MISSION HACKERS

BANGLADESH

Assignment No-05

Assignment Title: Scanning Ports & Protocols

Course Title: Cybersecurity & Ethical Hacking

Submitted by:

Name: Istiak Alam

Phone: 01765376101

Submission Date: 24-07-25

Lab Task Topic: Scanning IP and Find Vulnerabilities using Nmap / Zenmap.

Submitted to:

MD Sha Jalal
Founder of Mission Hackers Bangladesh

🔍 What is Nmap?

Nmap (short for **Network Mapper**) is a **powerful open-source tool** used for:

- Scanning networks
- Discovering hosts and services
- Mapping network topology
- Finding open ports and vulnerabilities

🧑‍💻 It’s a hacker's microscope for network reconnaissance.

📦 Why is Nmap Used in Ethical Hacking?

Purpose	Example
🔎 Host Discovery	Find live systems in a network
🔓 Port Scanning	Identify open ports (22, 80, 443, etc.)
🎯 Service Detection	Identify what service is running on a port
🛡️ OS Detection	Find the operating system of a host
🚪 Vulnerability Scanning	Spot weak or outdated services

💻 Installing Nmap on Kali Linux

Already installed by default in Kali Linux. To check:

```
nmap --version
```

If not installed:

```
sudo apt update
sudo apt install nmap
```

🧪 Basic Nmap Commands (with Explanation)

✅ 1. **Ping Scan (Host Discovery)**

```
nmap -sn 192.168.1.0/24
```

- Scans the whole subnet to find **which hosts are up**.
- -sn: Ping only, don't scan ports.

✅ 2. **Basic Scan a Single Host**

```
nmap 192.168.1.10
```

- Default scan on a host: shows **open ports** and services.

✅ 3. **Scan Multiple Targets**

```
nmap 192.168.1.10 192.168.1.20
```

Or from a file:

```
nmap -iL targets.txt
```

✅ 4. **Port Scan (TCP by default)**

```
nmap -p 80,443 192.168.1.10
```

- Scan specific ports only.

```
nmap -p- 192.168.1.10
```

- Scan **all 65535** TCP ports.

✅ 5. **Service Version Detection**

```
nmap -sV 192.168.1.10
```

- Detects **version of services** running on open ports.

✅ 6. **Operating System Detection**

```
nmap -O 192.168.1.10
```

- Attempts to detect **OS type**.

✅ 7. **Aggressive Scan (All-in-One)**

```
nmap -A 192.168.1.10
```

- Performs:
  - OS Detection (-O)
  - Version Detection (-sV)
  - Script Scanning (-sC)
  - Trace-route

🛑 Warning: Very **loud** (detectable). Use carefully.

✅ 8. **Scan a Website**

```
nmap scanme.nmap.org
```

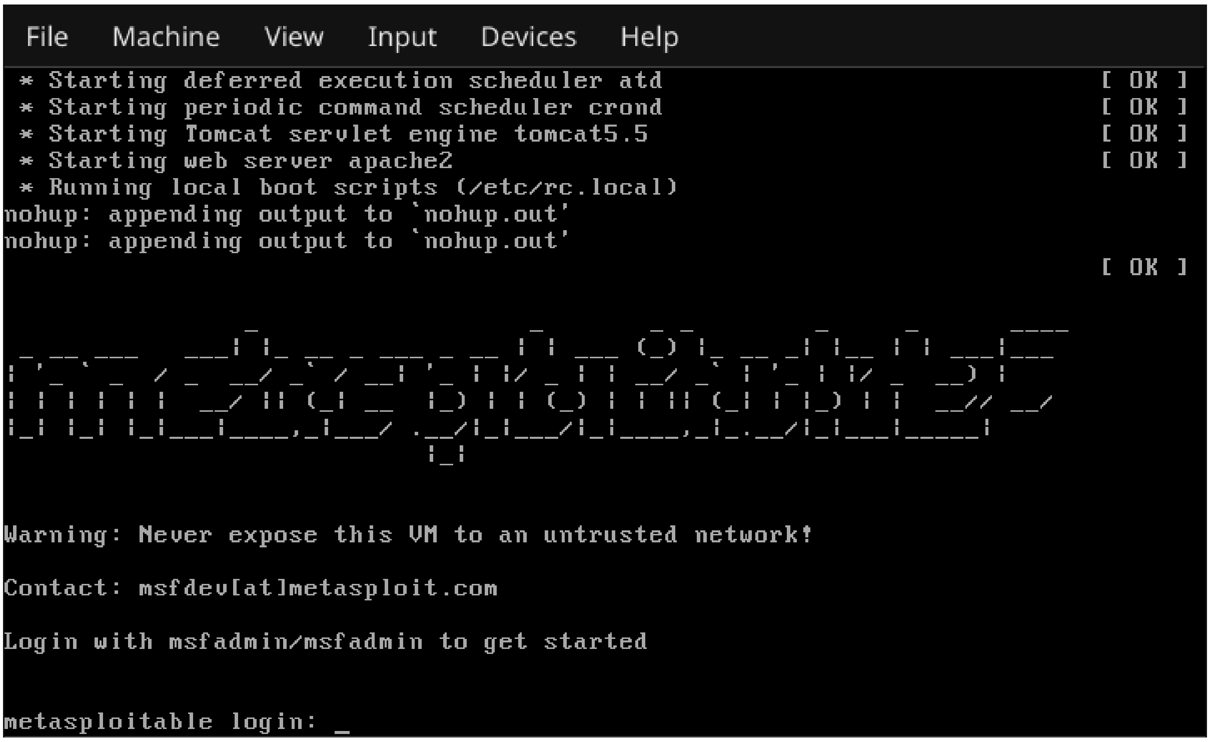
Note: scanme.nmap.org is an official **safe-to-scan** Nmap test server.

🧰 Nmap Scan Types

Option	Scan Type	Description
`-sS`	SYN Scan	Fast, stealthy (default)
`-sT`	TCP Connect	Full connection (less stealthy)
`-sU`	UDP Scan	Scans UDP ports
`-sA`	ACK Scan	Checks firewall rules
`-sN`	Null Scan	No flags set, stealth scan

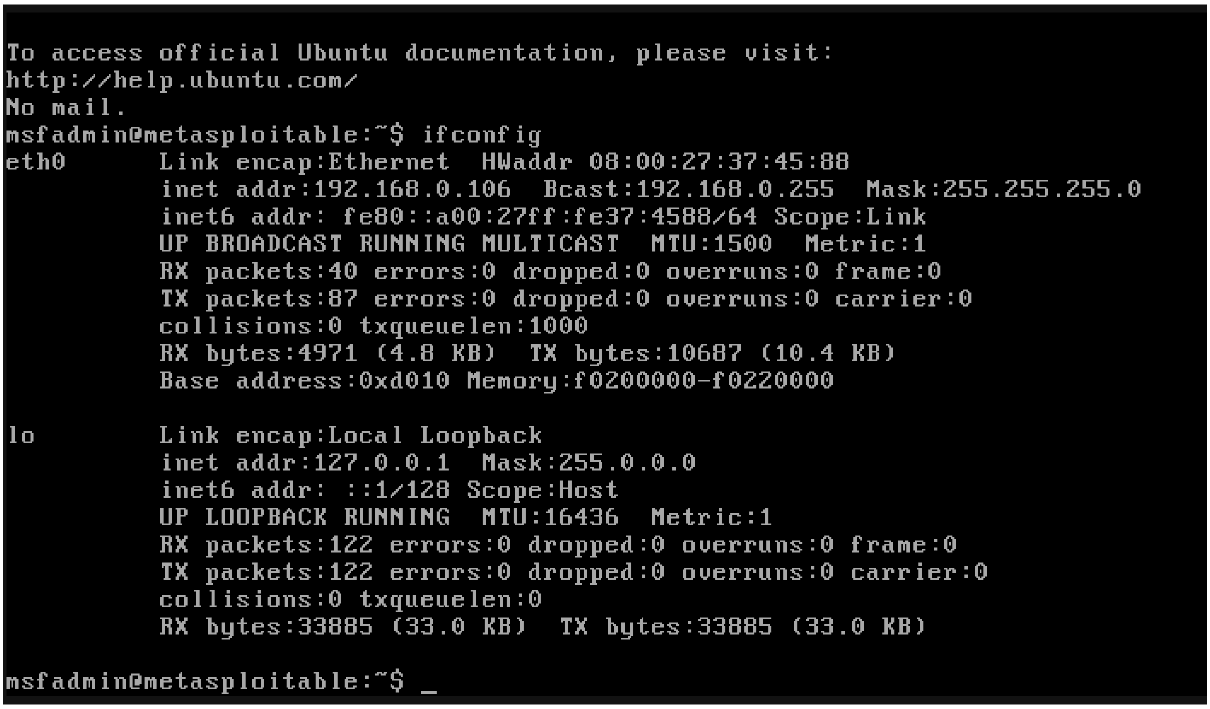
Lets Find Vulnerabilities of Metasploitable 2 using Nmap :

