Project: Vuln PenTest AUPP

Student

Name: TONG Panhavisal

ID: S35

Introduction

4PenTest_Final.sh

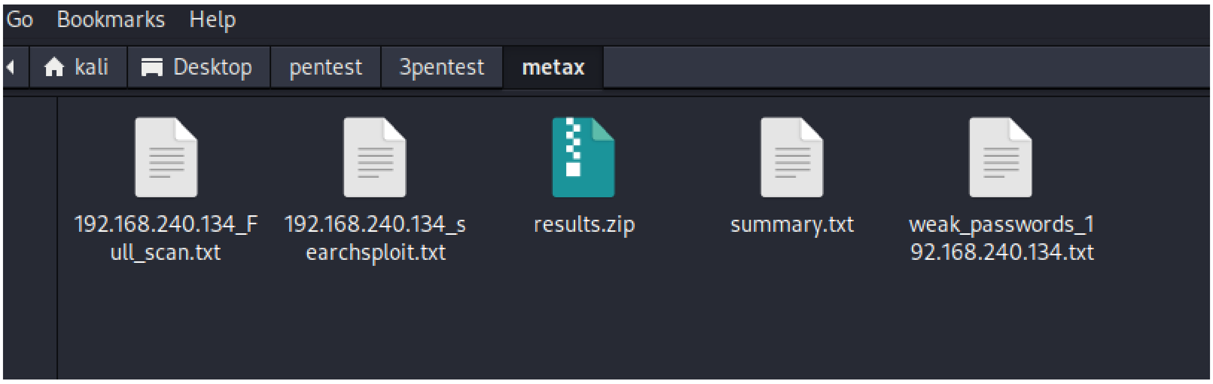
Script come with 2 others default file for user list and default password list .

userlist.txt

def_pass.txt

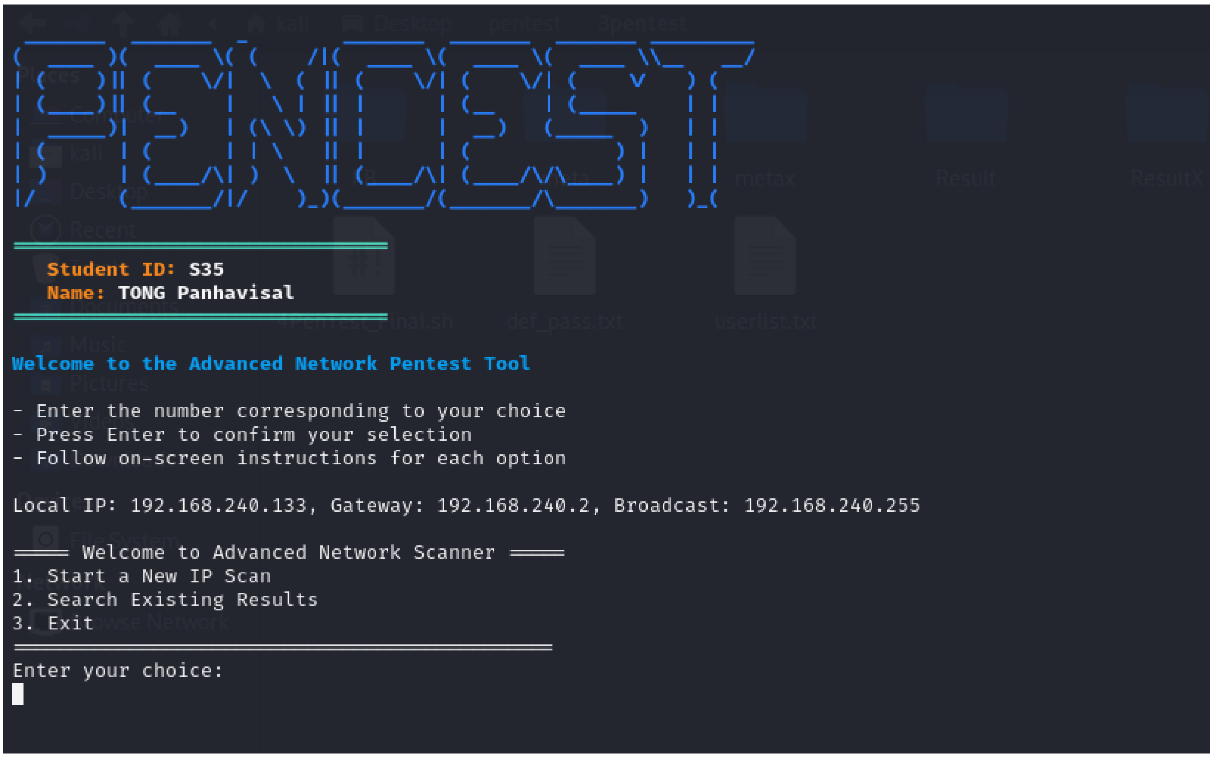
Sample Output File

File(s) by amount of found IP and auto zip the result. The password is auto attack, if found the weak password it will logged into another file for weak password with the machine IP.


Go
Bookmarks
Help
kali
Desktop
pentest
3pentest
metax
192.168.240.134_Full_scan.txt
192.168.240.134_searchsploit.txt
results.zip
summary.txt
weak_passwords_192.168.240.134.txt

Menu

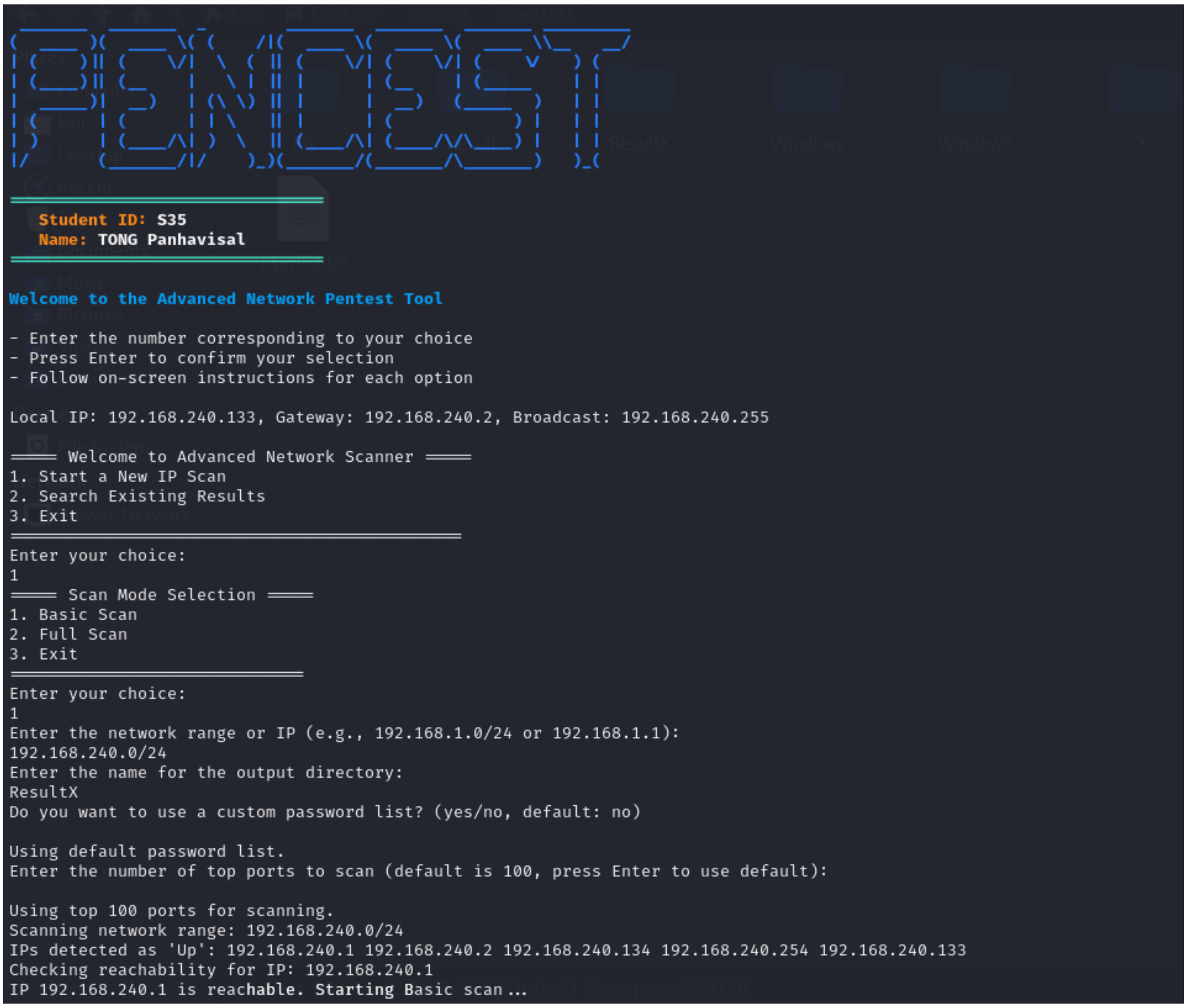
Friendly GUI for user to input.



