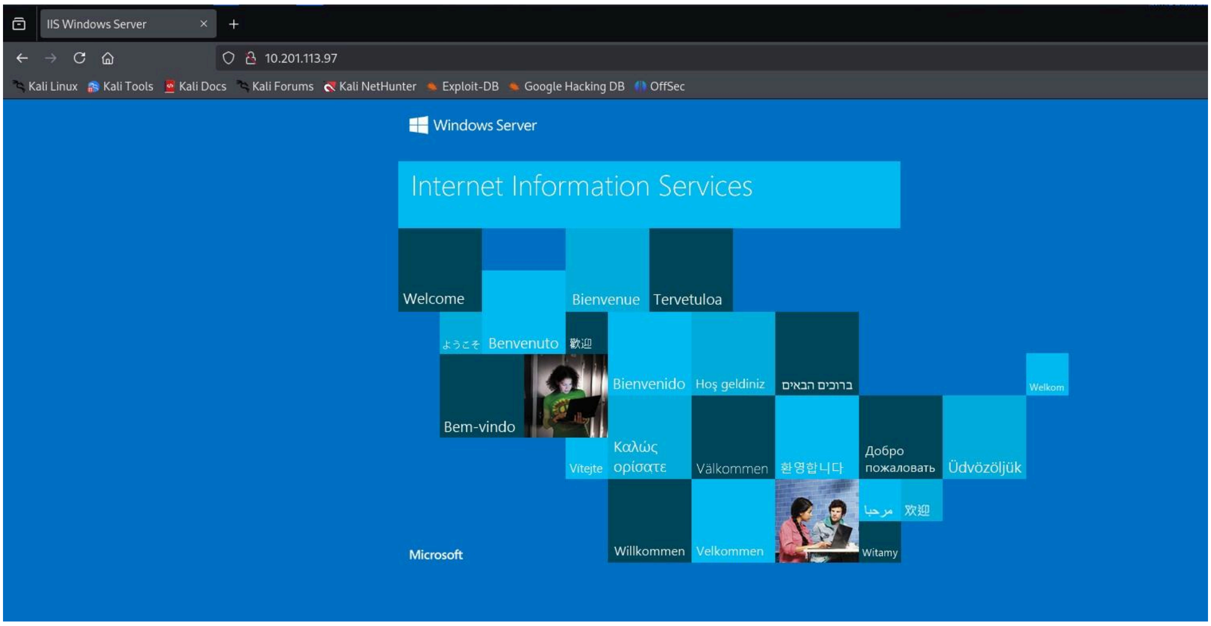
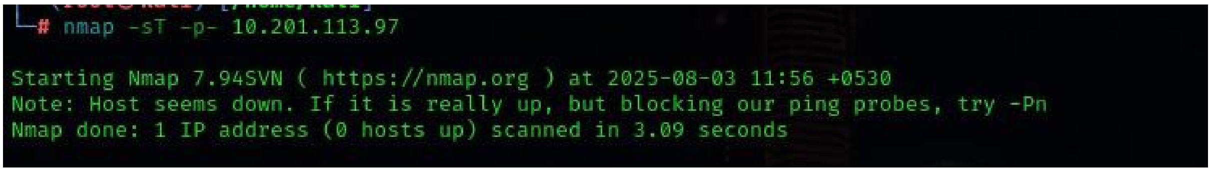
Report on Nmap–Muhammed Nidal