Step 1 : Open any Virtual Machine and boot Metasploitable2 Linux



```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

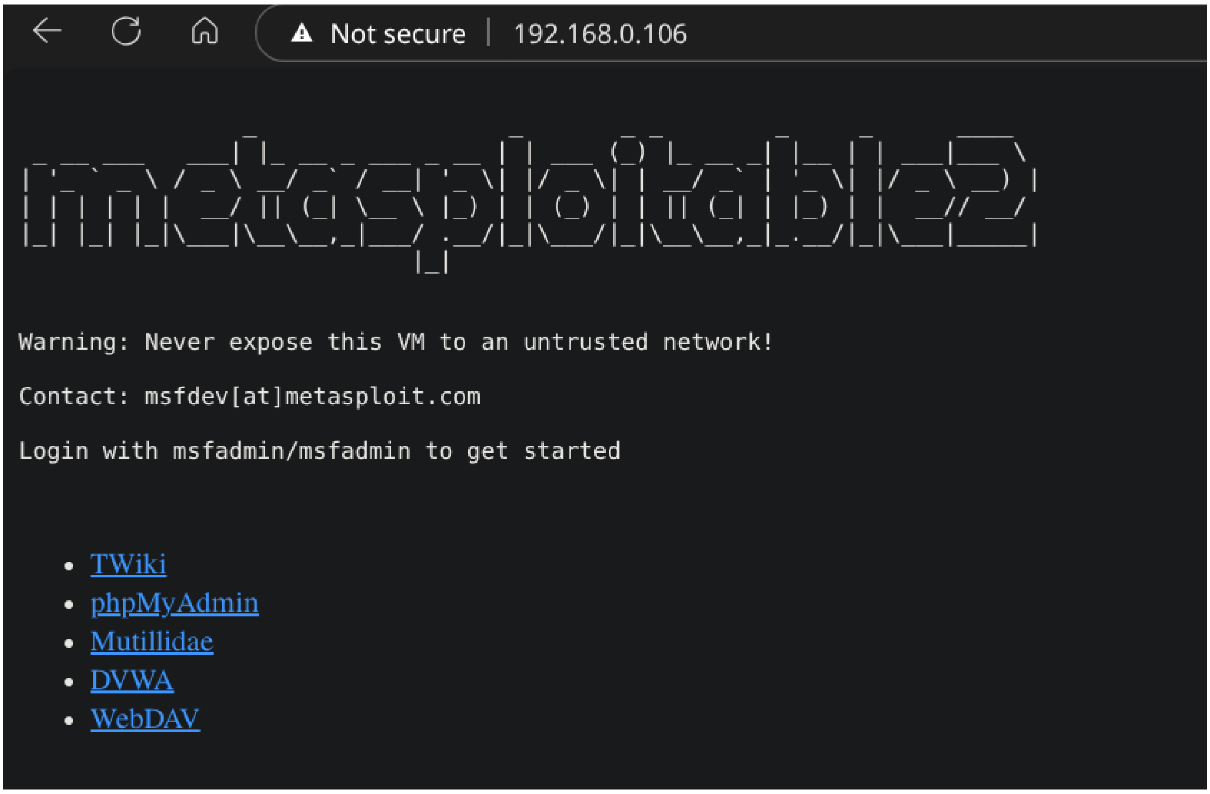
Step 2 : Login using **msfadmin** username and password
Step 3 : In the Metasploitable, find the IP address of the Vulnerable Machine by ‘ **ifconfig** ’



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:37:45:88
          inet addr:192.168.0.106  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe37:4588/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4971 (4.8 KB)  TX bytes:10687 (10.4 KB)
          Base address:0xd010 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:122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33885 (33.0 KB)  TX bytes:33885 (33.0 KB)

msfadmin@metasploitable:~$ _
```

we will get the IP showing in eth0 inet addr : **192.168.0.106**

Step 4 : In the host machine open browser and go the this IP, this will show the metasploitable2 host page



Warning: Never expose this VM to an untrusted network!

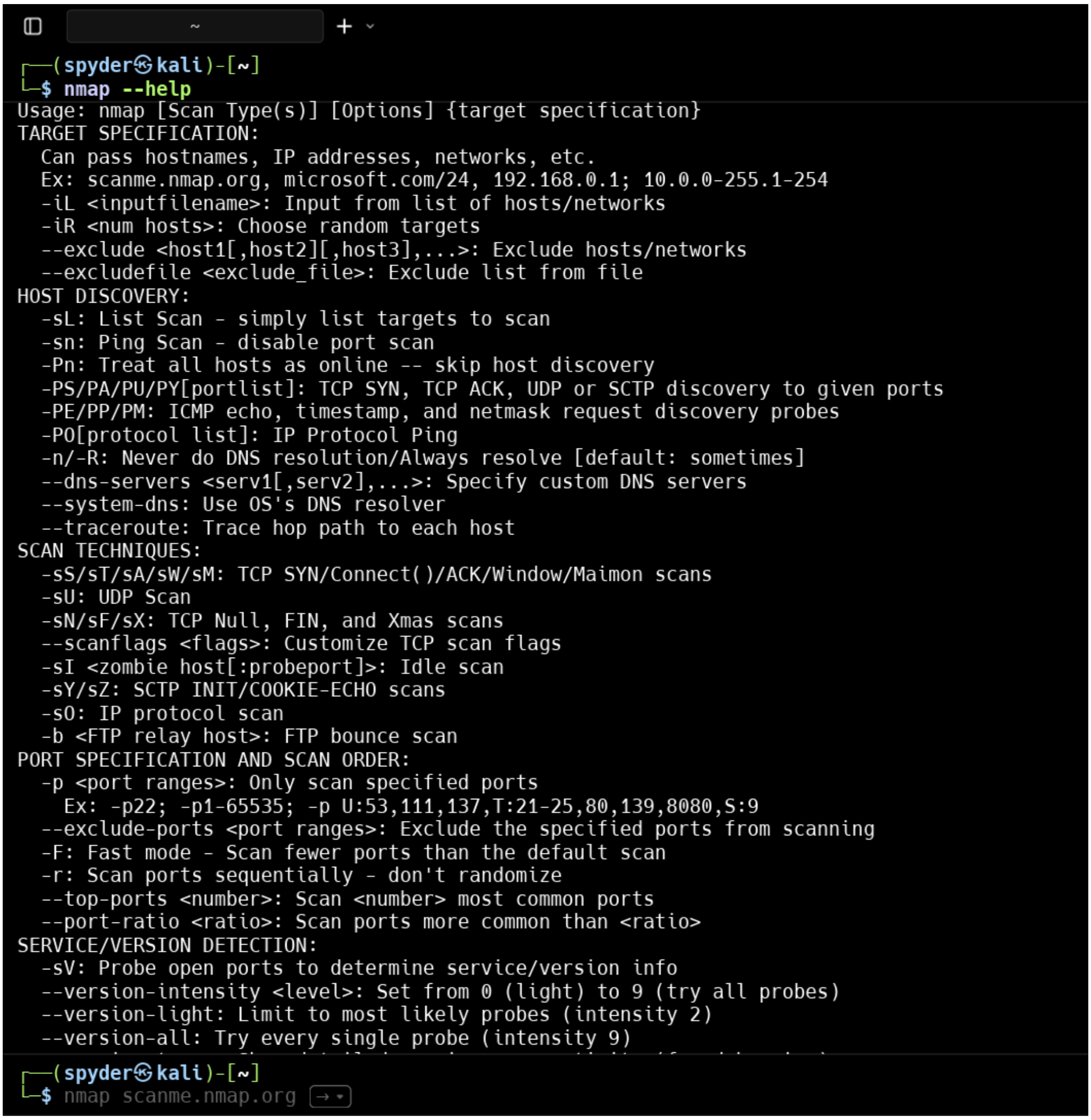
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