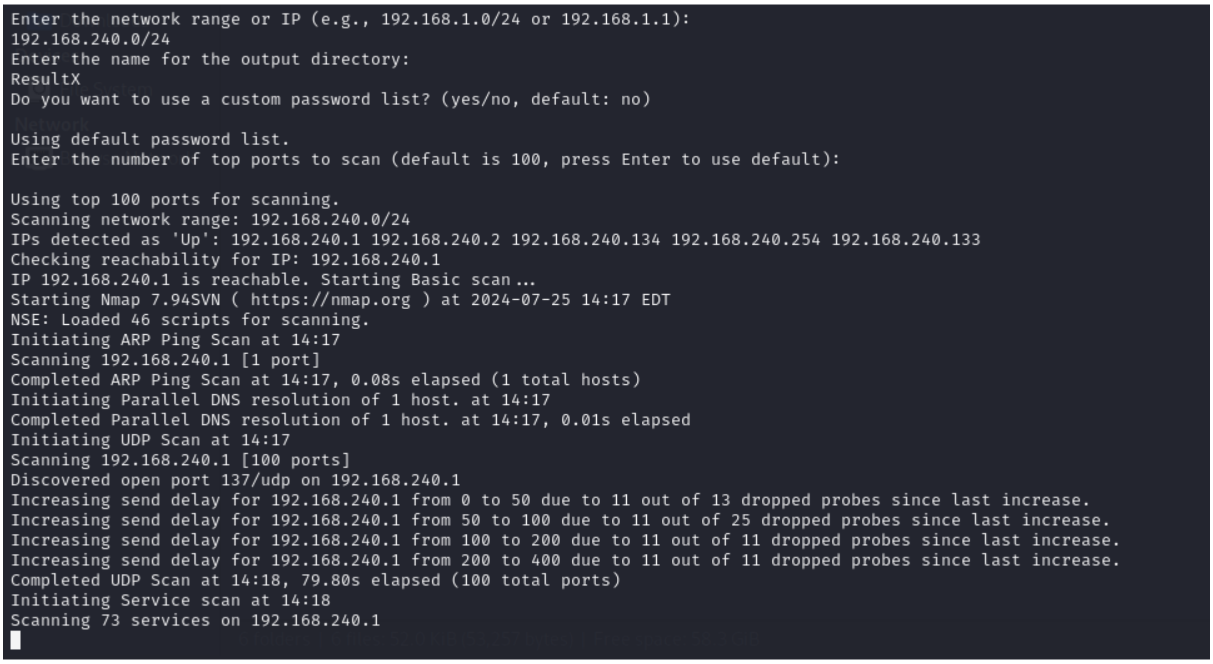
```
 _______  _______  _        _______  _______  _______ _________
(  ____ )(  ____ \( (    /|(  ____ \(  ____ \(  ____ \\__   __/
| (    )|| (    \/|  \  ( || (    \/| (    \/| (    \/   ) (   
| (____)|| (__    |   \ | || |      | (__    | (_____    | |   
|  _____)|  __)   | (\ \) || |      |  __)   (_____  )   | |   
| (      | (      | | \   || |      | (            ) |   | |   
| )      | (____/\| )  \  || (____/\| (____/\/\____) |   | |   
|/       (_______/|/    )_)(_______/(_______/\_______)   )_(   

════════════════════════════════
   Student ID: S35
   Name: TONG Panhavisal
════════════════════════════════

Welcome to the Advanced Network Pentest Tool

- Enter the number corresponding to your choice
- Press Enter to confirm your selection
- Follow on-screen instructions for each option

Local IP: 192.168.240.133, Gateway: 192.168.240.2, Broadcast: 192.168.240.255

════ Welcome to Advanced Network Scanner ════
1. Start a New IP Scan
2. Search Existing Results
3. Exit
══════════════════════════════════════════════

Enter your choice:
█
```

Basic Scan

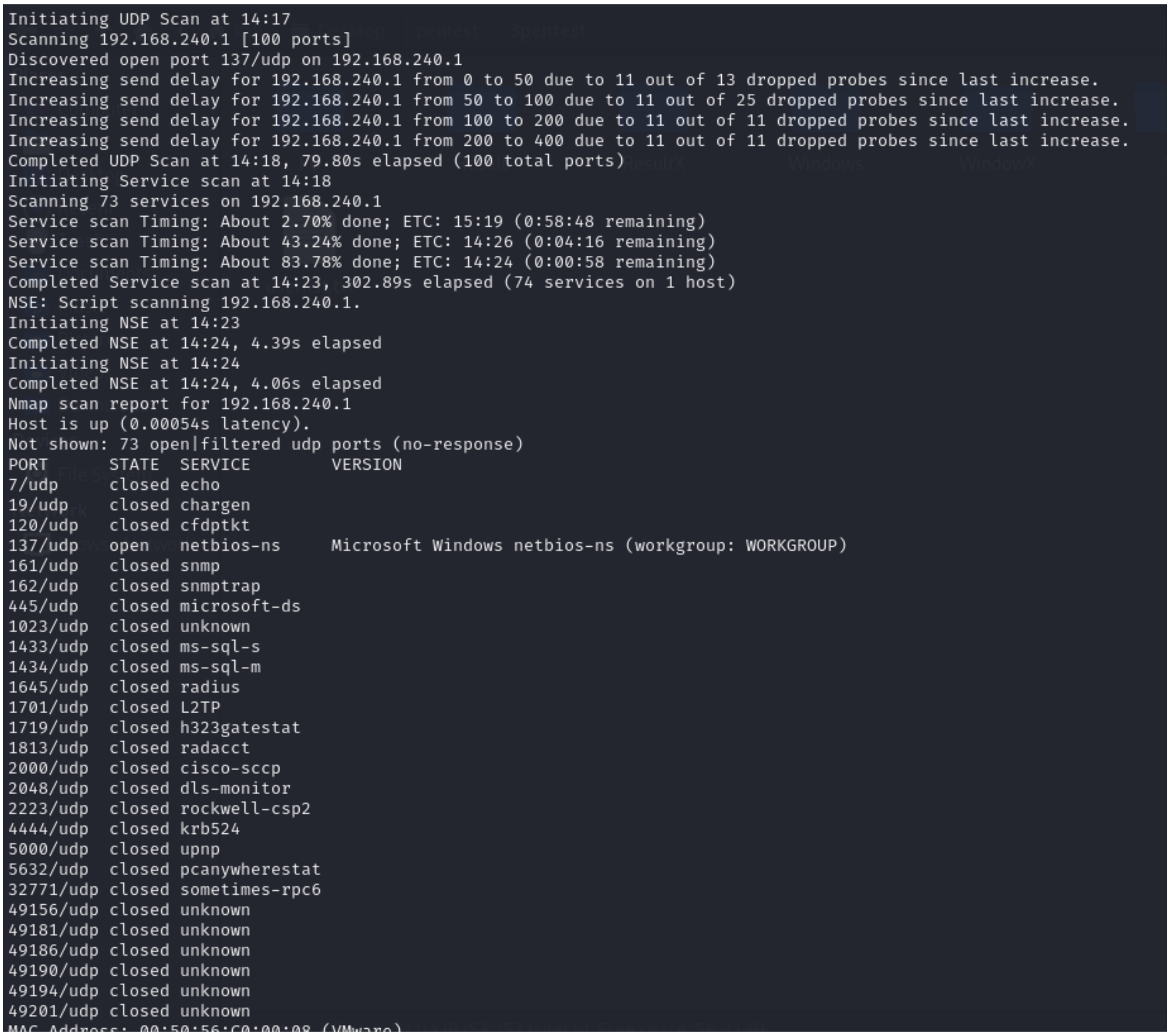
IP Range Scan, Port range is the amount of number the most common Port.



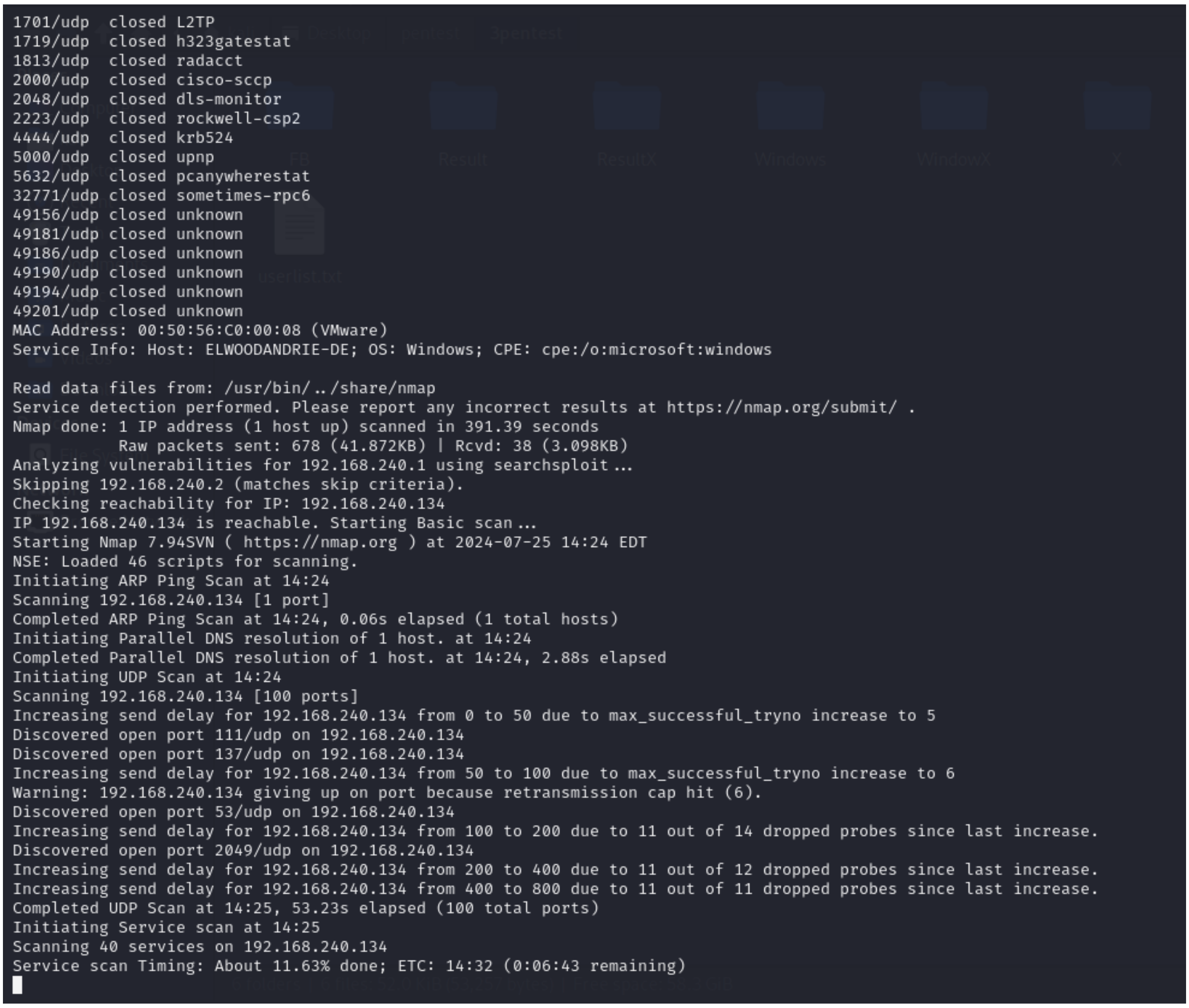
```
 _______  _______  _        _______  _______  _______ _________
(  ____ )(  ____ \( (    /|(  ____ \(  ____ \(  ____ \\__   __/
| (    )|| (    \/|  \  ( || (    \/| (    \/| (    \/   ) (
| (____)|| (__    |   \ | || |      | (__    | (_____    | |
|  _____)|  __)   | (\ \) || |      |  __)   (_____  )   | |
| (      | (      | | \   || |      | (            ) |   | |
| )      | (____/\| )  \  || (____/\| (____/\/\____) |   | |
|/       (_______/|/    )_)(_______/(_______/\_______)   )_(

════════════════════════════════
   Student ID: S35
   Name: TONG Panhavisal
════════════════════════════════

Welcome to the Advanced Network Pentest Tool

- Enter the number corresponding to your choice
- Press Enter to confirm your selection
- Follow on-screen instructions for each option

Local IP: 192.168.240.133, Gateway: 192.168.240.2, Broadcast: 192.168.240.255

═════ Welcome to Advanced Network Scanner ═════
1. Start a New IP Scan
2. Search Existing Results
3. Exit
══════════════════════════════════════════════
Enter your choice:
1
═════ Scan Mode Selection ═════
1. Basic Scan
2. Full Scan
3. Exit
══════════════════════════════
Enter your choice:
1
Enter the network range or IP (e.g., 192.168.1.0/24 or 192.168.1.1):
192.168.240.0/24
Enter the name for the output directory:
ResultX
Do you want to use a custom password list? (yes/no, default: no)

Using default password list.
Enter the number of top ports to scan (default is 100, press Enter to use default):

Using top 100 ports for scanning.
Scanning network range: 192.168.240.0/24
IPs detected as 'Up': 192.168.240.1 192.168.240.2 192.168.240.134 192.168.240.254 192.168.240.133
Checking reachability for IP: 192.168.240.1
IP 192.168.240.1 is reachable. Starting Basic scan...
```