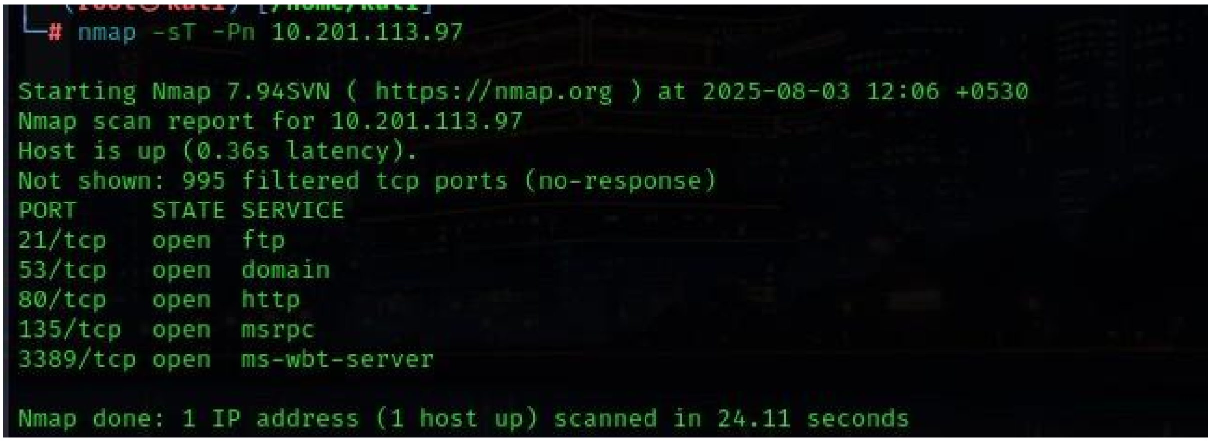


I Connected to the Tryhackme Openvpn and accessed the victim Ip
In first day i got 10.201.113.97 afterwards u can see there will be change in Victim IP's

TCP Connect Scans



```
└─# nmap -sT -p- 10.201.113.97

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-03 11:56 +0530
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
```

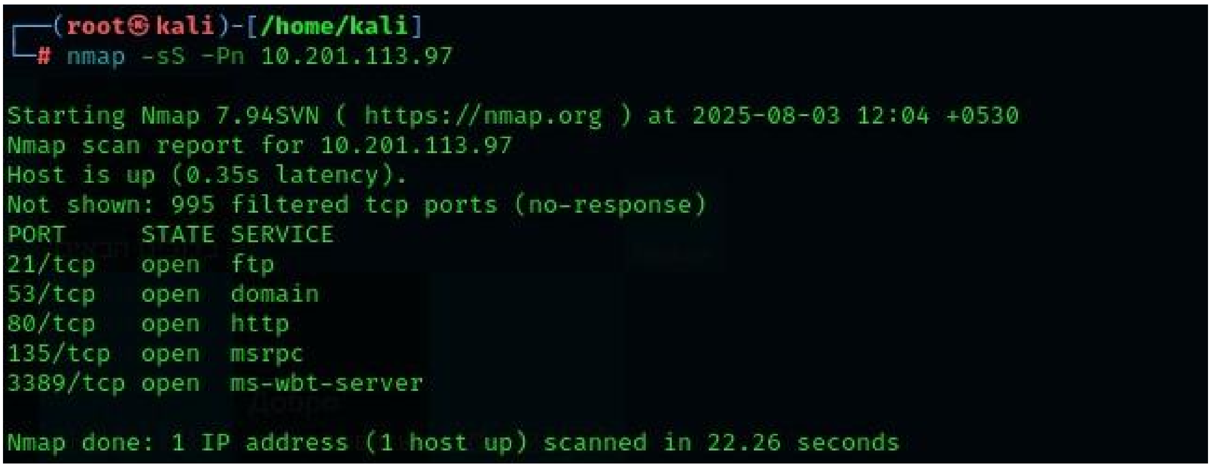


```
└─# nmap -sT -Pn 10.201.113.97

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-03 12:06 +0530
Nmap scan report for 10.201.113.97
Host is up (0.36s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 24.11 seconds
```

What i understood is that as the name suggested TCP is a 3 way handshake procedure basis on that i got info about open and closed ports, at first host was down, in 2nd method i forced nmap to beleive the host was up to scan the ports using -Pn