There we can see some vulnerable machines..

Step 5 : Open Terminal by ctrl+alt+t and run `nmap --help`



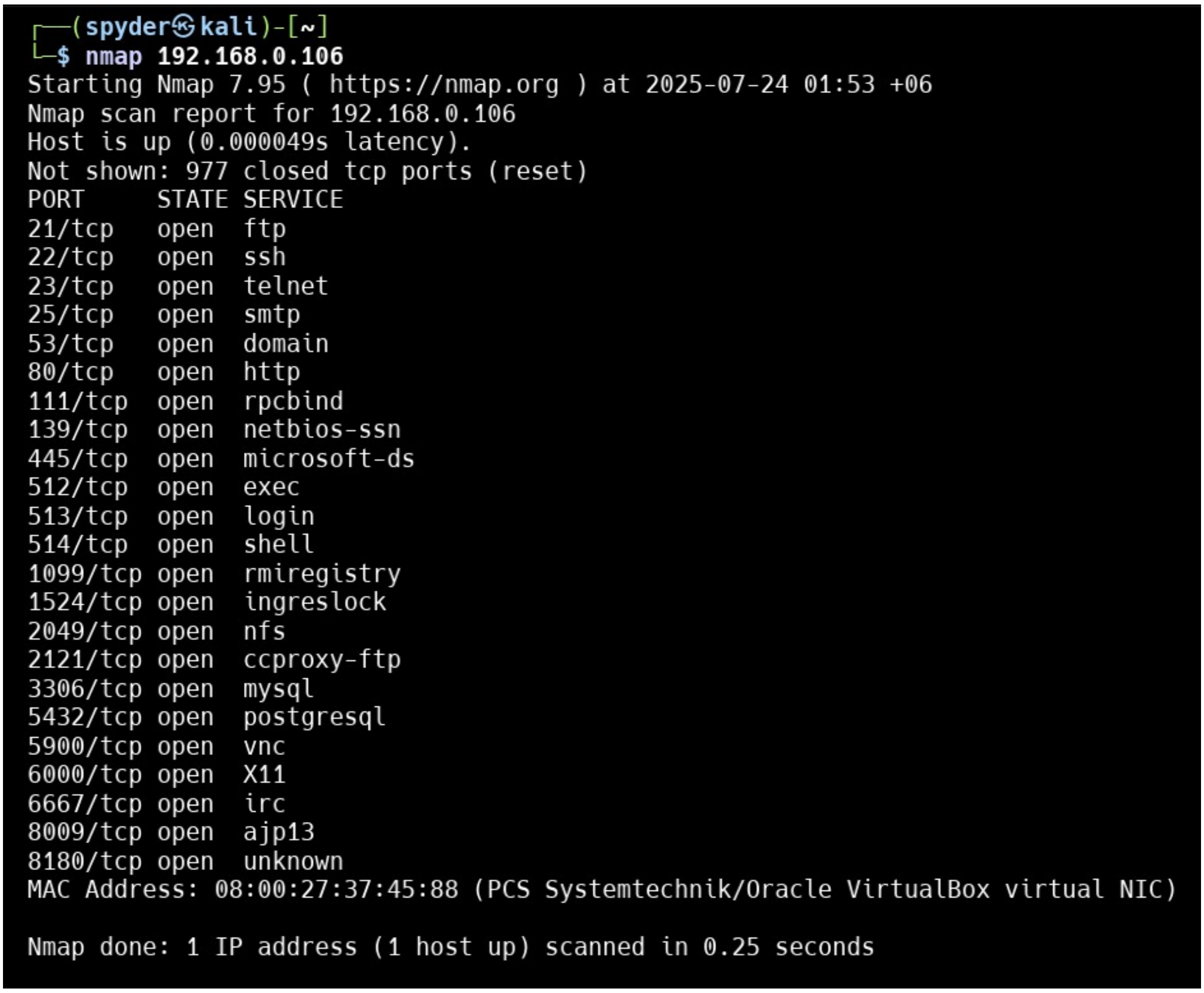
```
┌──(spyder㉿kali)-[~]
└─$ nmap --help
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
┌──(spyder㉿kali)-[~]
└─$ nmap scanme.nmap.org
```

Here we can see all the recommended commands and syntax of using nmap..

Using this Manual we can perform IP Address Vulnerabilities Scanning..

