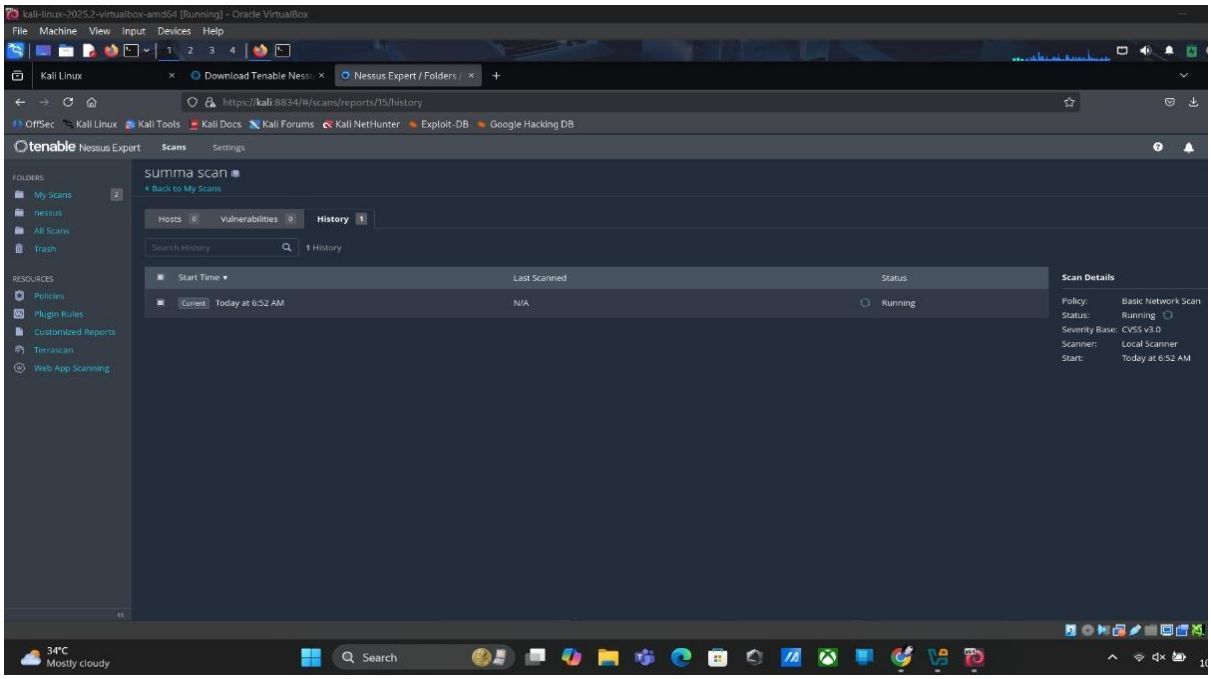
Since Metasploitable is intentionally vulnerable, remediation would include:

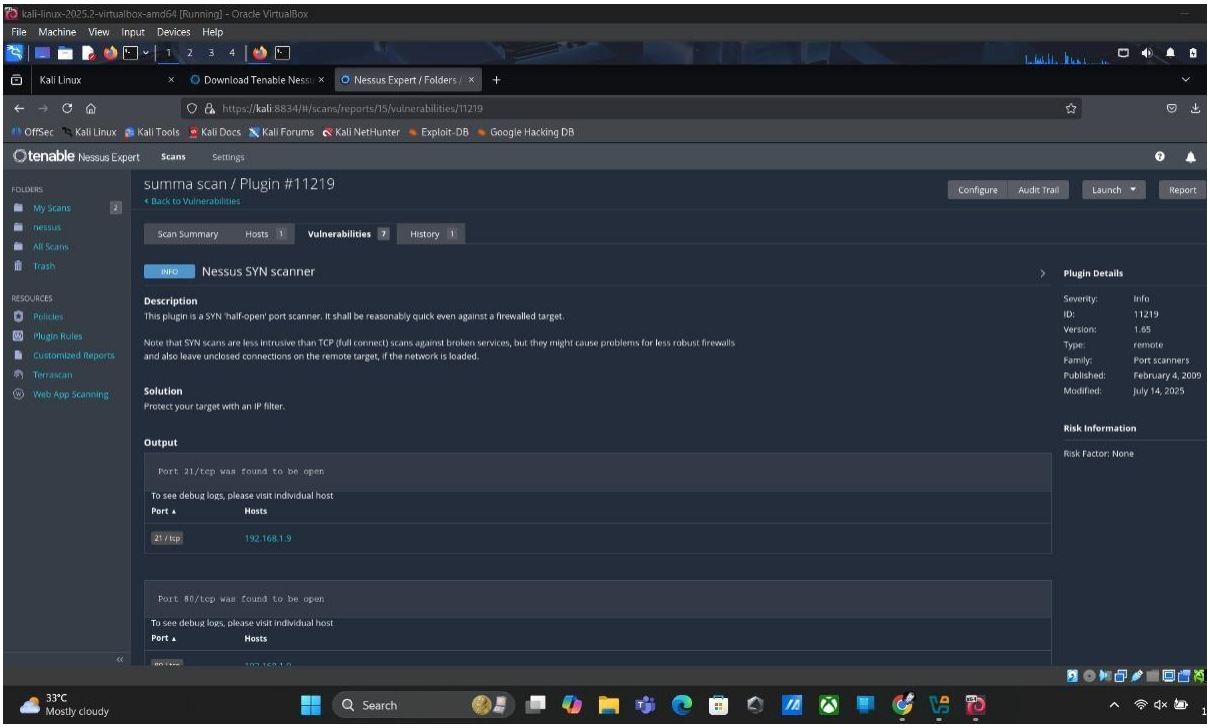
1. Remove vulnerable services (vsFTPd 2.3.4, UnrealIRCd)
2. Upgrade Samba to latest version
3. Disable Telnet (use SSH instead)
4. Close unused ports via firewall
5. Implement intrusion detection
6. Apply security patches regularly