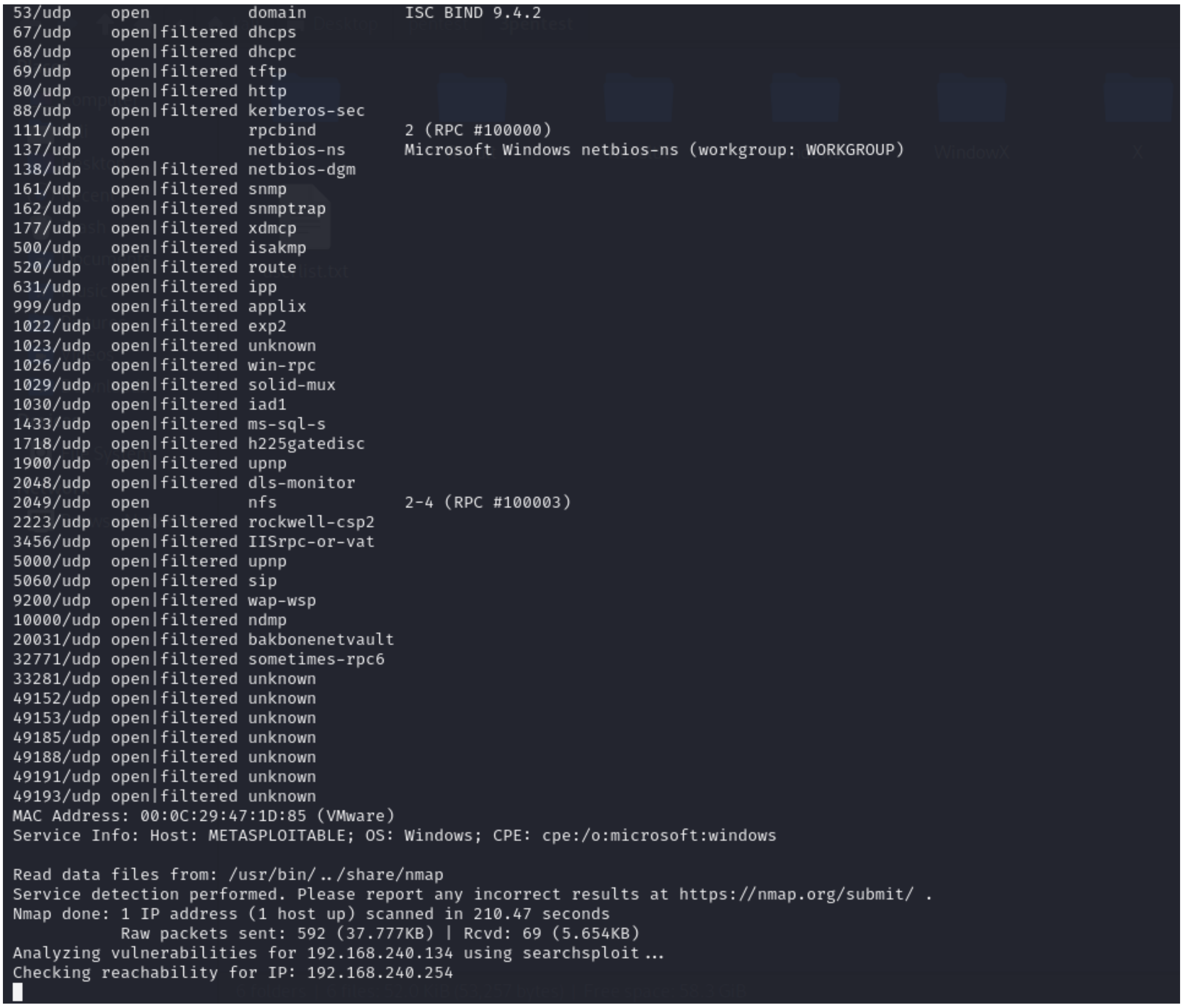
```
Enter the network range or IP (e.g., 192.168.1.0/24 or 192.168.1.1):
192.168.240.0/24
Enter the name for the output directory:
ResultX
Do you want to use a custom password list? (yes/no, default: no)

Using default password list.
Enter the number of top ports to scan (default is 100, press Enter to use default):

Using top 100 ports for scanning.
Scanning network range: 192.168.240.0/24
IPs detected as 'Up': 192.168.240.1 192.168.240.2 192.168.240.134 192.168.240.254 192.168.240.133
Checking reachability for IP: 192.168.240.1
IP 192.168.240.1 is reachable. Starting Basic scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 14:17 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 14:17
Scanning 192.168.240.1 [1 port]
Completed ARP Ping Scan at 14:17, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:17
Completed Parallel DNS resolution of 1 host. at 14:17, 0.01s elapsed
Initiating UDP Scan at 14:17
Scanning 192.168.240.1 [100 ports]
Discovered open port 137/udp on 192.168.240.1
Increasing send delay for 192.168.240.1 from 0 to 50 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 192.168.240.1 from 50 to 100 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 192.168.240.1 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.240.1 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
Completed UDP Scan at 14:18, 79.80s elapsed (100 total ports)
Initiating Service scan at 14:18
Scanning 73 services on 192.168.240.1
█
```