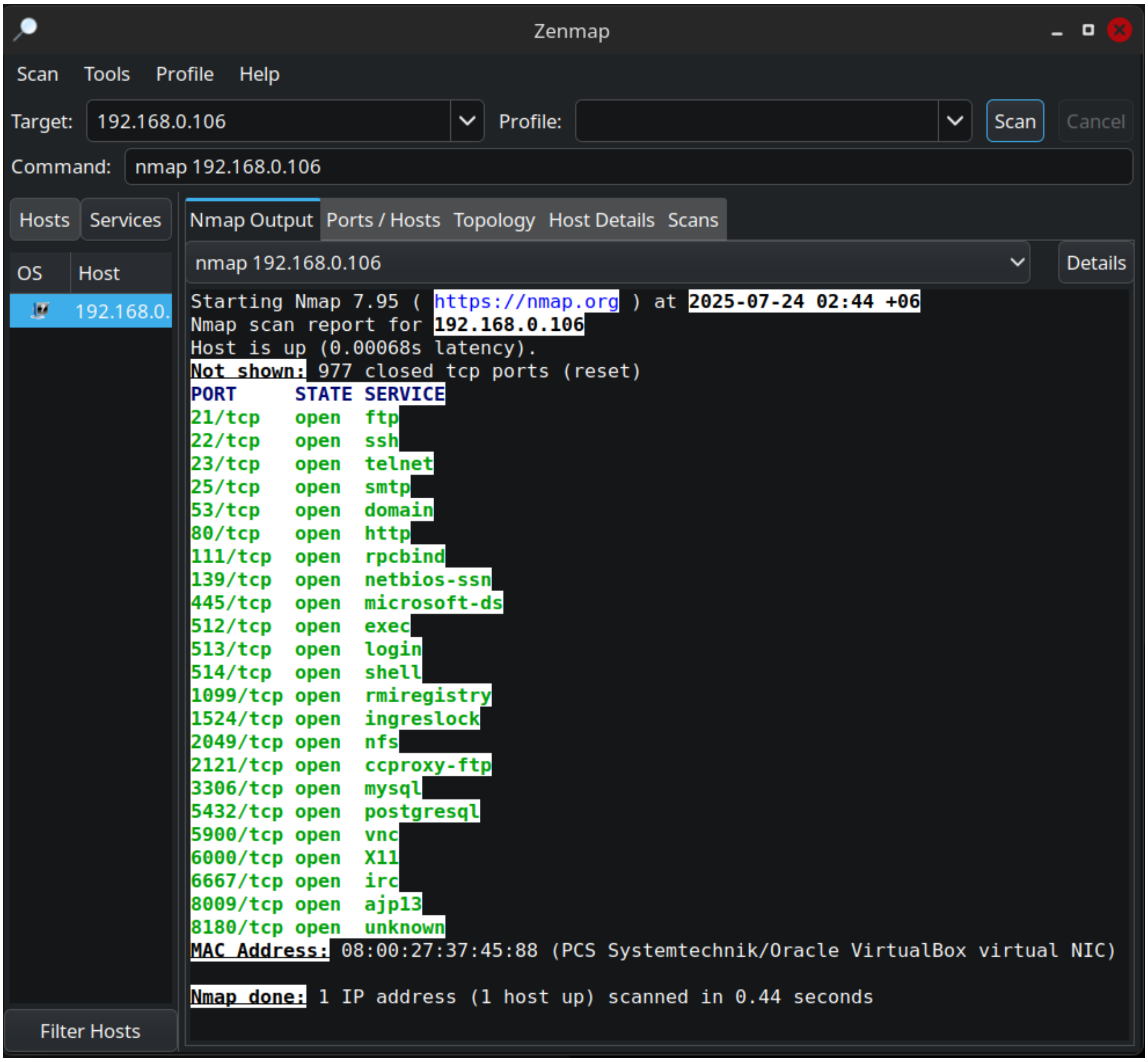
Step 6 : Start the Basic Scan for the Metasploitable machine in Nmap

```
nmap 192.168.0.106
```



```
┌──(spyder㉿kali)-[~]
└─$ nmap 192.168.0.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 01:53 +06
Nmap scan report for 192.168.0.106
Host is up (0.000049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:37:45:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

In the other hand we can use Zenmap for a basic scan..



Target: 192.168.0.106

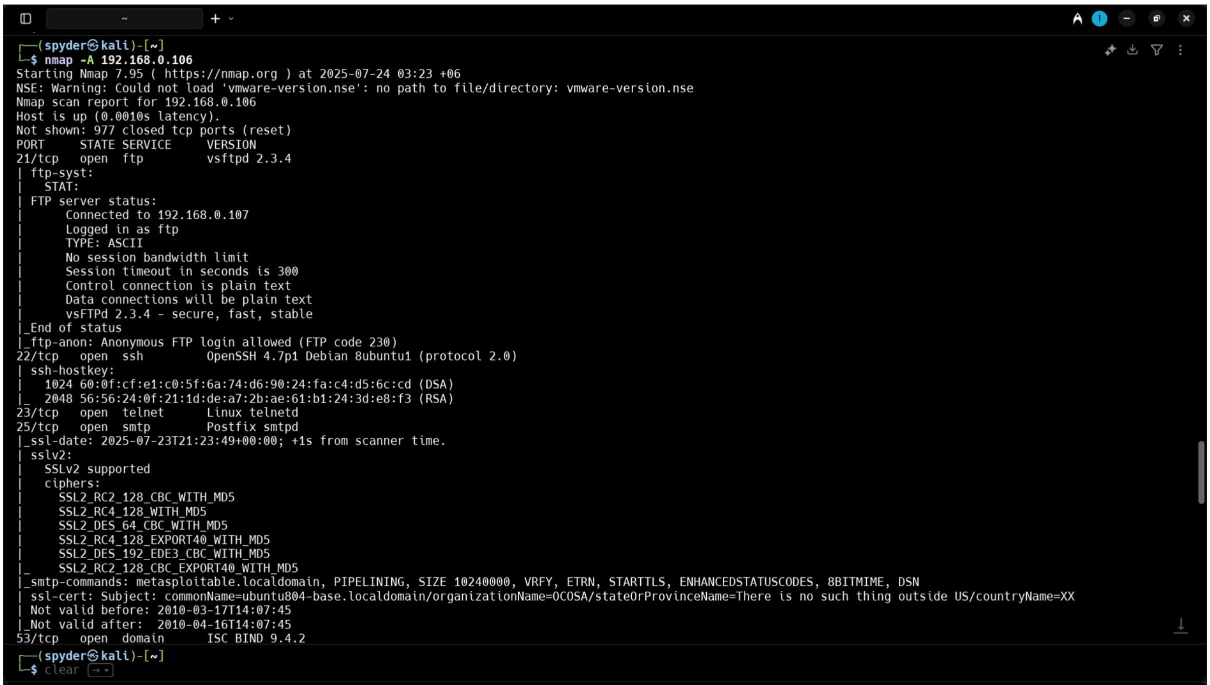
Command: nmap 192.168.0.106

nmap 192.168.0.106

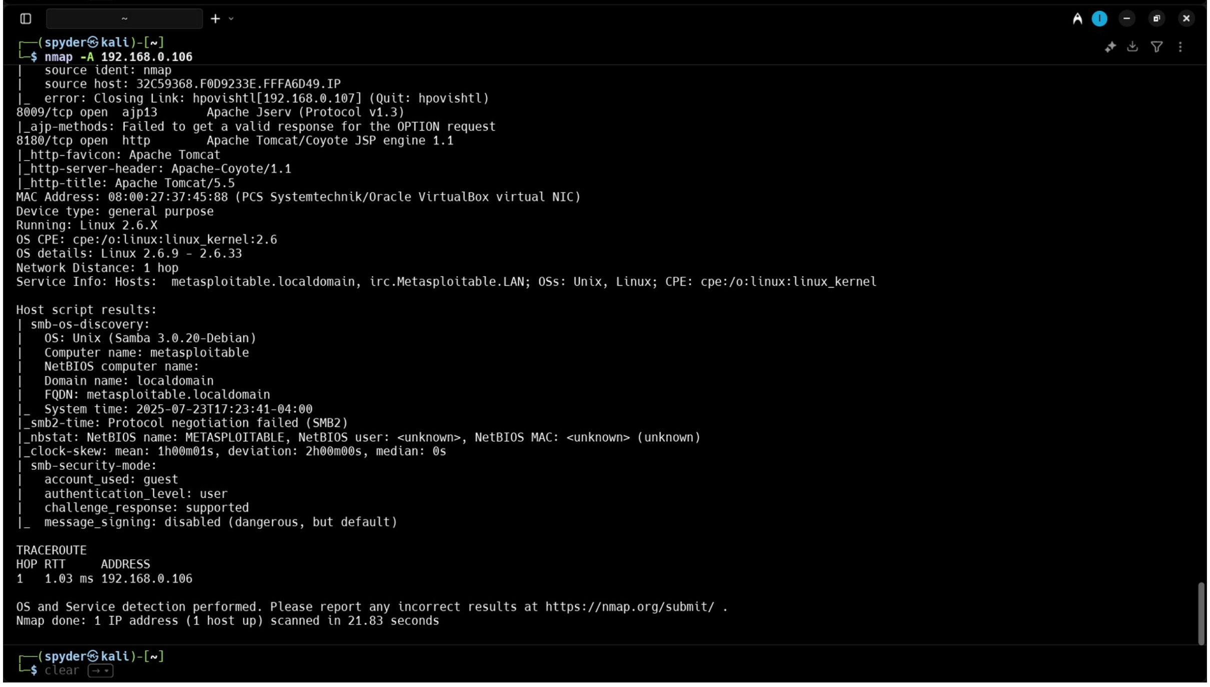
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 02:44 +06
Nmap scan report for 192.168.0.106
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
23/tcp    open   telnet
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
111/tcp   open   rpcbind
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
512/tcp   open   exec
513/tcp   open   login
514/tcp   open   shell
1099/tcp  open   rmiregistry
1524/tcp  open   ingreslock
2049/tcp  open   nfs
2121/tcp  open   ccproxy-ftp
3306/tcp  open   mysql
5432/tcp  open   postgresql
5900/tcp  open   vnc
6000/tcp  open   X11
6667/tcp  open   irc
8009/tcp  open   ajp13
8180/tcp  open   unknown
MAC Address: 08:00:27:37:45:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

Step 7 : Lets Start **Aggressive Scan (All-in-One) using**

