Practical – 1

Aim: Vulnerability Assessment of a system using NMAP 1. TCP SYN Scan 2.TCP FIN Scan 3. Port Scan.

Nmap is short for Network Mapper. It is an open- source security to ol for network exploration, security scanning and auditing. However, nmap command comes w ith lots of options that can make the utility more robust and difficult to follow for new users.

The purpose of this post is to introduce a user to the nmap command line tool to scan a host and/or network, so to find out the possible vulnerable points in the hosts. Y ou will also slearn how to use Nmap for offensive and defensive purposes.

1. **Scan a single host or an IP address (IPv4)**

nmap 192.168.1.112

Output:

2. **Scan using "-v" option.**

command with "-v" option is giving more detailed information about the remote machine.

nmap -v 192.168.1.112

Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -v  192.168.1.112
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:03 EDT
Initiating ARP Ping Scan at 19:03
Scanning 192.168.1.112 [1 port]
Completed ARP Ping Scan at 19:03, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:03
Completed Parallel DNS resolution of 1 host. at 19:03, 0.04s elapsed
Initiating SYN Stealth Scan at 19:03
Scanning 192.168.1.112 [1000 ports]
Discovered open port 135/tcp on 192.168.1.112
Discovered open port 139/tcp on 192.168.1.112
Discovered open port 445/tcp on 192.168.1.112
Discovered open port 5357/tcp on 192.168.1.112
Completed SYN Stealth Scan at 19:03, 10.91s elapsed (1000 total ports)
Nmap scan report for 192.168.1.112
Host is up (0.0012s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
           Raw packets sent: 3001 (132.028KB) | Rcvd: 13 (556B)
root@bt:~#
```

3. **Scan Multiple Hosts.**

   # nmap –v 192.168.1.112 192.168.1.108 192.168.1.100

Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -v  192.168.1.112 192.168.1.108 192.168.1.100
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:04 EDT
Initiating ARP Ping Scan at 19:04
Scanning 3 hosts [1 port/host]
Completed ARP Ping Scan at 19:04, 0.21s elapsed (3 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 19:04
Completed Parallel DNS resolution of 3 hosts. at 19:04, 0.04s elapsed
Initiating SYN Stealth Scan at 19:04
Scanning 3 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.1.108
Discovered open port 135/tcp on 192.168.1.108
Discovered open port 445/tcp on 192.168.1.108
Discovered open port 2869/tcp on 192.168.1.108
Discovered open port 135/tcp on 192.168.1.112
Discovered open port 445/tcp on 192.168.1.112
Discovered open port 139/tcp on 192.168.1.112
Completed SYN Stealth Scan against 192.168.1.108 in 1.96s (2 hosts left)
Completed SYN Stealth Scan against 192.168.1.100 in 2.22s (1 host left)
Discovered open port 5357/tcp on 192.168.1.112
Completed SYN Stealth Scan at 19:04, 11.32s elapsed (3000 total ports)
Nmap scan report for 192.168.1.112
Host is up (0.0018s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap scan report for 192.168.1.108
Host is up (0.00097s latency).
```

4. **Scan a whole Subnet**

   # nmap –v 192.168.1.*

   Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt : ~ # nmap  192.168.1.*
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT     STATE     SERVICE
80/tcp   open      http
113/tcp  filtered ident
MAC Address: 98:FC:11:DA:D3:20 (Cisco-Linksys)

Nmap scan report for 192.168.1.100
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.1.100 are closed
MAC Address: 80:6C:1B:4C:0E:8D (Unknown)

Nmap scan report for 192.168.1.101
Host is up (0.0011s latency).
Not shown: 982 filtered ports
PORT       STATE   SERVICE
25/tcp     closed  smtp
110/tcp    closed  pop3
135/tcp    open    msrpc
139/tcp    open    netbios-ssn
443/tcp    open    https
445/tcp    open    microsoft-ds
554/tcp    open    rtsp
902/tcp    open    iss-realsecure
912/tcp    open    apex-mesh
1001/tcp   closed  unknown
2869/tcp   open    icslap
5357/tcp   open    wsdapi
5432/tcp   closed  postgresql
root : nmap
```

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
445/tcp    closed microsoft-ds
554/tcp    open   rtsp
903/tcp    open   iss-console-mgr
1001/tcp   closed unknown
2869/tcp   open   icslap
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
10243/tcp  open   unknown
49152/tcp  open   unknown
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
49163/tcp  open   unknown
49165/tcp  open   unknown
MAC Address: 90:FB:A6:B0:FA:DB (Hon Hai Precision Ind.Co.Ltd)

Nmap scan report for 192.168.1.112
Host is up (0.0017s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap scan report for 192.168.1.113
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.1.113 are closed

Nmap done: 256 IP addresses (8 hosts up) scanned in 14.11 seconds
root@bt : ~ #
root : nmap
```