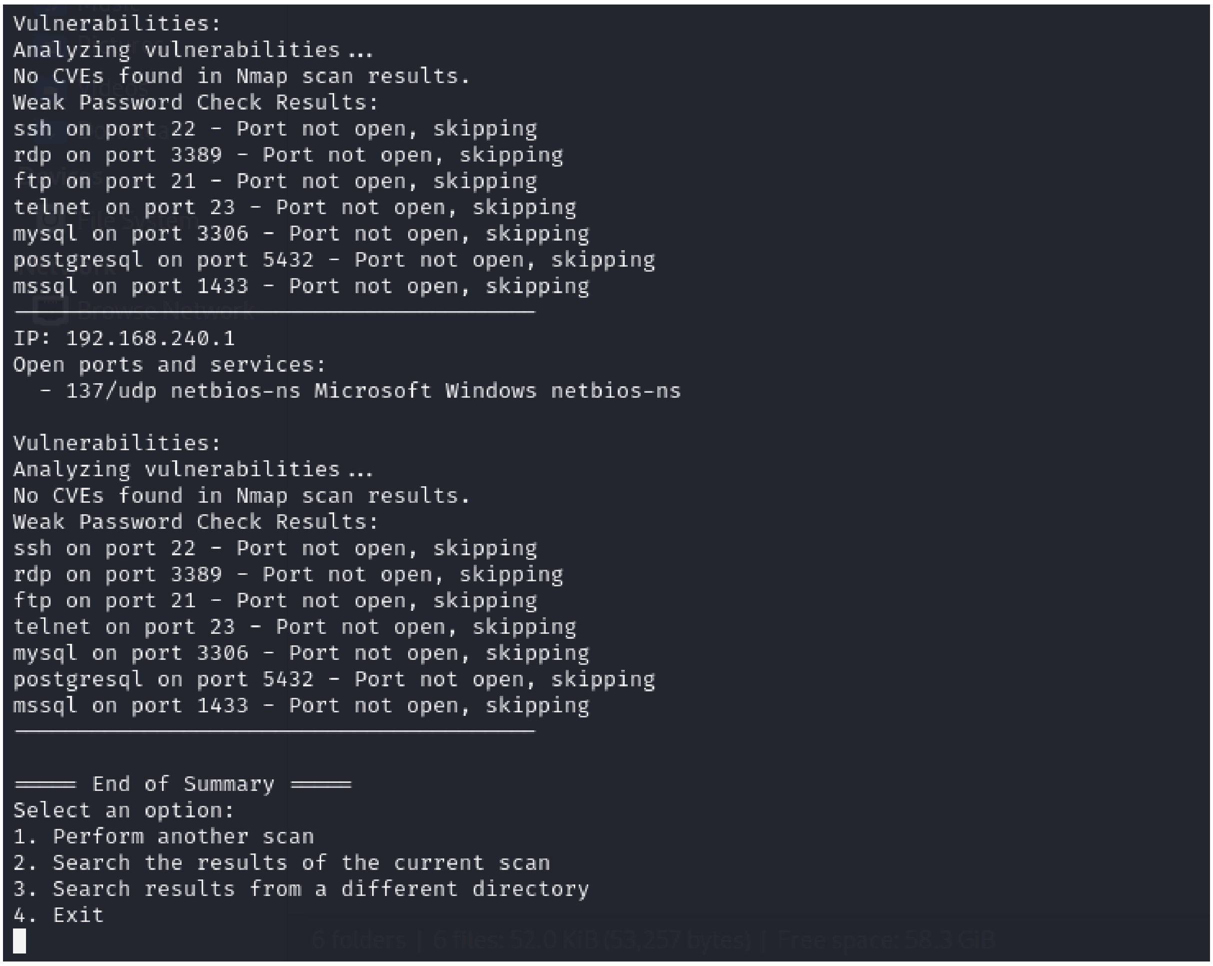
```
Initiating UDP Scan at 14:17
Scanning 192.168.240.1 [100 ports]
Discovered open port 137/udp on 192.168.240.1
Increasing send delay for 192.168.240.1 from 0 to 50 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 192.168.240.1 from 50 to 100 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 192.168.240.1 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.240.1 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
Completed UDP Scan at 14:18, 79.80s elapsed (100 total ports)
Initiating Service scan at 14:18
Scanning 73 services on 192.168.240.1
Service scan Timing: About 2.70% done; ETC: 15:19 (0:58:48 remaining)
Service scan Timing: About 43.24% done; ETC: 14:26 (0:04:16 remaining)
Service scan Timing: About 83.78% done; ETC: 14:24 (0:00:58 remaining)
Completed Service scan at 14:23, 302.89s elapsed (74 services on 1 host)
NSE: Script scanning 192.168.240.1.
Initiating NSE at 14:23
Completed NSE at 14:24, 4.39s elapsed
Initiating NSE at 14:24
Completed NSE at 14:24, 4.06s elapsed
Nmap scan report for 192.168.240.1
Host is up (0.00054s latency).
Not shown: 73 open|filtered udp ports (no-response)
PORT      STATE  SERVICE        VERSION
7/udp     closed echo
19/udp    closed chargen
120/udp   closed cfdptkt
137/udp   open   netbios-ns     Microsoft Windows netbios-ns (workgroup: WORKGROUP)
161/udp   closed snmp
162/udp   closed snmptrap
445/udp   closed microsoft-ds
1023/udp  closed unknown
1433/udp  closed ms-sql-s
1434/udp  closed ms-sql-m
1645/udp  closed radius
1701/udp  closed L2TP
1719/udp  closed h323gatestat
1813/udp  closed radacct
2000/udp  closed cisco-sccp
2048/udp  closed dls-monitor
2223/udp  closed rockwell-csp2
4444/udp  closed krb524
5000/udp  closed upnp
5632/udp  closed pcanywherestat
32771/udp closed sometimes-rpc6
49156/udp closed unknown
49181/udp closed unknown
49186/udp closed unknown
49190/udp closed unknown
49194/udp closed unknown
49201/udp closed unknown
MAC Address: 00:50:56:C0:00:08 (VMware)
```



```
1701/udp  closed L2TP
1719/udp  closed h323gatestat
1813/udp  closed radacct
2000/udp  closed cisco-sccp
2048/udp  closed dls-monitor
2223/udp  closed rockwell-csp2
4444/udp  closed krb524
5000/udp  closed upnp
5632/udp  closed pcanywherestat
32771/udp closed sometimes-rpc6
49156/udp closed unknown
49181/udp closed unknown
49186/udp closed unknown
49190/udp closed unknown
49194/udp closed unknown
49201/udp closed unknown
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: Host: ELWOODANDRIE-DE; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 391.39 seconds
           Raw packets sent: 678 (41.872KB) | Rcvd: 38 (3.098KB)
Analyzing vulnerabilities for 192.168.240.1 using searchsploit...
Skipping 192.168.240.2 (matches skip criteria).
Checking reachability for IP: 192.168.240.134
IP 192.168.240.134 is reachable. Starting Basic scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 14:24 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 14:24
Scanning 192.168.240.134 [1 port]
Completed ARP Ping Scan at 14:24, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:24
Completed Parallel DNS resolution of 1 host. at 14:24, 2.88s elapsed
Initiating UDP Scan at 14:24
Scanning 192.168.240.134 [100 ports]
Increasing send delay for 192.168.240.134 from 0 to 50 due to max_successful_tryno increase to 5
Discovered open port 111/udp on 192.168.240.134
Discovered open port 137/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 50 to 100 due to max_successful_tryno increase to 6
Warning: 192.168.240.134 giving up on port because retransmission cap hit (6).
Discovered open port 53/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 100 to 200 due to 11 out of 14 dropped probes since last increase.
Discovered open port 2049/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 200 to 400 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 192.168.240.134 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
Completed UDP Scan at 14:25, 53.23s elapsed (100 total ports)
Initiating Service scan at 14:25
Scanning 40 services on 192.168.240.134
Service scan Timing: About 11.63% done; ETC: 14:32 (0:06:43 remaining)
█
```

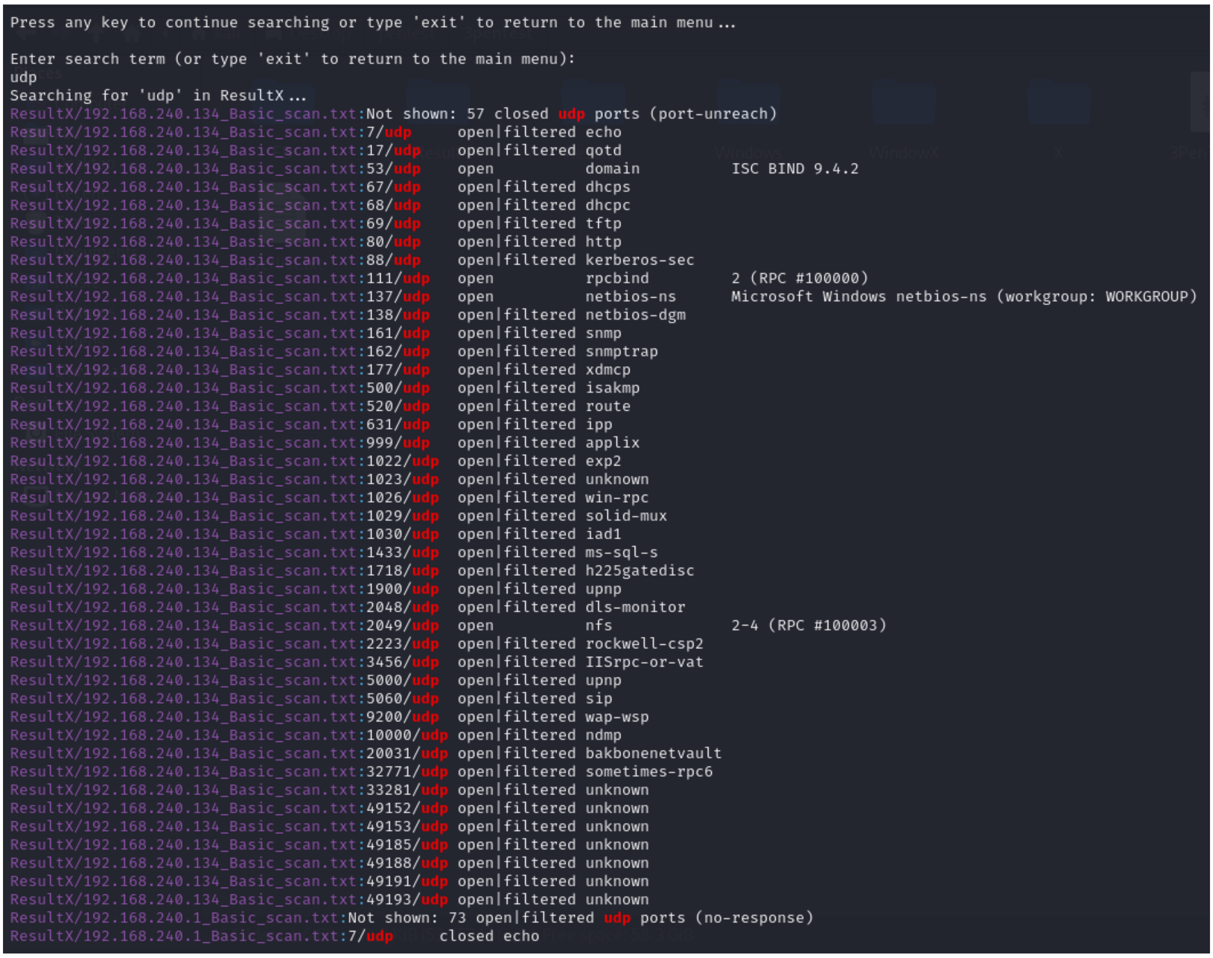


```
53/udp    open          domain          ISC BIND 9.4.2
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
80/udp    open|filtered http
88/udp    open|filtered kerberos-sec
111/udp   open          rpcbind         2 (RPC #100000)
137/udp   open          netbios-ns      Microsoft Windows netbios-ns (workgroup: WORKGROUP)
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
177/udp   open|filtered xdmcp
500/udp   open|filtered isakmp
520/udp   open|filtered route
631/udp   open|filtered ipp
999/udp   open|filtered applix
1022/udp  open|filtered exp2
1023/udp  open|filtered unknown
1026/udp  open|filtered win-rpc
1029/udp  open|filtered solid-mux
1030/udp  open|filtered iad1
1433/udp  open|filtered ms-sql-s
1718/udp  open|filtered h225gatedisc
1900/udp  open|filtered upnp
2048/udp  open|filtered dls-monitor
2049/udp  open          nfs             2-4 (RPC #100003)
2223/udp  open|filtered rockwell-csp2
3456/udp  open|filtered IISrpc-or-vat
5000/udp  open|filtered upnp
5060/udp  open|filtered sip
9200/udp  open|filtered wap-wsp
10000/udp open|filtered ndmp
20031/udp open|filtered bakbonenetvault
32771/udp open|filtered sometimes-rpc6
33281/udp open|filtered unknown
49152/udp open|filtered unknown
49153/udp open|filtered unknown
49185/udp open|filtered unknown
49188/udp open|filtered unknown
49191/udp open|filtered unknown
49193/udp open|filtered unknown
MAC Address: 00:0C:29:47:1D:85 (VMware)
Service Info: Host: METASPLOITABLE; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.47 seconds
           Raw packets sent: 592 (37.777KB) | Rcvd: 69 (5.654KB)
Analyzing vulnerabilities for 192.168.240.134 using searchsploit...
Checking reachability for IP: 192.168.240.254
```



```
Vulnerabilities:
Analyzing vulnerabilities...
No CVEs found in Nmap scan results.
Weak Password Check Results:
ssh on port 22 - Port not open, skipping
rdp on port 3389 - Port not open, skipping
ftp on port 21 - Port not open, skipping
telnet on port 23 - Port not open, skipping
mysql on port 3306 - Port not open, skipping
postgresql on port 5432 - Port not open, skipping
mssql on port 1433 - Port not open, skipping
────────────────────────────────────────
IP: 192.168.240.1
Open ports and services:
  - 137/udp netbios-ns Microsoft Windows netbios-ns

Vulnerabilities:
Analyzing vulnerabilities...
No CVEs found in Nmap scan results.
Weak Password Check Results:
ssh on port 22 - Port not open, skipping
rdp on port 3389 - Port not open, skipping
ftp on port 21 - Port not open, skipping
telnet on port 23 - Port not open, skipping
mysql on port 3306 - Port not open, skipping
postgresql on port 5432 - Port not open, skipping
mssql on port 1433 - Port not open, skipping
────────────────────────────────────────

═════ End of Summary ═════
Select an option:
1. Perform another scan
2. Search the results of the current scan
3. Search results from a different directory
4. Exit
█
```