```
nmap -A 192.168.0.106
```

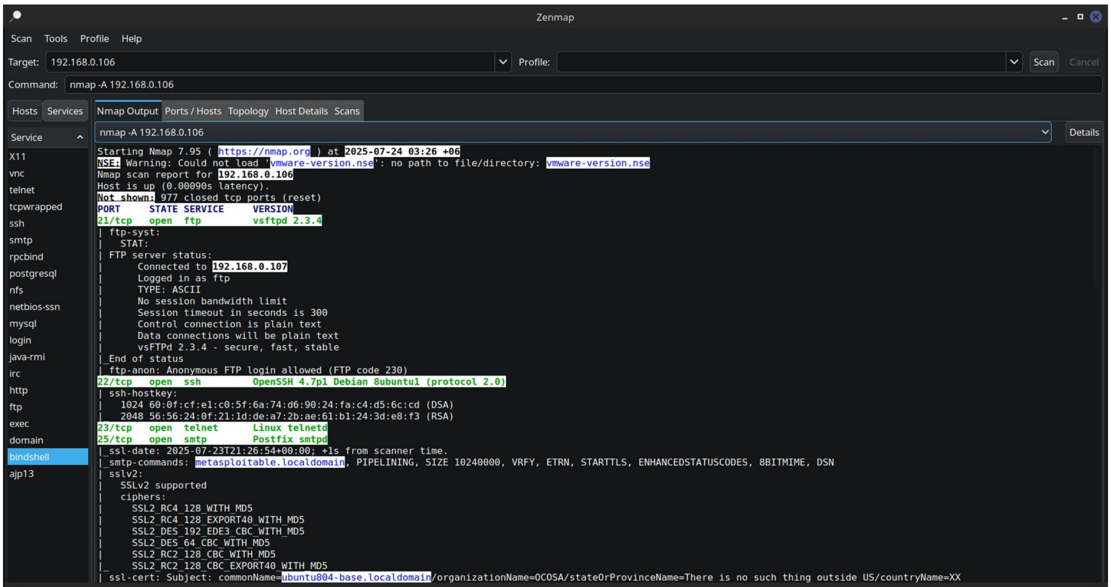


```
┌──(spyder㉿kali)-[~]
└─$ nmap -A 192.168.0.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:23 +06
NSE: Warning: Could not load 'vmware-version.nse': no path to file/directory: vmware-version.nse
Nmap scan report for 192.168.0.106
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.107
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-07-23T21:23:49+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
┌──(spyder㉿kali)-[~]
└─$ clear
```



```
┌──(spyder㉿kali)-[~]
└─$ nmap -A 192.168.0.106
|   source ident: nmap
|   source host: 32C59368.F0D9233E.FFFA6D49.IP
|_  error: Closing Link: hpovishtl[192.168.0.107] (Quit: hpovishtl)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:37:45:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-07-23T17:23:41-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   1.03 ms 192.168.0.106

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.83 seconds

┌──(spyder㉿kali)-[~]
└─$ clear
```

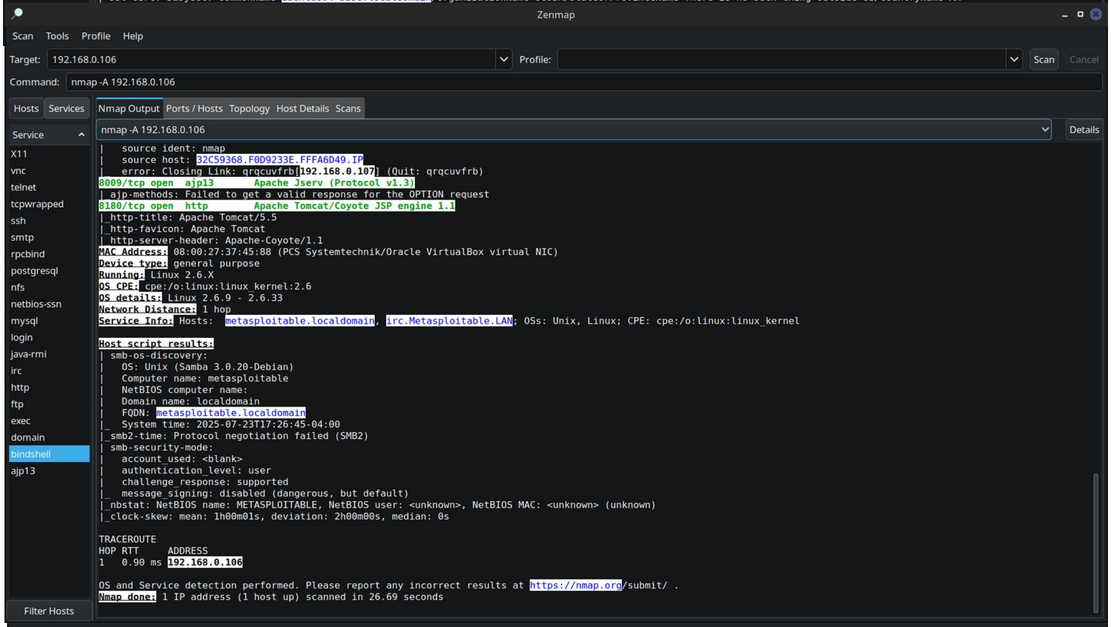
Start Aggressive Scan Using Zenmap :



Target: 192.168.0.106

Command: nmap -A 192.168.0.106

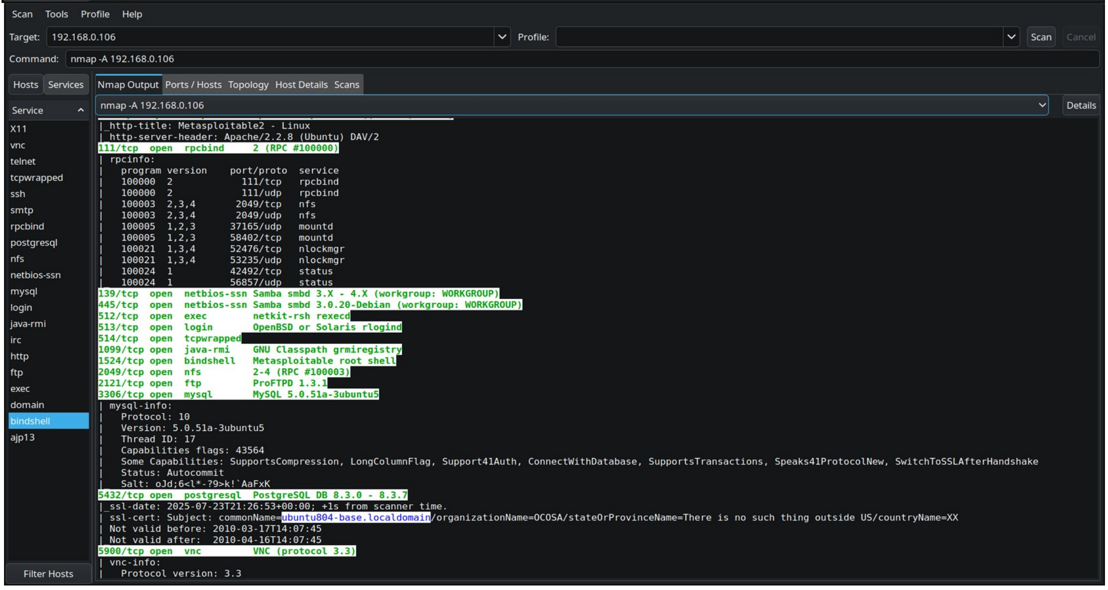
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:26 +06
NSE: Warning: Could not load 'vmware-version.nse': no path to file/directory: vmware-version.nse
Nmap scan report for 192.168.0.106
Host is up (0.00090s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.107
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-07-23T21:26:54+00:00; +1s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```



Target: 192.168.0.106

Command: nmap -A 192.168.0.106