Report on Nmap–Muhammed Nidal

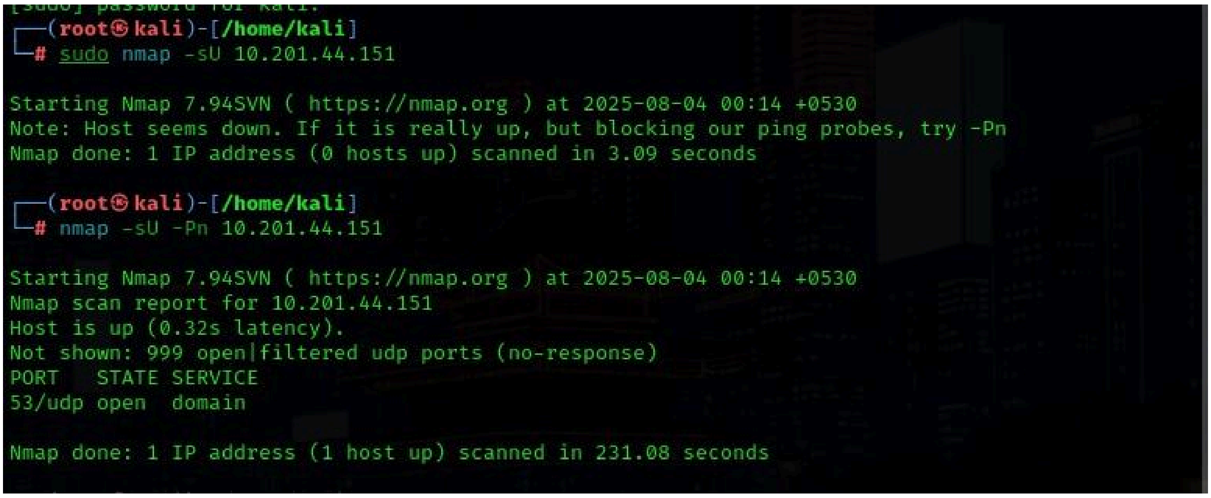
SYN SCAN



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -Pn 10.201.113.97

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-03 12:04 +0530
Nmap scan report for 10.201.113.97
Host is up (0.35s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 22.26 seconds
```

More stealthier than the Tcp one because , 3 way handshake only 2 way is completed and RST is replied to tear the connection instead of ACK

UDP SCAN

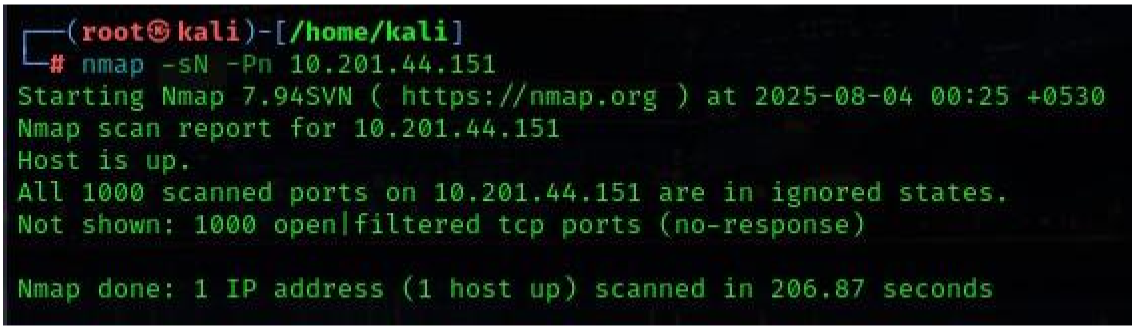


```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sU 10.201.44.151

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 00:14 +0530
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -Pn 10.201.44.151