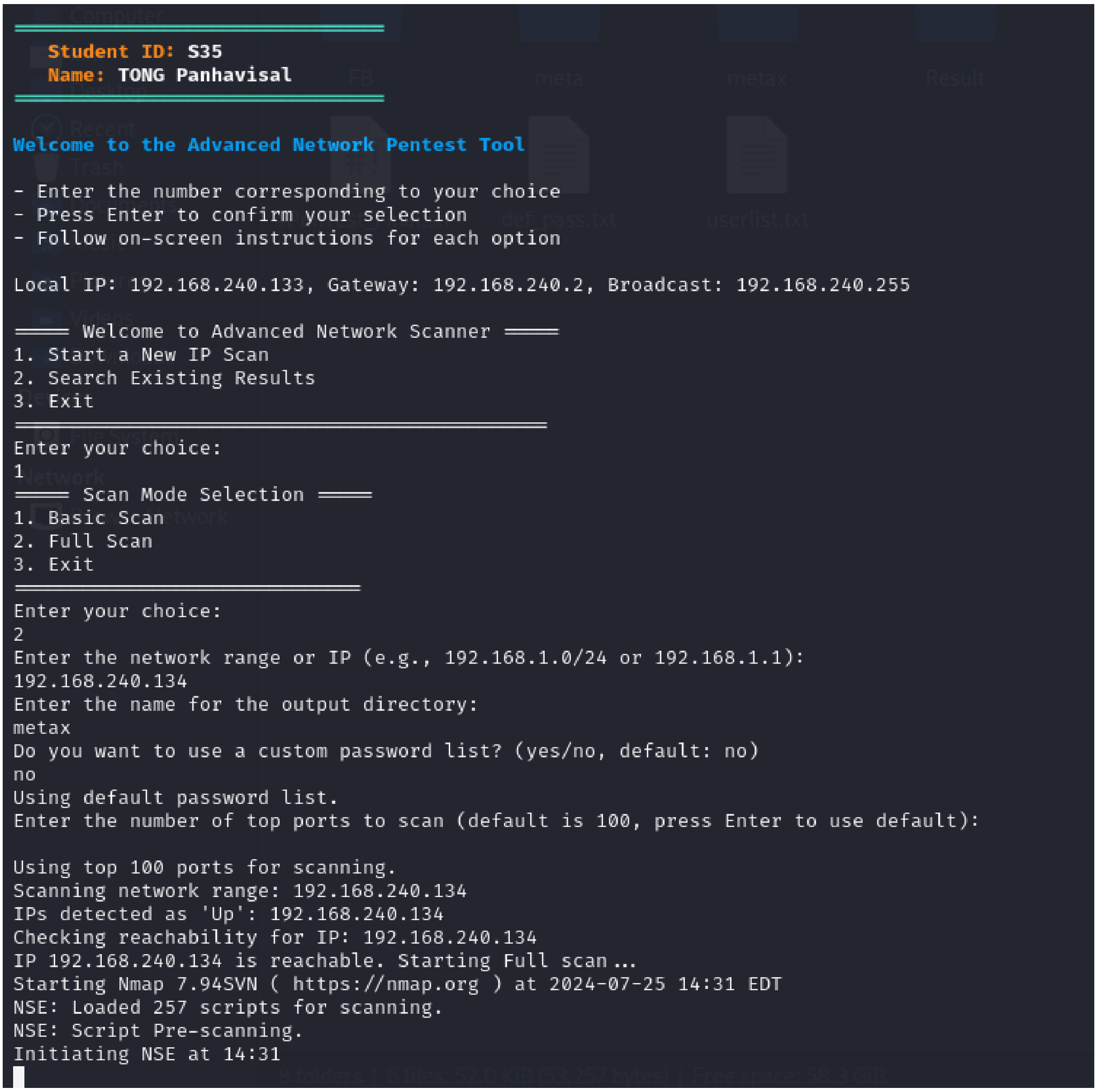
Search Result



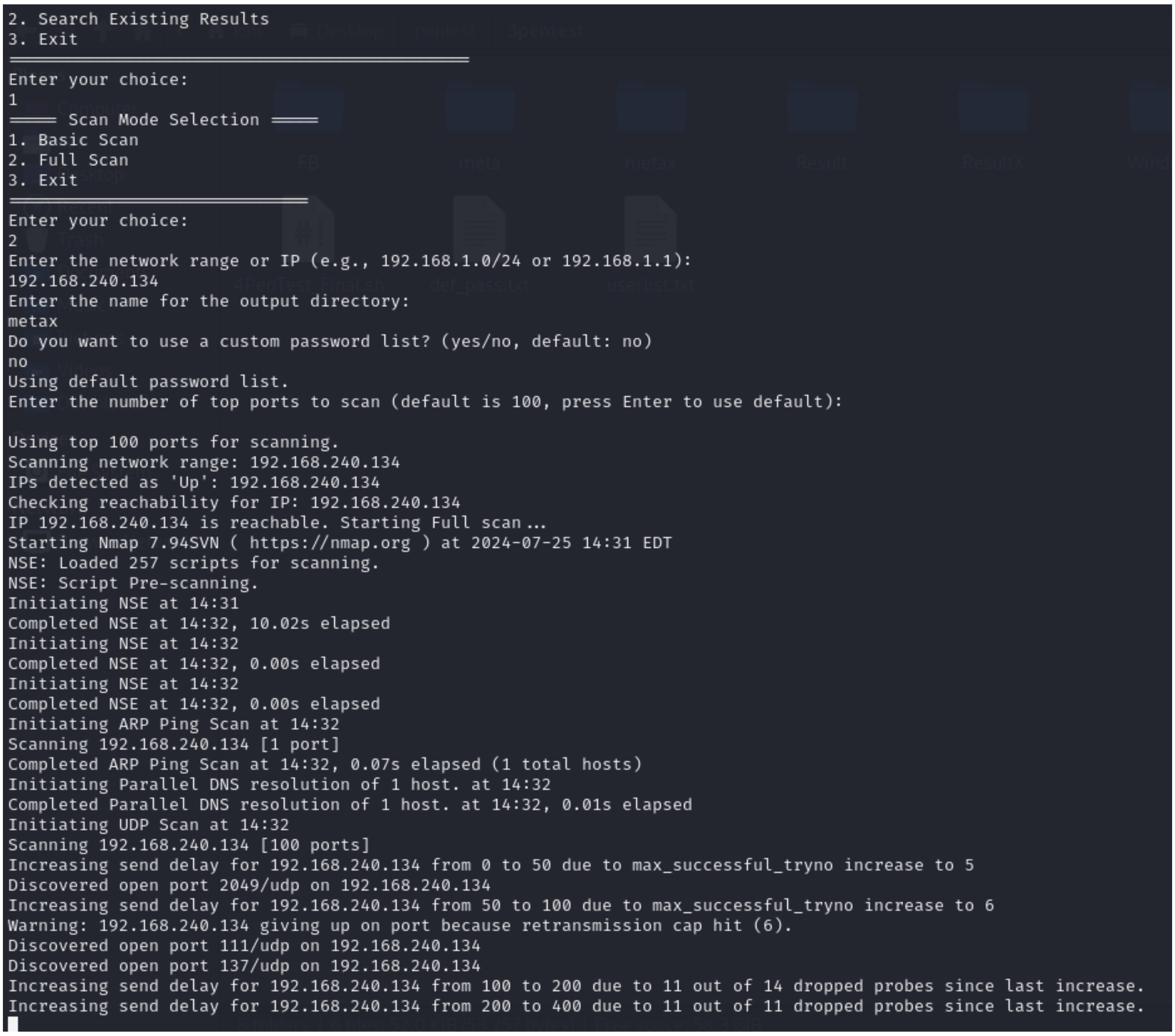
```
Press any key to continue searching or type 'exit' to return to the main menu...

Enter search term (or type 'exit' to return to the main menu):
udp
Searching for 'udp' in ResultX...
ResultX/192.168.240.134_Basic_scan.txt:Not shown: 57 closed udp ports (port-unreach)
ResultX/192.168.240.134_Basic_scan.txt:7/udp     open|filtered echo
ResultX/192.168.240.134_Basic_scan.txt:17/udp    open|filtered qotd
ResultX/192.168.240.134_Basic_scan.txt:53/udp    open          domain          ISC BIND 9.4.2
ResultX/192.168.240.134_Basic_scan.txt:67/udp    open|filtered dhcps
ResultX/192.168.240.134_Basic_scan.txt:68/udp    open|filtered dhcpc
ResultX/192.168.240.134_Basic_scan.txt:69/udp    open|filtered tftp
ResultX/192.168.240.134_Basic_scan.txt:80/udp    open|filtered http
ResultX/192.168.240.134_Basic_scan.txt:88/udp    open|filtered kerberos-sec
ResultX/192.168.240.134_Basic_scan.txt:111/udp   open          rpcbind         2 (RPC #100000)
ResultX/192.168.240.134_Basic_scan.txt:137/udp   open          netbios-ns      Microsoft Windows netbios-ns (workgroup: WORKGROUP)
ResultX/192.168.240.134_Basic_scan.txt:138/udp   open|filtered netbios-dgm
ResultX/192.168.240.134_Basic_scan.txt:161/udp   open|filtered snmp
ResultX/192.168.240.134_Basic_scan.txt:162/udp   open|filtered snmptrap
ResultX/192.168.240.134_Basic_scan.txt:177/udp   open|filtered xdmcp
ResultX/192.168.240.134_Basic_scan.txt:500/udp   open|filtered isakmp
ResultX/192.168.240.134_Basic_scan.txt:520/udp   open|filtered route
ResultX/192.168.240.134_Basic_scan.txt:631/udp   open|filtered ipp
ResultX/192.168.240.134_Basic_scan.txt:999/udp   open|filtered applix
ResultX/192.168.240.134_Basic_scan.txt:1022/udp  open|filtered exp2
ResultX/192.168.240.134_Basic_scan.txt:1023/udp  open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:1026/udp  open|filtered win-rpc
ResultX/192.168.240.134_Basic_scan.txt:1029/udp  open|filtered solid-mux
ResultX/192.168.240.134_Basic_scan.txt:1030/udp  open|filtered iad1
ResultX/192.168.240.134_Basic_scan.txt:1433/udp  open|filtered ms-sql-s
ResultX/192.168.240.134_Basic_scan.txt:1718/udp  open|filtered h225gatedisc
ResultX/192.168.240.134_Basic_scan.txt:1900/udp  open|filtered upnp
ResultX/192.168.240.134_Basic_scan.txt:2048/udp  open|filtered dls-monitor
ResultX/192.168.240.134_Basic_scan.txt:2049/udp  open          nfs             2-4 (RPC #100003)
ResultX/192.168.240.134_Basic_scan.txt:2223/udp  open|filtered rockwell-csp2
ResultX/192.168.240.134_Basic_scan.txt:3456/udp  open|filtered IISrpc-or-vat
ResultX/192.168.240.134_Basic_scan.txt:5000/udp  open|filtered upnp
ResultX/192.168.240.134_Basic_scan.txt:5060/udp  open|filtered sip
ResultX/192.168.240.134_Basic_scan.txt:9200/udp  open|filtered wap-wsp
ResultX/192.168.240.134_Basic_scan.txt:10000/udp open|filtered ndmp
ResultX/192.168.240.134_Basic_scan.txt:20031/udp open|filtered bakbonenetvault
ResultX/192.168.240.134_Basic_scan.txt:32771/udp open|filtered sometimes-rpc6
ResultX/192.168.240.134_Basic_scan.txt:33281/udp open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:49152/udp open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:49153/udp open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:49185/udp open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:49188/udp open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:49191/udp open|filtered unknown
ResultX/192.168.240.134_Basic_scan.txt:49193/udp open|filtered unknown
ResultX/192.168.240.1_Basic_scan.txt:Not shown: 73 open|filtered udp ports (no-response)
ResultX/192.168.240.1_Basic_scan.txt:7/udp    closed echo
```