```
|   source ident: nmap
|   source host: 32C59368.F0D9233E.FFFA6D49.IP
|_  error: Closing Link: qrqcuvfrb[192.168.0.107] (Quit: qrqcuvfrb)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:37:45:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-07-23T17:26:45-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 0s

TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms 192.168.0.106

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.69 seconds
```



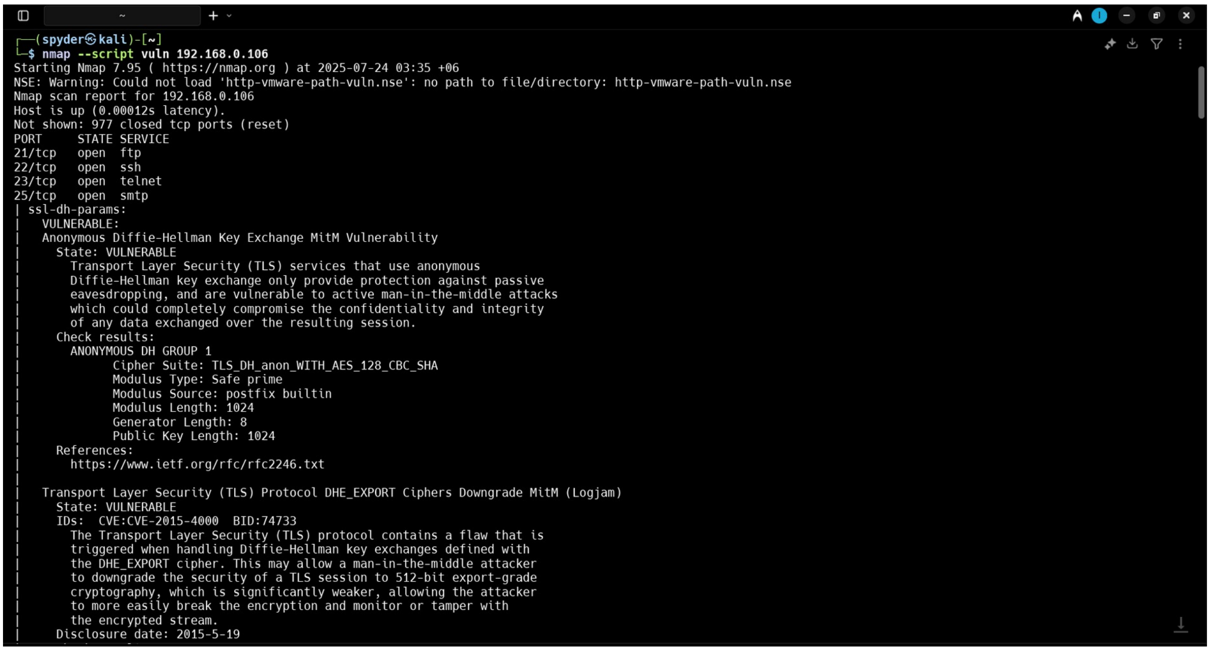
Target: 192.168.0.106

Command: nmap -A 192.168.0.106

```
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37165/udp   mountd
|   100005  1,2,3      58402/tcp   mountd
|   100021  1,3,4      52476/tcp   nlockmgr
|   100021  1,3,4      53235/udp   nlockmgr
|   100024  1          42492/tcp   status
|_  100024  1          56857/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, LongColumnFlag, Support41Auth, ConnectWithDatabase, SupportsTransactions, Speaks41ProtocolNew, SwitchToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: oJd;6<l*-?9>k!`AaFxK
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-07-23T21:26:53+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
```

Step 8 : Starting Aggressive Scan with OS , services, Script scan and vulnerabilities finder

`nmap --script vuln 192.168.0.106`