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 00:14 +0530
Nmap scan report for 10.201.44.151
Host is up (0.32s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 231.08 seconds
```

Report on Nmap–Muhammed Nidal

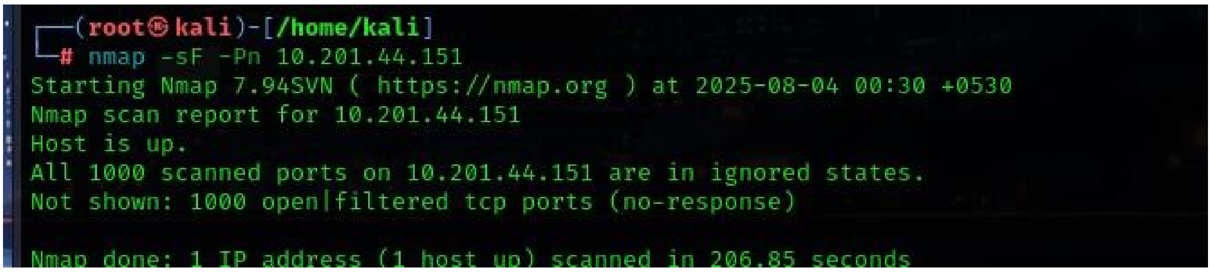
Instead of Tcp protocol UDp protocol is used and ports that use this protocol can only be accessed.
Slower than Tcp ones

Null scan



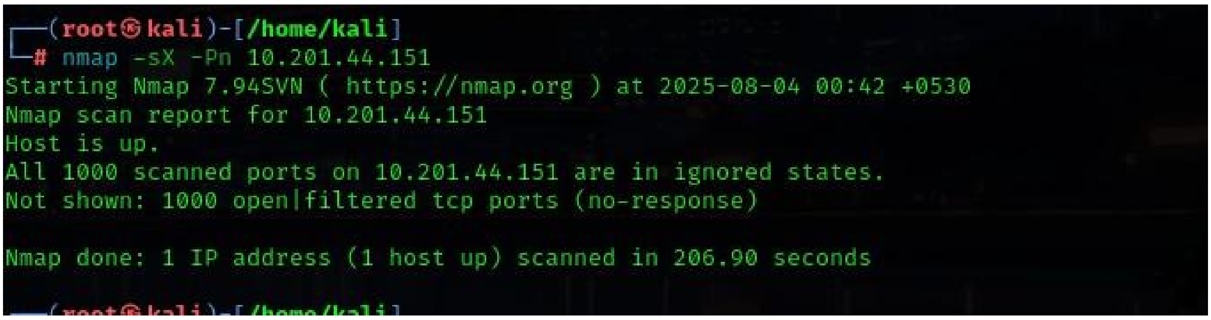
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sN -Pn 10.201.44.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 00:25 +0530
Nmap scan report for 10.201.44.151
Host is up.
All 1000 scanned ports on 10.201.44.151 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 206.87 seconds
```

Packets doesnt contain any packets , if closed a reply is gotten else no reply



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sF -Pn 10.201.44.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 00:30 +0530
Nmap scan report for 10.201.44.151
Host is up.
All 1000 scanned ports on 10.201.44.151 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 206.85 seconds
```

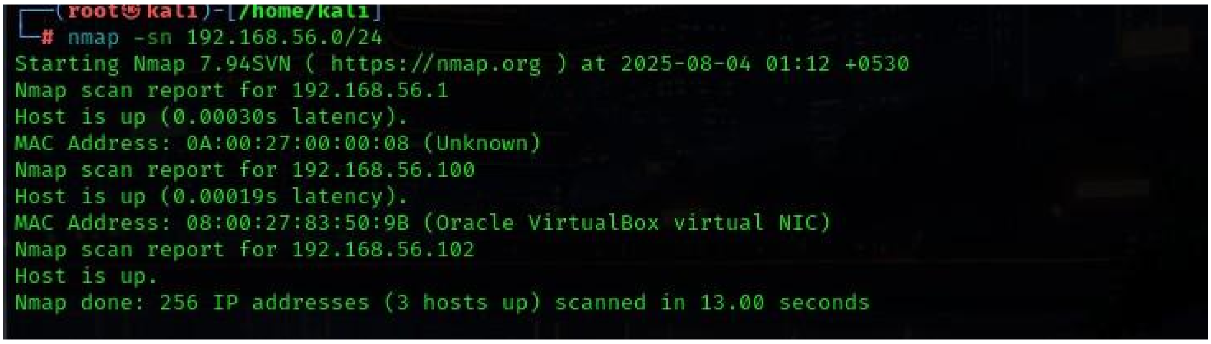
Fin scan – similar to null scan but instead of empty packets fin flags are contained



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sX -Pn 10.201.44.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 00:42 +0530
Nmap scan report for 10.201.44.151
Host is up.
All 1000 scanned ports on 10.201.44.151 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 206.90 seconds

┌──(root㉿kali)-[/home/kali]
```