5. **Scan Multiple Servers using last octet of IP address.**

   # nmap –v 192.168.1.1,108,113,112

Output:

```
root : nmap <2>
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap 192.168.1.100,108,113,112
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:13 EDT
Nmap scan report for 192.168.1.108
Host is up (0.0016s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 08:00:27:29:1E:33 (Cadmus Computer Systems)

Nmap scan report for 192.168.1.113
Host is up (0.000019s latency).
All 1000 scanned ports on 192.168.1.113 are closed

Nmap scan report for 192.168.1.112
Host is up (0.0012s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap done: 4 IP addresses (3 hosts up) scanned in 6.71 seconds
root@bt:~#
```

6. **Scan list of Hosts from a File.**

   # nmap –iL host.txt

Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -iL host.txt
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:20 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.1.100 are closed
MAC Address: 80:6C:1B:4C:0E:8D (Unknown)

Nmap scan report for 192.168.1.108
Host is up (0.00071s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 08:00:27:29:1E:33 (Cadmus Computer Systems)

Nmap scan report for 192.168.1.112
Host is up (0.0036s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap done: 4 IP addresses (3 hosts up) scanned in 10.99 seconds
root@bt:~#
```

7. **Scan an IP Address Range**

   # nmap 192.168.1.1,100-200

Output:

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help

root@bt:~# nmap 192.168.1.100-200
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:24 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0086s latency).
All 1000 scanned ports on 192.168.1.100 are closed
MAC Address: 80:6C:1B:4C:0E:8D (Unknown)

Nmap scan report for 192.168.1.101
Host is up (0.00092s latency).
Not shown: 982 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
110/tcp   closed pop3
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
554/tcp   open   rtsp
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1001/tcp  closed unknown
2869/tcp  open   icslap
5357/tcp  open   wsdapi
5432/tcp  closed postgresql
10243/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp closed unknown
49156/tcp open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)
```

```
root:n
File  Edit  View  Bookmarks  Settings  Help
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap scan report for 192.168.1.105
Host is up (0.0057s latency).
All 1000 scanned ports on 192.168.1.105 are closed
MAC Address: 84:8E:DF:A5:99:0C (Unknown)

Nmap scan report for 192.168.1.108
Host is up (0.0022s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  icslap
MAC Address: 08:00:27:29:1E:33 (Cadmus Computer Systems)

Nmap scan report for 192.168.1.109
Host is up (0.00076s latency).
Not shown: 980 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
110/tcp   closed pop3
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   closed microsoft-ds
554/tcp   open   rtsp
903/tcp   open   iss-console-mgr
1001/tcp  closed unknown
2869/tcp  open   icslap
5357/tcp  open   wsdapi
5432/tcp  closed postgresql
```

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
445/tcp    closed microsoft-ds
554/tcp    open   rtsp
903/tcp    open   iss-console-mgr
1001/tcp   closed unknown
2869/tcp   open   icslap
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
10243/tcp  open   unknown
49152/tcp  open   unknown
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
49163/tcp  open   unknown
49165/tcp  open   unknown
MAC Address: 90:FB:A6:B0:FA:DB (Hon Hai Precision Ind.Co.Ltd)

Nmap scan report for 192.168.1.112
Host is up (0.0016s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap scan report for 192.168.1.113
Host is up (0.000018s latency).
All 1000 scanned ports on 192.168.1.113 are closed

Nmap done: 101 IP addresses (7 hosts up) scanned in 11.43 seconds
root@bt:~#
```

8. Scan Network Excluding Remote Hosts.

nmap 192.168.1.* --exclude 192.168.1.100

Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap 192.168.1.* --exclude 192.168.1.100
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:27 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 998 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
113/tcp  filtered ident
MAC Address: 98:FC:11:DA:D3:20 (Cisco-Linksys)

Nmap scan report for 192.168.1.101
Host is up (0.0027s latency).
Not shown: 982 filtered ports
PORT       STATE  SERVICE
25/tcp     closed smtp
110/tcp    closed pop3
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
554/tcp    open   rtsp
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
1001/tcp   closed unknown
2869/tcp   open   icslap
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
10243/tcp  open   unknown
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
```