```
┌──(spyder㉿kali)-[~]
└─$ nmap --script vuln 192.168.0.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:35 +06
NSE: Warning: Could not load 'http-vmware-path-vuln.nse': no path to file/directory: http-vmware-path-vuln.nse
Nmap scan report for 192.168.0.106
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
```

Full Report is here :

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:35 +06
NSE: Warning: Could not load 'http-vmware-path-vuln.nse': no path to
file/directory: http-vmware-path-vuln.nse
Nmap scan report for 192.168.0.106
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against
passive
|       eavesdropping, and are vulnerable to active man-in-the-middle
attacks
|       which could completely compromise the confidentiality and
integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|      Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers
Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|         The Transport Layer Security (TLS) protocol contains a flaw
that is
|         triggered when handling Diffie-Hellman key exchanges defined
with
|          the DHE_EXPORT cipher. This may allow a man-in-the-middle
attacker
|        to downgrade the security of a TLS session to 512-bit export-
grade
|          cryptography, which is significantly weaker, allowing the
attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman
groups
|        of insufficient strength, especially those using one of a few
commonly
|         shared groups, may be susceptible to passive eavesdropping
attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
```

```
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and
other
|           products, uses nondeterministic CBC padding, which makes it
easier
|             for man-in-the-middle attackers to obtain cleartext data
via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.securityfocus.com/bid/70574
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-trace: TRACE is enabled
| http-sql-injection:
|   Possible sqli for queries:
|                          http://192.168.0.106:80/mutillidae/index.php?
page=framing.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=notes.php%27%20OR%20sqlspider
|            http://192.168.0.106:80/mutillidae/index.php?page=password-
generator.php%27%20OR%20sqlspider&username=anonymous
|                          http://192.168.0.106:80/mutillidae/index.php?
page=register.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?do=toggle-
hints%27%20OR%20sqlspider&page=home.php
|                          http://192.168.0.106:80/mutillidae/index.php?
page=installation.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=html5-
storage.php%27%20OR%20sqlspider
|                                   http://192.168.0.106:80/mutillidae/?
page=login.php%27%20OR%20sqlspider
|       http://192.168.0.106:80/mutillidae/index.php?page=pen-test-tool-
lookup.php%27%20OR%20sqlspider
|         http://192.168.0.106:80/mutillidae/index.php?page=site-footer-
xss-discussion.php%27%20OR%20sqlspider
|                       http://192.168.0.106:80/mutillidae/?page=source-
viewer.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/?page=view-someones-
blog.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?do=toggle-
security%27%20OR%20sqlspider&page=home.php
|                http://192.168.0.106:80/mutillidae/index.php?page=user-
poll.php%27%20OR%20sqlspider
```

```
|                          http://192.168.0.106:80/mutillidae/index.php?
page=login.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/?page=user-
info.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=home.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/mutillidae/index.php?page=set-background-
color.php%27%20OR%20sqlspider
|                 http://192.168.0.106:80/mutillidae/index.php?page=dns-
lookup.php%27%20OR%20sqlspider
|      http://192.168.0.106:80/mutillidae/index.php?page=view-someones-
blog.php%27%20OR%20sqlspider
|                 http://192.168.0.106:80/mutillidae/index.php?page=php-
errors.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=usage-
instructions.php%27%20OR%20sqlspider
|              http://192.168.0.106:80/mutillidae/index.php?page=secret-
administrative-pages.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?page=user-
info.php%27%20OR%20sqlspider
|              http://192.168.0.106:80/mutillidae/index.php?page=change-
log.htm%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=capture-
data.php%27%20OR%20sqlspider
|                                   http://192.168.0.106:80/mutillidae/?
page=credits.php%27%20OR%20sqlspider
|                    http://192.168.0.106:80/mutillidae/?page=text-file-
viewer.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
|        http://192.168.0.106:80/mutillidae/index.php?page=add-to-your-
blog.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/?page=show-
log.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/mutillidae/index.php?page=arbitrary-file-
inclusion.php%27%20OR%20sqlspider
|              http://192.168.0.106:80/mutillidae/index.php?page=source-
viewer.php%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=browser-
info.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=credits.php%27%20OR%20sqlspider
|                  http://192.168.0.106:80/mutillidae/?page=add-to-your-
blog.php%27%20OR%20sqlspider
|            http://192.168.0.106:80/mutillidae/index.php?page=captured-
data.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?page=show-
log.php%27%20OR%20sqlspider
|           http://192.168.0.106:80/mutillidae/index.php?page=text-file-
viewer.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.0.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.0.106:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.0.106:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.9%27%20OR%20sqlspider&rev1=1.10
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.9&rev1=1.10%27%20OR%20sqlspider
|                       http://192.168.0.106:80/view/TWiki/TWikiHistory?
rev=1.9%27%20OR%20sqlspider
|                       http://192.168.0.106:80/view/TWiki/TWikiHistory?
rev=1.8%27%20OR%20sqlspider
|                       http://192.168.0.106:80/oops/TWiki/TWikiHistory?
template=oopsrev%27%20OR%20sqlspider&param1=1.10
|                       http://192.168.0.106:80/oops/TWiki/TWikiHistory?
template=oopsrev&param1=1.10%27%20OR%20sqlspider
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.7%27%20OR%20sqlspider&rev1=1.8
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.7&rev1=1.8%27%20OR%20sqlspider
|                       http://192.168.0.106:80/view/TWiki/TWikiHistory?
rev=1.7%27%20OR%20sqlspider
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.8%27%20OR%20sqlspider&rev1=1.9
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.8&rev1=1.9%27%20OR%20sqlspider
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.9%27%20OR%20sqlspider&rev1=1.10
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.9&rev1=1.10%27%20OR%20sqlspider
|                       http://192.168.0.106:80/view/TWiki/TWikiHistory?
rev=1.9%27%20OR%20sqlspider
|                       http://192.168.0.106:80/view/TWiki/TWikiHistory?
rev=1.8%27%20OR%20sqlspider
|                       http://192.168.0.106:80/oops/TWiki/TWikiHistory?
template=oopsrev%27%20OR%20sqlspider&param1=1.10
|                       http://192.168.0.106:80/oops/TWiki/TWikiHistory?
template=oopsrev&param1=1.10%27%20OR%20sqlspider
|                       http://192.168.0.106:80/view/TWiki/TWikiHistory?
rev=1.7%27%20OR%20sqlspider
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.7%27%20OR%20sqlspider&rev1=1.8
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.7&rev1=1.8%27%20OR%20sqlspider
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.8%27%20OR%20sqlspider&rev1=1.9
|                      http://192.168.0.106:80/rdiff/TWiki/TWikiHistory?
rev2=1.8&rev1=1.9%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=framing.php%27%20OR%20sqlspider
|            http://192.168.0.106:80/mutillidae/index.php?page=password-
generator.php%27%20OR%20sqlspider&username=anonymous
|                          http://192.168.0.106:80/mutillidae/index.php?
page=register.php%27%20OR%20sqlspider
|         http://192.168.0.106:80/mutillidae/index.php?page=add-to-your-
blog.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=installation.php%27%20OR%20sqlspider
```

```
|              http://192.168.0.106:80/mutillidae/index.php?page=html5-
storage.php%27%20OR%20sqlspider
|                                  http://192.168.0.106:80/mutillidae/?
page=login.php%27%20OR%20sqlspider
|      http://192.168.0.106:80/mutillidae/index.php?page=pen-test-tool-
lookup.php%27%20OR%20sqlspider
|        http://192.168.0.106:80/mutillidae/index.php?page=site-footer-
xss-discussion.php%27%20OR%20sqlspider
|                      http://192.168.0.106:80/mutillidae/?page=source-
viewer.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/?page=view-someones-
blog.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=user-
poll.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/index.php?
page=login.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/index.php?
page=home.php%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=source-
viewer.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/mutillidae/index.php?page=set-background-
color.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?page=dns-
lookup.php%27%20OR%20sqlspider
|      http://192.168.0.106:80/mutillidae/index.php?page=view-someones-
blog.php%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=secret-
administrative-pages.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/index.php?
page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=user-
info.php%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=change-
log.htm%27%20OR%20sqlspider
|            http://192.168.0.106:80/mutillidae/index.php?page=capture-
data.php%27%20OR%20sqlspider
|                                  http://192.168.0.106:80/mutillidae/?
page=credits.php%27%20OR%20sqlspider
|                   http://192.168.0.106:80/mutillidae/?page=text-file-
viewer.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/index.php?
page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/mutillidae/index.php?page=arbitrary-file-
inclusion.php%27%20OR%20sqlspider
|                        http://192.168.0.106:80/mutillidae/?page=show-
log.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=rene-
magritte.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/index.php?
page=credits.php%27%20OR%20sqlspider
|            http://192.168.0.106:80/mutillidae/index.php?page=browser-
info.php%27%20OR%20sqlspider
|                 http://192.168.0.106:80/mutillidae/?page=add-to-your-
blog.php%27%20OR%20sqlspider
```

```
|           http://192.168.0.106:80/mutillidae/index.php?page=captured-
data.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=show-
log.php%27%20OR%20sqlspider
|          http://192.168.0.106:80/mutillidae/index.php?page=text-file-
viewer.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/?page=user-
info.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=framing.php%27%20OR%20sqlspider
|           http://192.168.0.106:80/mutillidae/index.php?page=password-
generator.php%27%20OR%20sqlspider&username=anonymous
|                          http://192.168.0.106:80/mutillidae/index.php?
page=register.php%27%20OR%20sqlspider
|        http://192.168.0.106:80/mutillidae/index.php?page=add-to-your-
blog.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=installation.php%27%20OR%20sqlspider
|              http://192.168.0.106:80/mutillidae/index.php?page=html5-
storage.php%27%20OR%20sqlspider
|                                   http://192.168.0.106:80/mutillidae/?
page=login.php%27%20OR%20sqlspider
|      http://192.168.0.106:80/mutillidae/index.php?page=pen-test-tool-
lookup.php%27%20OR%20sqlspider
|        http://192.168.0.106:80/mutillidae/index.php?page=site-footer-
xss-discussion.php%27%20OR%20sqlspider
|                       http://192.168.0.106:80/mutillidae/?page=source-
viewer.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/?page=view-someones-
blog.php%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=user-
poll.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=login.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/?page=user-
info.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=home.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/mutillidae/index.php?page=set-background-
color.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?page=dns-
lookup.php%27%20OR%20sqlspider
|      http://192.168.0.106:80/mutillidae/index.php?page=view-someones-
blog.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=change-
log.htm%27%20OR%20sqlspider
|               http://192.168.0.106:80/mutillidae/index.php?page=user-
info.php%27%20OR%20sqlspider
|                                   http://192.168.0.106:80/mutillidae/?
page=credits.php%27%20OR%20sqlspider
```

```
|             http://192.168.0.106:80/mutillidae/index.php?page=capture-
data.php%27%20OR%20sqlspider
|              http://192.168.0.106:80/mutillidae/index.php?page=secret-
administrative-pages.php%27%20OR%20sqlspider
|                    http://192.168.0.106:80/mutillidae/?page=text-file-
viewer.php%27%20OR%20sqlspider
|     http://192.168.0.106:80/mutillidae/index.php?page=arbitrary-file-
inclusion.php%27%20OR%20sqlspider
|                         http://192.168.0.106:80/mutillidae/?page=show-
log.php%27%20OR%20sqlspider
|              http://192.168.0.106:80/mutillidae/index.php?page=source-
viewer.php%27%20OR%20sqlspider
|                          http://192.168.0.106:80/mutillidae/index.php?
page=credits.php%27%20OR%20sqlspider
|             http://192.168.0.106:80/mutillidae/index.php?page=browser-
info.php%27%20OR%20sqlspider
|            http://192.168.0.106:80/mutillidae/index.php?page=captured-
data.php%27%20OR%20sqlspider
|                  http://192.168.0.106:80/mutillidae/?page=add-to-your-
blog.php%27%20OR%20sqlspider
|                http://192.168.0.106:80/mutillidae/index.php?page=show-
log.php%27%20OR%20sqlspider
|_         http://192.168.0.106:80/mutillidae/index.php?page=text-file-
viewer.php%27%20OR%20sqlspider
| http-csrf:
|     Spidering    limited    to:    maxdepth=3;    maxpagecount=20;
withinhost=192.168.0.106
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.0.106:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.0.106:80/dvwa/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
|     Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
|     Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
|     Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
|     Path: http://192.168.0.106:80/twiki/TWikiDocumentation.html
|     Form id:
|_    Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
```

```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to
debug)
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|       /doc/:  Potentially  interesting  directory  w/  listing  on
'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|       RMI  registry  default  configuration  remote  code  execution
vulnerability
|     State: VULNERABLE
|         Default configuration of RMI registry allows loading classes
from remote URLs which can lead to remote code execution.
|
|     References:
|_
https://github.com/rapid7/metasploit-framework/blob/master/modules/
exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and
other
|           products, uses nondeterministic CBC padding, which makes it
easier
|             for man-in-the-middle attackers to obtain cleartext data
via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
```

```
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.securityfocus.com/bid/70574
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before
1.0.1h
|       does not properly restrict processing of ChangeCipherSpec
messages,
|       which allows man-in-the-middle attackers to trigger use of a
zero
|       length master key in certain OpenSSL-to-OpenSSL communications,
and
|       consequently hijack sessions or obtain sensitive information,
via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.cvedetails.com/cve/2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman
groups
|       of insufficient strength, especially those using one of a few
commonly
|       shared groups, may be susceptible to passive eavesdropping
attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd.
See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.jsp:
|     JSESSIONID:
```

```
|       httponly flag not set
|   /admin/adminLogin.jsp:
|     JSESSIONID:
|       httponly flag not set
|
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.htm
l:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|_      httponly flag not set
| 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:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
```

```
|
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.htm
l: OpenCart/FCKeditor File upload
|    /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP
Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
MAC  Address:  08:00:27:37:45:88  (PCS  Systemtechnik/Oracle  VirtualBox
virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 334.17 seconds
```