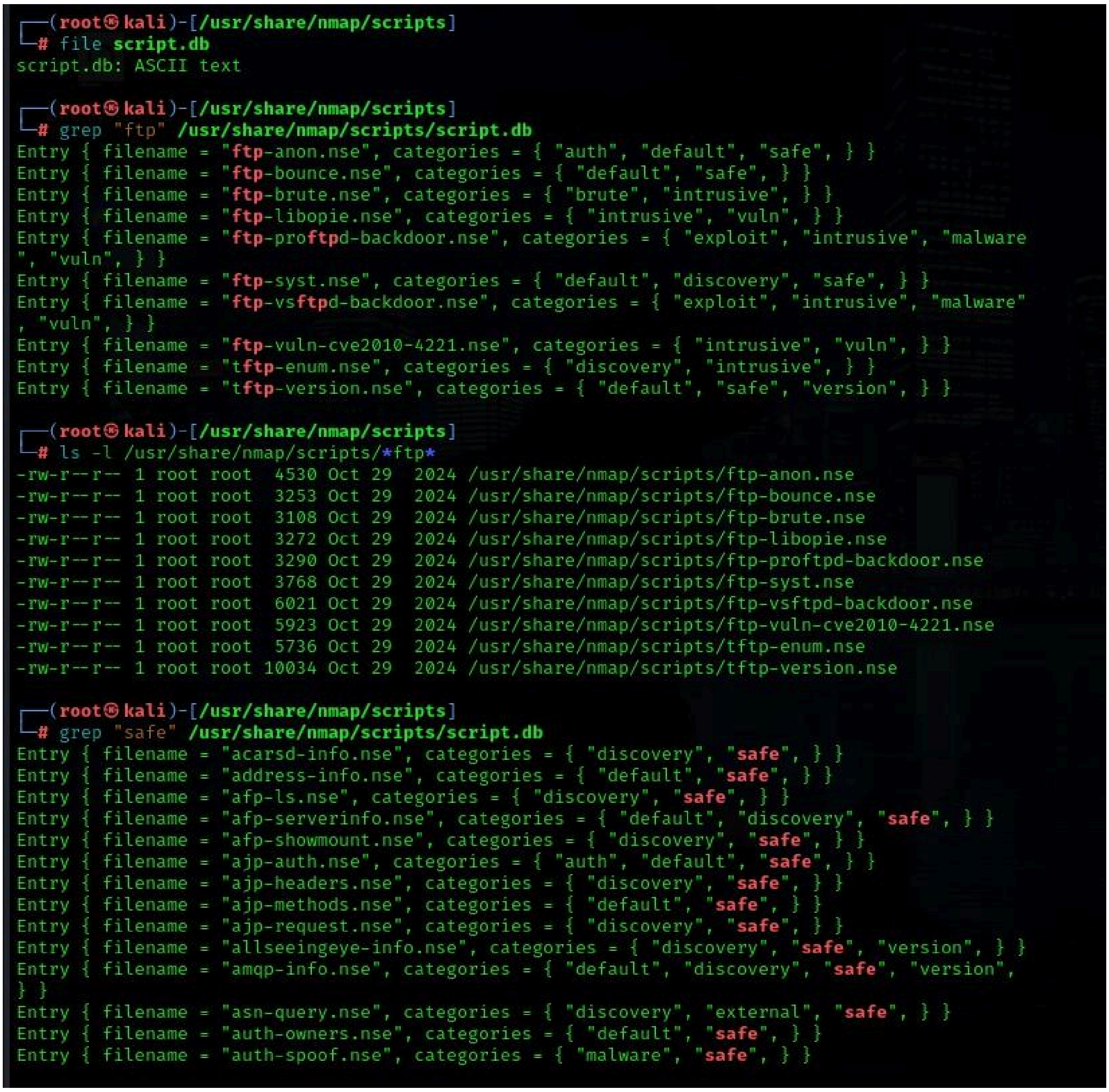
Xmas scan - malformed tcp packets and expect a reply for closed ports

Report on Nmap–Muhammed Nidal



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 01:12 +0530
Nmap scan report for 192.168.56.1
Host is up (0.00030s latency).
MAC Address: 0A:00:27:00:00:08 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00019s latency).
MAC Address: 08:00:27:83:50:9B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 13.00 seconds
```

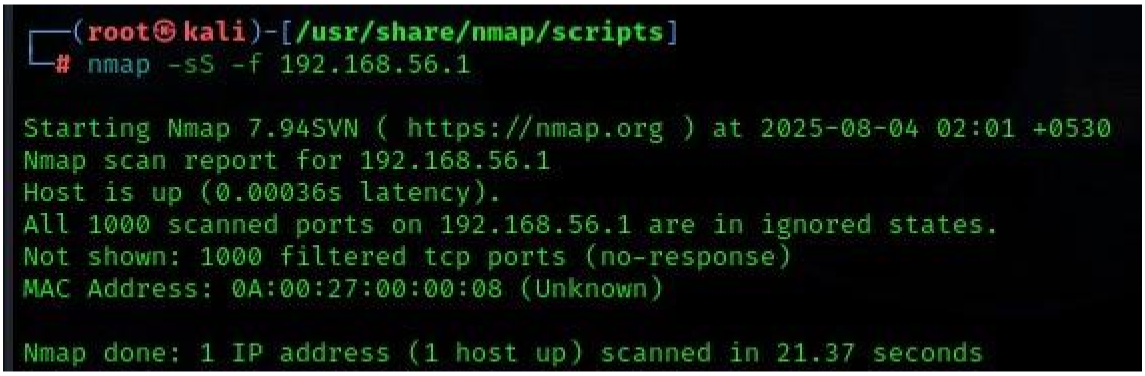
Ping Sweep on my network done and i was able to see the host up with their MAC