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
445/tcp   closed microsoft-ds
554/tcp   open   rtsp
903/tcp   open   iss-console-mgr
1001/tcp  closed unknown
2869/tcp  open   icslap
5357/tcp  open   wsdapi
5432/tcp  closed postgresql
10243/tcp open   unknown
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp closed unknown
49156/tcp open   unknown
49163/tcp open   unknown
49165/tcp open   unknown
MAC Address: 90:FB:A6:B0:FA:DB (Hon Hai Precision Ind.Co.Ltd)

Nmap scan report for 192.168.1.112
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap scan report for 192.168.1.113
Host is up (0.000026s latency).
All 1000 scanned ports on 192.168.1.113 are closed

Nmap done: 255 IP addresses (7 hosts up) scanned in 23.13 seconds
root@bt:~#
```

9. **Scan OS information and Trace route.**

   # nmap -A 192.168.1.112

Output:

```
root : bash
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -A  192.168.1.112

Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:29 EDT
Nmap scan report for 192.168.1.112
Host is up (0.0018s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE     VERSION
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  netbios-ssn
5357/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vis
ta::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or W
indows 7, Microsoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ADMIN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d7:27:5b (Cadmus Computer Syst
ems)
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
root : bash
```

```
root : bash
File  Edit  View  Bookmarks  Settings  Help
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vis
ta::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or W
indows 7, Microsoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ADMIN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d7:27:5b (Cadmus Computer Syst
ems)
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   NetBIOS computer name: ADMIN-PC
|   Workgroup: WORKGROUP
|_  System time: 2015-07-23 19:30:22 UTC+5.5