Summarized List of all the ssl-dh-params Vulnerabilities :

1. Anonymous Diffie-Hellman Key Exchange MitM Vulnerability :

```
Check results:
      ANONYMOUS DH GROUP 1
             Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
             Modulus Type: Safe prime
             Modulus Source: postfix builtin
             Modulus Length: 1024
             Generator Length: 8
             Public Key Length: 1024
```

2. Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)

```
IDs:  CVE:CVE-2015-4s000  BID:74733
Check results:
       EXPORT-GRADE DH GROUP 1
             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
             Modulus Type: Safe prime
             Modulus Source: Unknown/Custom-generated
             Modulus Length: 512
             Generator Length: 8
             Public Key Length: 512
```

3. Diffie-Hellman Key Exchange Insufficient Group Strength

```
Check results:
       WEAK DH GROUP 1
             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
             Modulus Type: Safe prime
             Modulus Source: postfix builtin
             Modulus Length: 1024
             Generator Length: 8
             Public Key Length: 1024
```

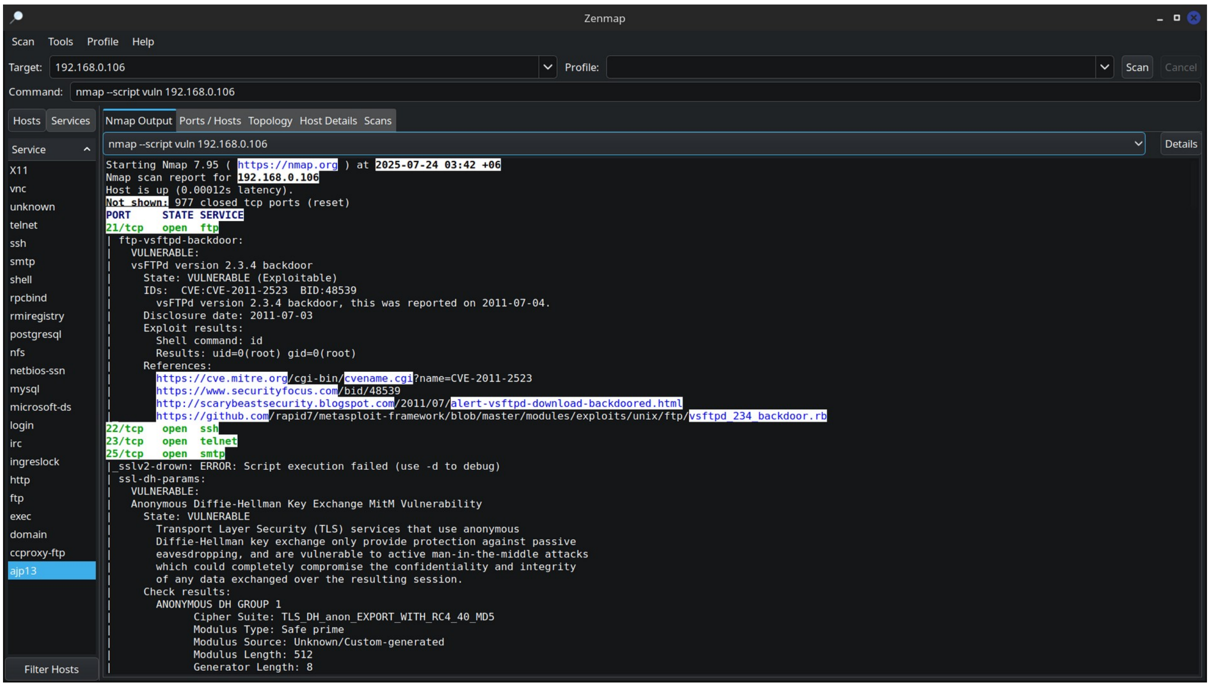
Summarized List of all the ssl-poodle Vulnerabilities :

1. SSL POODLE information leak
```
IDs:  CVE:CVE-2014-3566  BID:70574
Check results:
       TLS_RSA_WITH_AES_128_CBC_SHA
```

Summarized List of all the http-slowloris-check Vulnerabilities :

1. Slowloris DOS attack
```
IDs:  CVE:CVE-2007-6750
```

Same as we can find Vulnerabilities using Zenmap :



Target: 192.168.0.106

Command: nmap --script vuln 192.168.0.106

```
nmap --script vuln 192.168.0.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:42 +06
Nmap scan report for 192.168.0.106
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
```