Full Scan

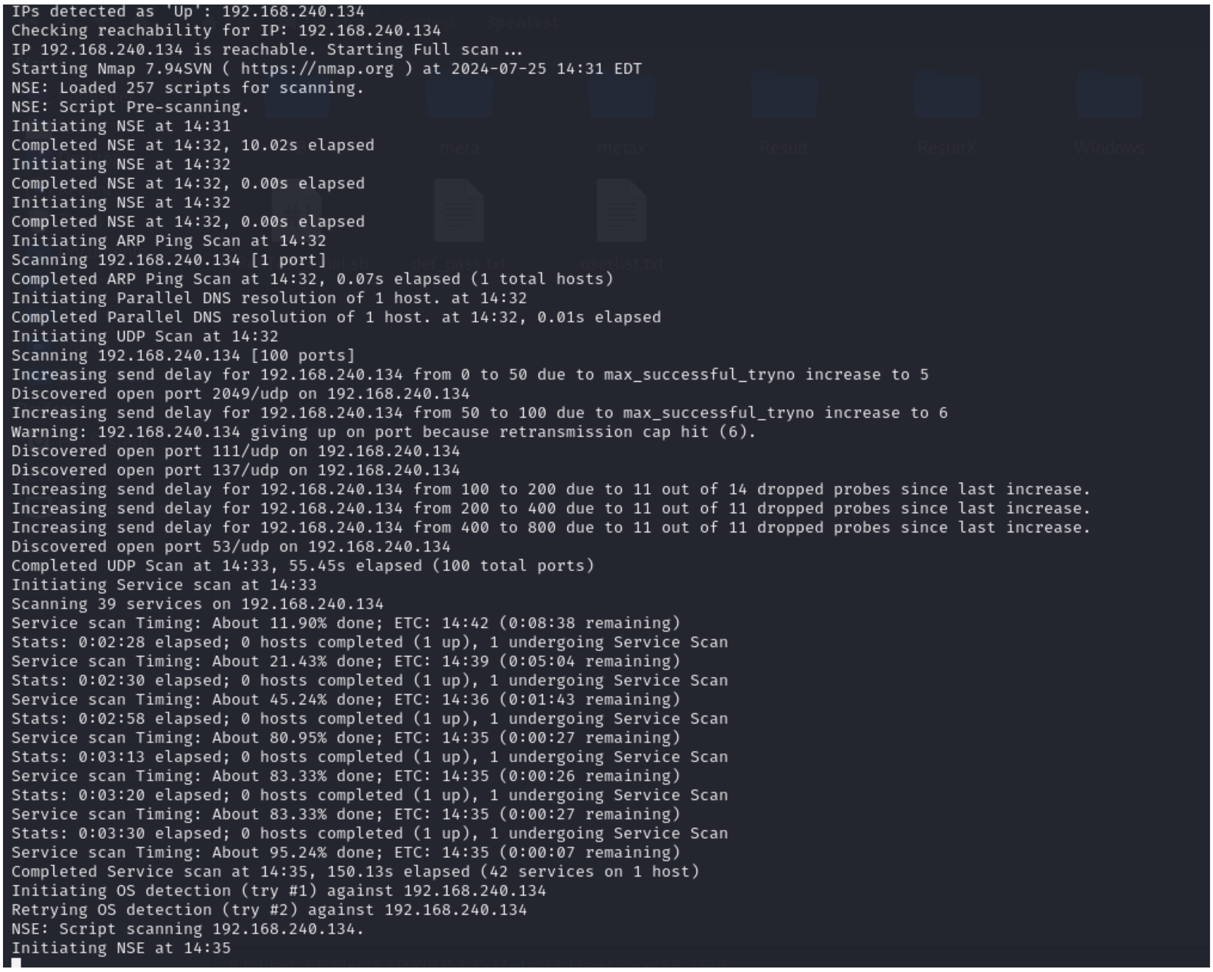
Support both IP and Range Scans. But in this case, I use a direct IP scan for faster results.



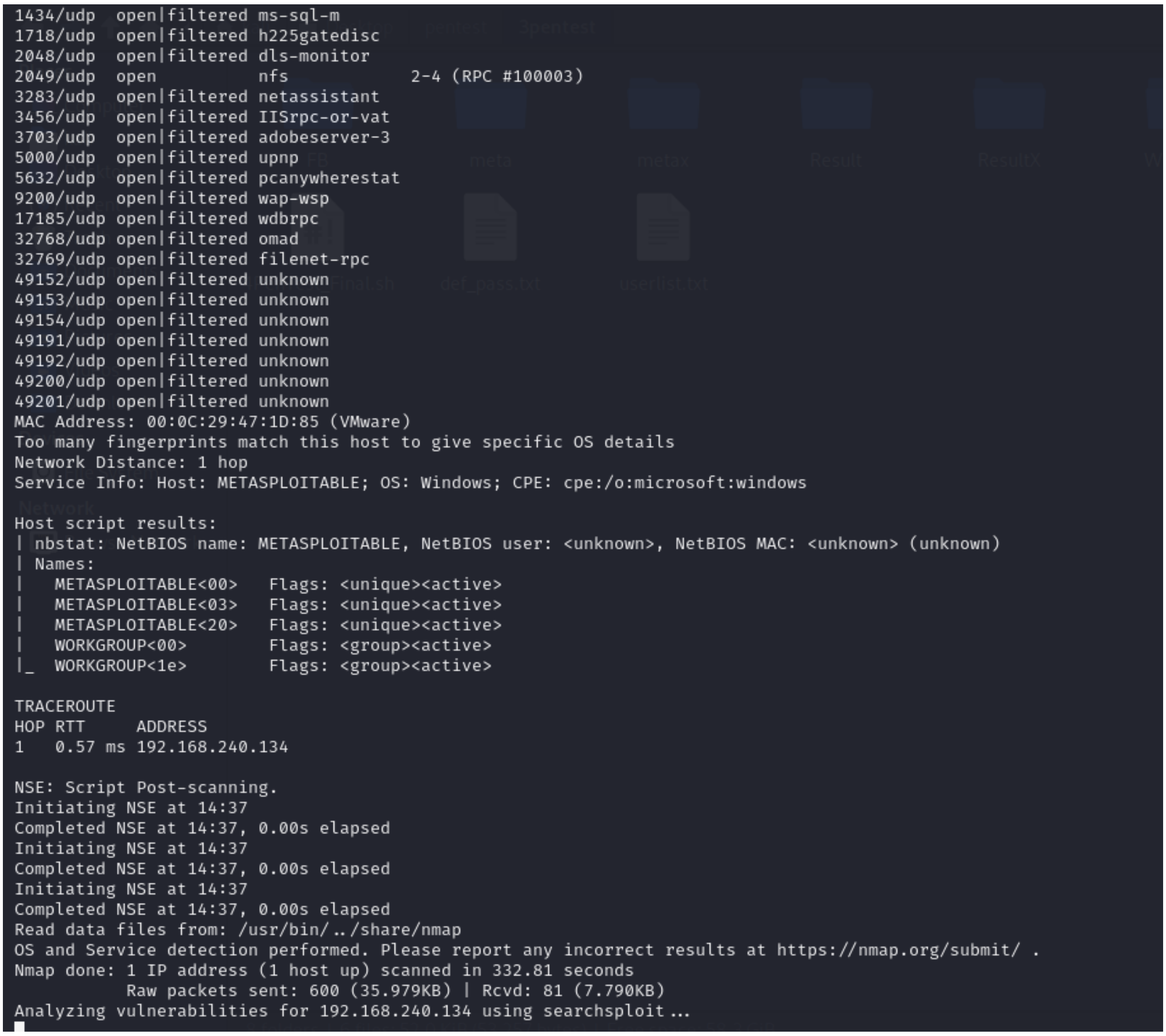
```
════════════════════════════════
   Student ID: S35
   Name: TONG Panhavisal
════════════════════════════════

Welcome to the Advanced Network Pentest Tool

- Enter the number corresponding to your choice
- Press Enter to confirm your selection
- Follow on-screen instructions for each option

Local IP: 192.168.240.133, Gateway: 192.168.240.2, Broadcast: 192.168.240.255

═════ Welcome to Advanced Network Scanner ═════
1. Start a New IP Scan
2. Search Existing Results
3. Exit
══════════════════════════════════════════════
Enter your choice:
1
═════ Scan Mode Selection ═════
1. Basic Scan
2. Full Scan
3. Exit
══════════════════════════════
Enter your choice:
2
Enter the network range or IP (e.g., 192.168.1.0/24 or 192.168.1.1):
192.168.240.134
Enter the name for the output directory:
metax
Do you want to use a custom password list? (yes/no, default: no)
no
Using default password list.
Enter the number of top ports to scan (default is 100, press Enter to use default):

Using top 100 ports for scanning.
Scanning network range: 192.168.240.134
IPs detected as 'Up': 192.168.240.134
Checking reachability for IP: 192.168.240.134
IP 192.168.240.134 is reachable. Starting Full scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 14:31 EDT
NSE: Loaded 257 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:31
```



```
2. Search Existing Results
3. Exit
════════════════════════════════════════
Enter your choice:
1
════ Scan Mode Selection ════
1. Basic Scan
2. Full Scan
3. Exit
══════════════════════════
Enter your choice:
2
Enter the network range or IP (e.g., 192.168.1.0/24 or 192.168.1.1):
192.168.240.134
Enter the name for the output directory:
metax
Do you want to use a custom password list? (yes/no, default: no)
no
Using default password list.
Enter the number of top ports to scan (default is 100, press Enter to use default):

Using top 100 ports for scanning.
Scanning network range: 192.168.240.134
IPs detected as 'Up': 192.168.240.134
Checking reachability for IP: 192.168.240.134
IP 192.168.240.134 is reachable. Starting Full scan ...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 14:31 EDT
NSE: Loaded 257 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:31
Completed NSE at 14:32, 10.02s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating ARP Ping Scan at 14:32
Scanning 192.168.240.134 [1 port]
Completed ARP Ping Scan at 14:32, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:32
Completed Parallel DNS resolution of 1 host. at 14:32, 0.01s elapsed
Initiating UDP Scan at 14:32
Scanning 192.168.240.134 [100 ports]
Increasing send delay for 192.168.240.134 from 0 to 50 due to max_successful_tryno increase to 5
Discovered open port 2049/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 50 to 100 due to max_successful_tryno increase to 6
Warning: 192.168.240.134 giving up on port because retransmission cap hit (6).
Discovered open port 111/udp on 192.168.240.134
Discovered open port 137/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 100 to 200 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 192.168.240.134 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
```