```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# file script.db
script.db: ASCII text

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# grep "ftp" /usr/share/nmap/scripts/script.db
Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ftp-bounce.nse", categories = { "default", "safe", } }
Entry { filename = "ftp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ftp-libopie.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "ftp-proftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware
", "vuln", } }
Entry { filename = "ftp-syst.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "ftp-vsftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware"
, "vuln", } }
Entry { filename = "ftp-vuln-cve2010-4221.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "tftp-enum.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "tftp-version.nse", categories = { "default", "safe", "version", } }

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls -l /usr/share/nmap/scripts/*ftp*
-rw-r--r-- 1 root root  4530 Oct 29  2024 /usr/share/nmap/scripts/ftp-anon.nse
-rw-r--r-- 1 root root  3253 Oct 29  2024 /usr/share/nmap/scripts/ftp-bounce.nse
-rw-r--r-- 1 root root  3108 Oct 29  2024 /usr/share/nmap/scripts/ftp-brute.nse
-rw-r--r-- 1 root root  3272 Oct 29  2024 /usr/share/nmap/scripts/ftp-libopie.nse
-rw-r--r-- 1 root root  3290 Oct 29  2024 /usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 Oct 29  2024 /usr/share/nmap/scripts/ftp-syst.nse
-rw-r--r-- 1 root root  6021 Oct 29  2024 /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 Oct 29  2024 /usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 Oct 29  2024 /usr/share/nmap/scripts/tftp-enum.nse
-rw-r--r-- 1 root root 10034 Oct 29  2024 /usr/share/nmap/scripts/tftp-version.nse

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# grep "safe" /usr/share/nmap/scripts/script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "amqp-info.nse", categories = { "default", "discovery", "safe", "version",
} }
Entry { filename = "asn-query.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "auth-owners.nse", categories = { "default", "safe", } }
Entry { filename = "auth-spoof.nse", categories = { "malware", "safe", } }
```

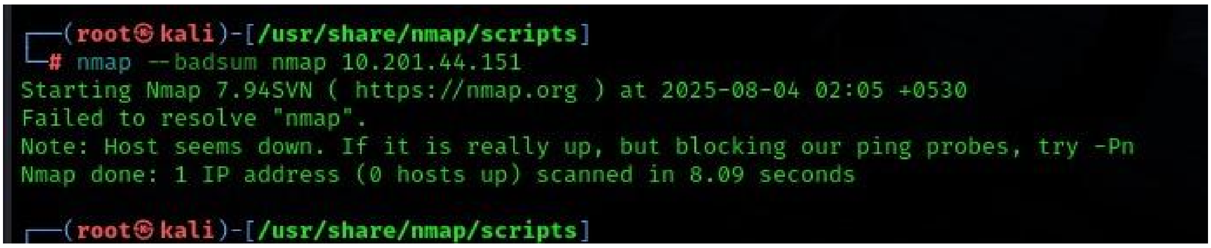
Nse scripts in Nmap directory listing of files and directories actively used for reconnaissance

Report on Nmap–Muhammed Nidal



```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sS -f 192.168.56.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 02:01 +0530
Nmap scan report for 192.168.56.1
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds
```

-f used to fragment the packets as some old firewalls are not able to merge the splitted fragments



```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap --badsum nmap 10.201.44.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 02:05 +0530
Failed to resolve "nmap".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 8.09 seconds

┌──(root㉿kali)-[/usr/share/nmap/scripts]
```

Presence of firewall can be checked using check sum