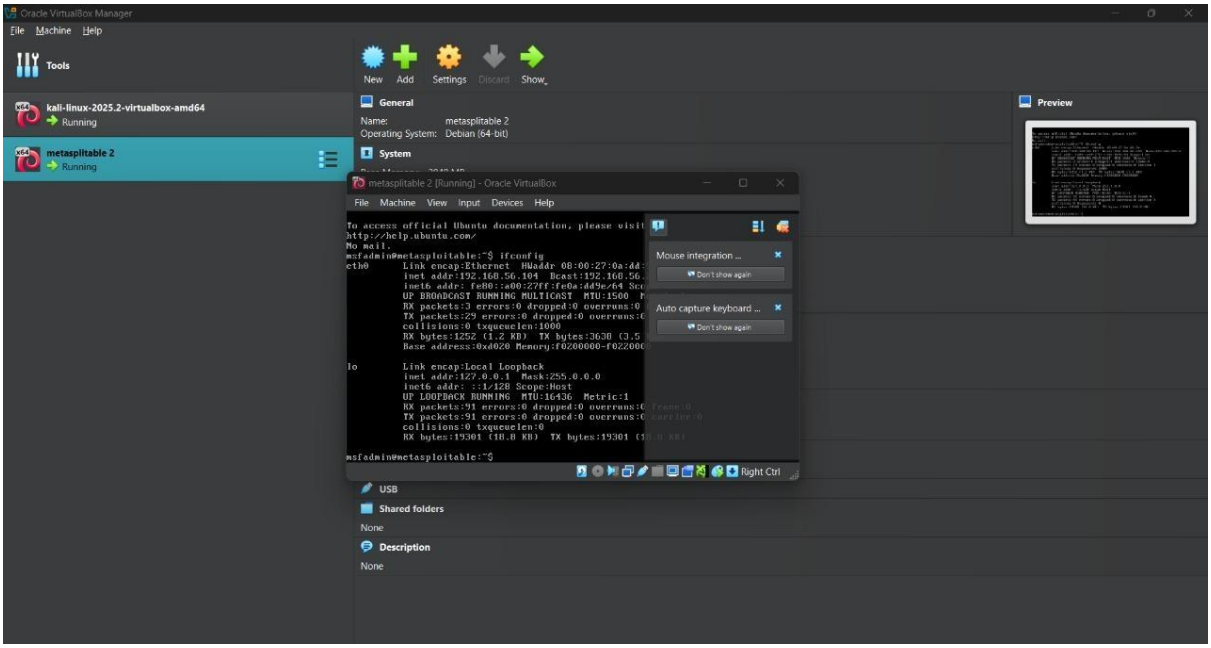
7. Key Concepts Applied

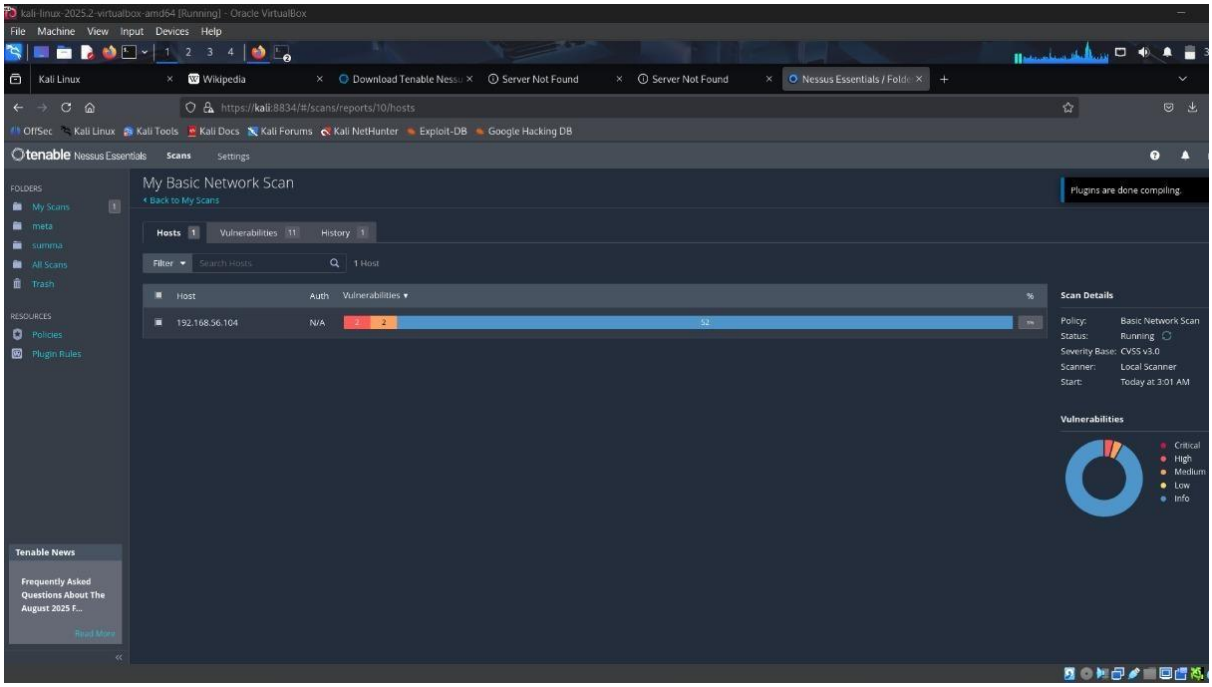
- Vulnerability scanning
- CVSS scoring
- Service enumeration
- Risk prioritization
- Remediation planning






kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
Download Tenable Nessus
Nessus Expert / Folders /
https://kali:8834/#/scans/reports/15/vulnerabilities/11219
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Expert
Scans
Settings
FOLDERS
My Scans
nessus
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
Web App Scanning
summa scan / Plugin #11219
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Scan Summary
Hosts 1
Vulnerabilities 7
History 1
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Port 21/tcp was found to be open
To see debug logs, please visit individual host
Port ▲
Hosts
21 / tcp
192.168.1.9
Port 80/tcp was found to be open
To see debug logs, please visit individual host
Port ▲
Hosts
Plugin Details
Severity: Info
ID: 11219
Version: 1.65
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: July 14, 2025
Risk Information
Risk Factor: None
33°C
Mostly cloudy
Search


Oracle VirtualBox Manager
File Machine Help
Tools
New
Add
Settings
Discard
Show
kali-linux-2025.2-virtualbox-amd64
Running
metasploitable 2
Running
General
Name: metasploitable 2
Operating System: Debian (64-bit)
System
Preview
metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:0a:4d:
inet addr:192.168.56.104 Bcast:192.168.56.
inet6 addr: fe80::a00:27ff:fe0a:4d9e/64 Sc
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:3 errors:0 dropped:0 overruns:0
TX packets:29 errors:0 dropped:0 overruns:0
collisions:0 txqueuelen:1000
RX bytes:1252 (1.2 KB) TX bytes:3630 (3.5
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0
TX packets:91 errors:0 dropped:0 overruns:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$
Mouse integration ...
Don't show again
Auto capture keyboard ...
Don't show again
Right Ctrl
USB
Shared folders
None
Description
None


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
Wikipedia
Download Tenable Ness
Server Not Found
Server Not Found
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/10/hosts
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
meta
summa
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Frequently Asked Questions About The August 2025 F...
Read More
My Basic Network Scan
Back to My Scans
Plugins are done compiling.
Hosts 1
Vulnerabilities 11
History 1
Filter
Search Hosts
1 Host
Host
Auth
Vulnerabilities
192.168.56.104
N/A
52
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:01 AM
Vulnerabilities
Critical
High
Medium
Low
Info