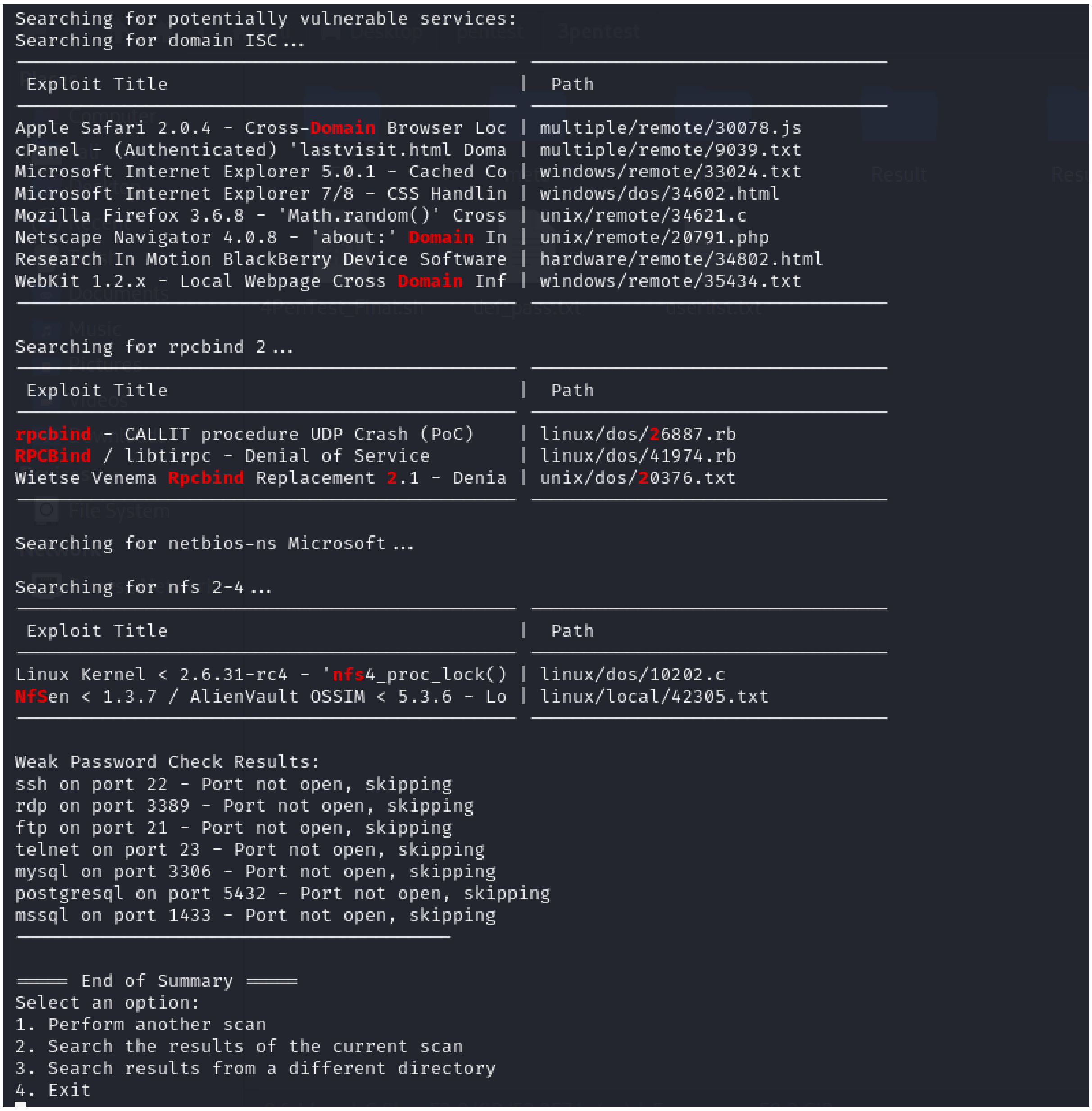


```
IPs detected as 'Up': 192.168.240.134
Checking reachability for IP: 192.168.240.134
IP 192.168.240.134 is reachable. Starting Full scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 14:31 EDT
NSE: Loaded 257 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:31
Completed NSE at 14:32, 10.02s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating ARP Ping Scan at 14:32
Scanning 192.168.240.134 [1 port]
Completed ARP Ping Scan at 14:32, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:32
Completed Parallel DNS resolution of 1 host. at 14:32, 0.01s elapsed
Initiating UDP Scan at 14:32
Scanning 192.168.240.134 [100 ports]
Increasing send delay for 192.168.240.134 from 0 to 50 due to max_successful_tryno increase to 5
Discovered open port 2049/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 50 to 100 due to max_successful_tryno increase to 6
Warning: 192.168.240.134 giving up on port because retransmission cap hit (6).
Discovered open port 111/udp on 192.168.240.134
Discovered open port 137/udp on 192.168.240.134
Increasing send delay for 192.168.240.134 from 100 to 200 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 192.168.240.134 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.240.134 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
Discovered open port 53/udp on 192.168.240.134
Completed UDP Scan at 14:33, 55.45s elapsed (100 total ports)
Initiating Service scan at 14:33
Scanning 39 services on 192.168.240.134
Service scan Timing: About 11.90% done; ETC: 14:42 (0:08:38 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 21.43% done; ETC: 14:39 (0:05:04 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.24% done; ETC: 14:36 (0:01:43 remaining)
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.95% done; ETC: 14:35 (0:00:27 remaining)
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 14:35 (0:00:26 remaining)
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 14:35 (0:00:27 remaining)
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.24% done; ETC: 14:35 (0:00:07 remaining)
Completed Service scan at 14:35, 150.13s elapsed (42 services on 1 host)
Initiating OS detection (try #1) against 192.168.240.134
Retrying OS detection (try #2) against 192.168.240.134
NSE: Script scanning 192.168.240.134.
Initiating NSE at 14:35
```



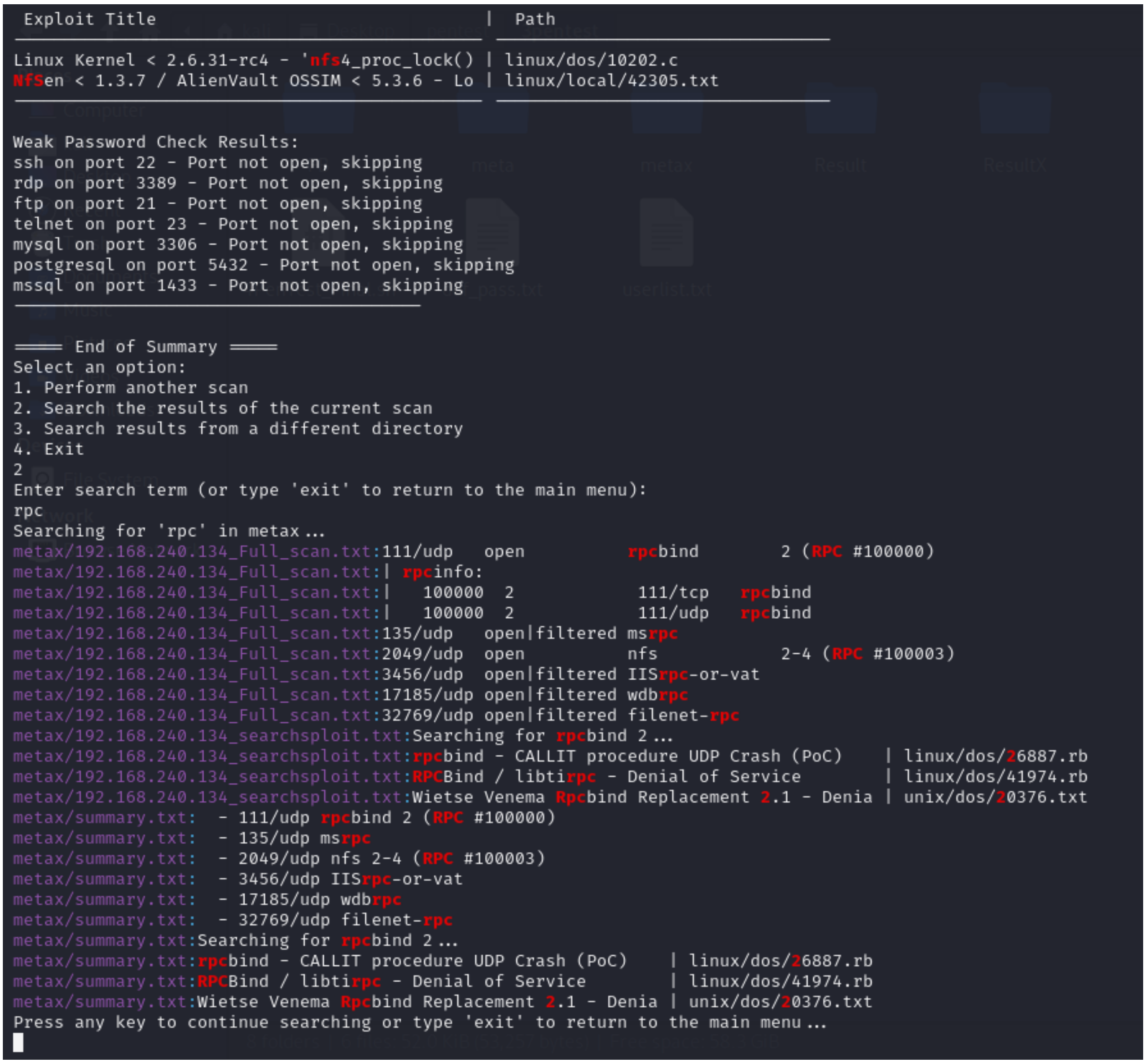
```
1434/udp  open|filtered ms-sql-m
1718/udp  open|filtered h225gatedisc
2048/udp  open|filtered dls-monitor
2049/udp  open          nfs           2-4 (RPC #100003)
3283/udp  open|filtered netassistant
3456/udp  open|filtered IISrpc-or-vat
3703/udp  open|filtered adobeserver-3
5000/udp  open|filtered upnp
5632/udp  open|filtered pcanywherestat
9200/udp  open|filtered wap-wsp
17185/udp open|filtered wdbrpc
32768/udp open|filtered omad
32769/udp open|filtered filenet-rpc
49152/udp open|filtered unknown
49153/udp open|filtered unknown
49154/udp open|filtered unknown
49191/udp open|filtered unknown
49192/udp open|filtered unknown
49200/udp open|filtered unknown
49201/udp open|filtered unknown
MAC Address: 00:0C:29:47:1D:85 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: METASPLOITABLE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>

TRACEROUTE
HOP RTT     ADDRESS
1   0.57 ms 192.168.240.134

NSE: Script Post-scanning.
Initiating NSE at 14:37
Completed NSE at 14:37, 0.00s elapsed
Initiating NSE at 14:37
Completed NSE at 14:37, 0.00s elapsed
Initiating NSE at 14:37
Completed NSE at 14:37, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 332.81 seconds
           Raw packets sent: 600 (35.979KB) | Rcvd: 81 (7.790KB)
Analyzing vulnerabilities for 192.168.240.134 using searchsploit...
```

Vulnerablilities Mapping

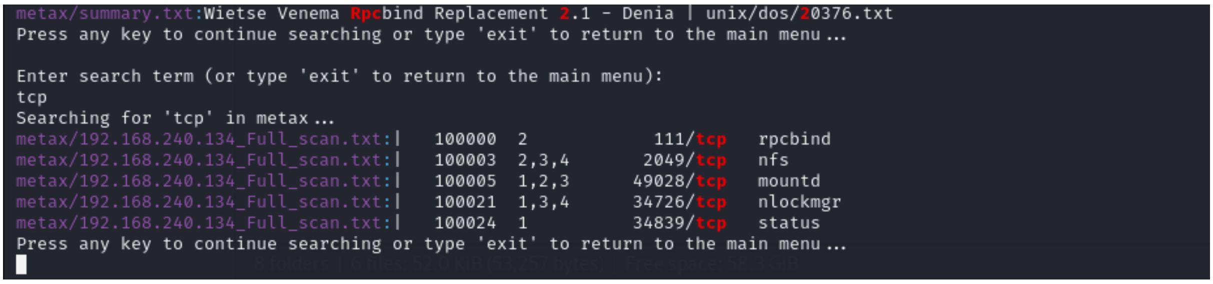


```
Searching for potentially vulnerable services:
Searching for domain ISC ...
 ─────────────────────────────────────────────── ──────────────────────────────────
  Exploit Title                                 |  Path
 ─────────────────────────────────────────────── ──────────────────────────────────
Apple Safari 2.0.4 - Cross-Domain Browser Loc | multiple/remote/30078.js
cPanel - (Authenticated) 'lastvisit.html Doma | multiple/remote/9039.txt
Microsoft Internet Explorer 5.0.1 - Cached Co | windows/remote/33024.txt
Microsoft Internet Explorer 7/8 - CSS Handlin | windows/dos/34602.html
Mozilla Firefox 3.6.8 - 'Math.random()' Cross | unix/remote/34621.c
Netscape Navigator 4.0.8 - 'about:' Domain In | unix/remote/20791.php
Research In Motion BlackBerry Device Software | hardware/remote/34802.html
WebKit 1.2.x - Local Webpage Cross Domain Inf | windows/remote/35434.txt
 ─────────────────────────────────────────────── ──────────────────────────────────

Searching for rpcbind 2 ...
 ─────────────────────────────────────────────── ──────────────────────────────────
  Exploit Title                                 |  Path
 ─────────────────────────────────────────────── ──────────────────────────────────
rpcbind - CALLIT procedure UDP Crash (PoC)    | linux/dos/26887.rb
RPCBind / libtirpc - Denial of Service        | linux/dos/41974.rb
Wietse Venema Rpcbind Replacement 2.1 - Denia | unix/dos/20376.txt
 ─────────────────────────────────────────────── ──────────────────────────────────

Searching for netbios-ns Microsoft ...

Searching for nfs 2-4 ...
 ─────────────────────────────────────────────── ──────────────────────────────────
  Exploit Title                                 |  Path
 ─────────────────────────────────────────────── ──────────────────────────────────
Linux Kernel < 2.6.31-rc4 - 'nfs4_proc_lock() | linux/dos/10202.c
NfSen < 1.3.7 / AlienVault OSSIM < 5.3.6 - Lo | linux/local/42305.txt
 ─────────────────────────────────────────────── ──────────────────────────────────


Weak Password Check Results:
ssh on port 22 - Port not open, skipping
rdp on port 3389 - Port not open, skipping
ftp on port 21 - Port not open, skipping
telnet on port 23 - Port not open, skipping
mysql on port 3306 - Port not open, skipping
postgresql on port 5432 - Port not open, skipping
mssql on port 1433 - Port not open, skipping
 ────────────────────────────────────────


═════ End of Summary ═════
Select an option:
1. Perform another scan
2. Search the results of the current scan
3. Search results from a different directory
4. Exit
```

Search Result



```
 Exploit Title                                          |  Path
────────────────────────────────────────────────────────────────────────────────────
Linux Kernel < 2.6.31-rc4 - 'nfs4_proc_lock() | linux/dos/10202.c
NfSen < 1.3.7 / AlienVault OSSIM < 5.3.6 - Lo | linux/local/42305.txt
────────────────────────────────────────────────────────────────────────────────────

Weak Password Check Results:
ssh on port 22 - Port not open, skipping
rdp on port 3389 - Port not open, skipping
ftp on port 21 - Port not open, skipping
telnet on port 23 - Port not open, skipping
mysql on port 3306 - Port not open, skipping
postgresql on port 5432 - Port not open, skipping
mssql on port 1433 - Port not open, skipping
────────────────────────────────────────

═══ End of Summary ═══
Select an option:
1. Perform another scan
2. Search the results of the current scan
3. Search results from a different directory
4. Exit
2
Enter search term (or type 'exit' to return to the main menu):
rpc
Searching for 'rpc' in metax ...
metax/192.168.240.134_Full_scan.txt:111/udp   open          rpcbind       2 (RPC #100000)
metax/192.168.240.134_Full_scan.txt:| rpcinfo:
metax/192.168.240.134_Full_scan.txt:|   100000  2            111/tcp   rpcbind
metax/192.168.240.134_Full_scan.txt:|   100000  2            111/udp   rpcbind
metax/192.168.240.134_Full_scan.txt:135/udp   open|filtered msrpc
metax/192.168.240.134_Full_scan.txt:2049/udp  open          nfs           2-4 (RPC #100003)
metax/192.168.240.134_Full_scan.txt:3456/udp  open|filtered IISrpc-or-vat
metax/192.168.240.134_Full_scan.txt:17185/udp open|filtered wdbrpc
metax/192.168.240.134_Full_scan.txt:32769/udp open|filtered filenet-rpc
metax/192.168.240.134_searchsploit.txt:Searching for rpcbind 2 ...
metax/192.168.240.134_searchsploit.txt:rpcbind - CALLIT procedure UDP Crash (PoC)    | linux/dos/26887.rb
metax/192.168.240.134_searchsploit.txt:RPCBind / libtirpc - Denial of Service        | linux/dos/41974.rb
metax/192.168.240.134_searchsploit.txt:Wietse Venema Rpcbind Replacement 2.1 - Denia | unix/dos/20376.txt
metax/summary.txt:  - 111/udp rpcbind 2 (RPC #100000)
metax/summary.txt:  - 135/udp msrpc
metax/summary.txt:  - 2049/udp nfs 2-4 (RPC #100003)
metax/summary.txt:  - 3456/udp IISrpc-or-vat
metax/summary.txt:  - 17185/udp wdbrpc
metax/summary.txt:  - 32769/udp filenet-rpc
metax/summary.txt:Searching for rpcbind 2 ...
metax/summary.txt:rpcbind - CALLIT procedure UDP Crash (PoC)    | linux/dos/26887.rb
metax/summary.txt:RPCBind / libtirpc - Denial of Service        | linux/dos/41974.rb
metax/summary.txt:Wietse Venema Rpcbind Replacement 2.1 - Denia | unix/dos/20376.txt
Press any key to continue searching or type 'exit' to return to the main menu ...
█
```



```
metax/summary.txt:Wietse Venema Rpcbind Replacement 2.1 - Denia | unix/dos/20376.txt
Press any key to continue searching or type 'exit' to return to the main menu ...

Enter search term (or type 'exit' to return to the main menu):
tcp
Searching for 'tcp' in metax ...
metax/192.168.240.134_Full_scan.txt:|   100000  2           111/tcp   rpcbind
metax/192.168.240.134_Full_scan.txt:|   100003  2,3,4      2049/tcp   nfs
metax/192.168.240.134_Full_scan.txt:|   100005  1,2,3     49028/tcp   mountd
metax/192.168.240.134_Full_scan.txt:|   100021  1,3,4     34726/tcp   nlockmgr
metax/192.168.240.134_Full_scan.txt:|   100024  1         34839/tcp   status
Press any key to continue searching or type 'exit' to return to the main menu ...
█
```