TRACEROUTE
HOP RTT     ADDRESS
1   1.76 ms 192.168.1.112

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.41 seconds
root@bt: # 
root : bash
```

10. Enable OS Detection with Nmap.

nmap -O 192.168.1.101

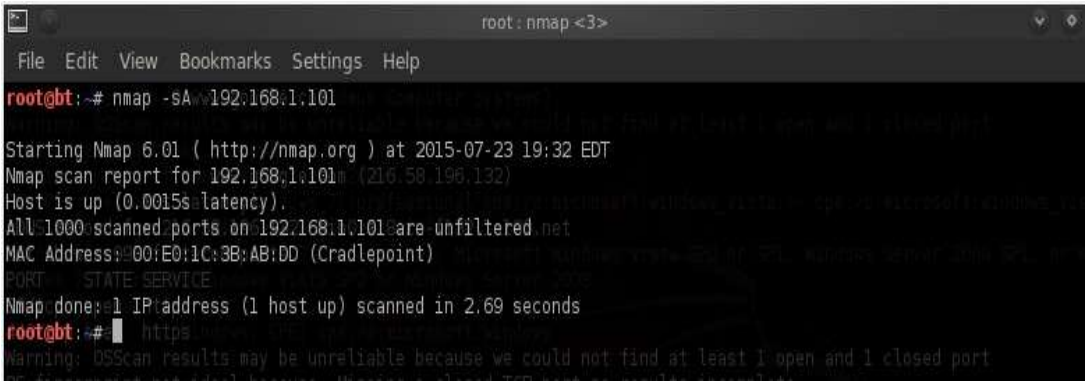
Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt: # nmap -O 192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:33 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0010s latency).
Not shown: 982 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
110/tcp   closed pop3
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
554/tcp   open   rtsp
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1001/tcp  closed unknown
2869/tcp  open   icslap
5357/tcp  open   wsdapi
5432/tcp  closed postgresql
10243/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp closed unknown
49156/tcp open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)
Device type: general purpose
Running: Microsoft Windows 2008|7
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows 7 or Windows Server 2008 SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

11. Scan a Host to Detect Firewall.

nmap -sA 192.168.1.101

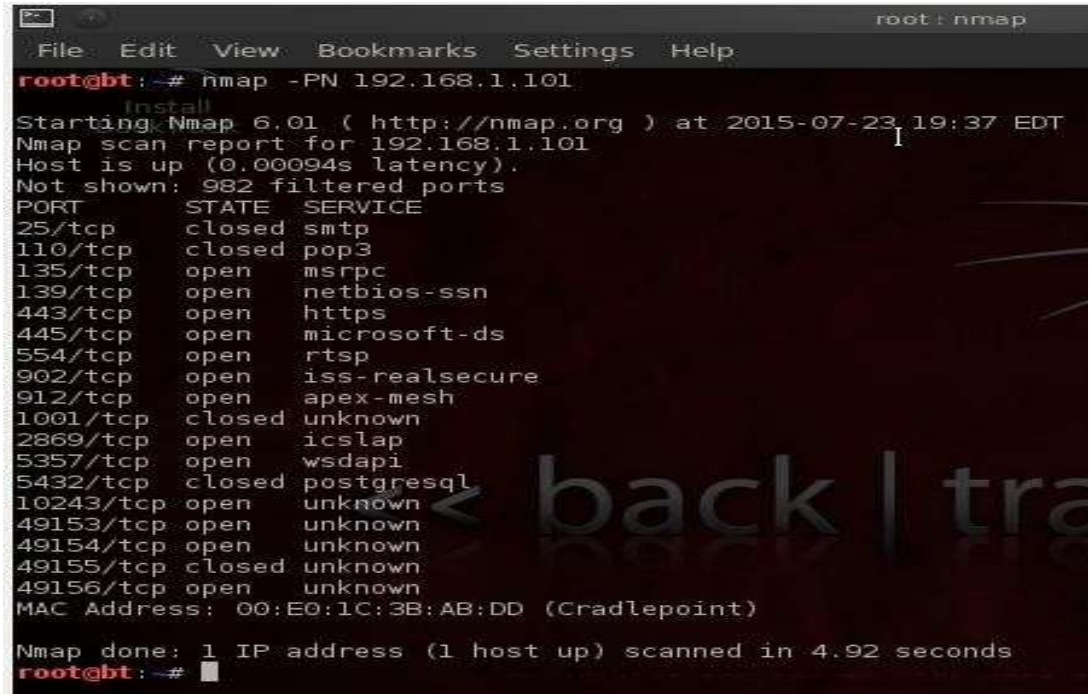
Output:



12. Scan a Host to check its protected by Firewall.

nmap -PN 192.168.1.101

Output:



13. Find out Live hosts in a Network

nmap -sP 192.168.1.*

Output:

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -sP 192.168.1.*
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00096s latency).
MAC Address: 98:FC:11:DA:D3:20 (Cisco-Linksys)
Nmap scan report for 192.168.1.100
Host is up (0.025s latency).
MAC Address: 80:6C:1B:4C:0E:8D (Unknown)
Nmap scan report for 192.168.1.101
Host is up (0.00053s latency).
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)
Nmap scan report for 192.168.1.105
Host is up (0.091s latency).
MAC Address: 84:8E:DF:A5:99:0C (Unknown)
Nmap scan report for 192.168.1.108
Host is up (0.0018s latency).
MAC Address: 08:00:27:29:1E:33 (Cadmus Computer Systems)
Nmap scan report for 192.168.1.109
Host is up (0.00056s latency).
MAC Address: 90:FB:A6:B0:FA:DB (Hon Hai Precision Ind.Co.Ltd)
Nmap scan report for 192.168.1.112
Host is up (0.00090s latency).
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 8.40 seconds
root@bt:~#
```

14. Perform a Fast Scan.

nmap -F 192.168.1.*

Output

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -F 192.168.1.*
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0010s latency).
Not shown: 98 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
113/tcp  filtered ident
MAC Address: 98:FC:11:DA:D3:20 (Cisco-Linksys)

Nmap scan report for 192.168.1.101
Host is up (0.00084s latency).
Not shown: 87 filtered ports
PORT       STATE  SERVICE
25/tcp     closed smtp
110/tcp    closed pop3
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
554/tcp    open   rtsp
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap scan report for 192.168.1.105
Host is up (0.062s latency).
All 100 scanned ports on 192.168.1.105 are closed
```

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
PORT      STATE  SERVICE
25/tcp    closed smtp
110/tcp   closed pop3
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   closed microsoft-ds
554/tcp   open   rtsp
5357/tcp  open   wsdapi
5432/tcp  closed postgresql
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp closed unknown
49156/tcp open   unknown
MAC Address: 90:FB:A6:B0:FA:DB (Hon Hai Precision Ind.Co.Ltd)

Nmap scan report for 192.168.1.112
Host is up (0.0011s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:D7:27:5B (Cadmus Computer Systems)

Nmap scan report for 192.168.1.113
Host is up (0.000018s latency).
All 100 scanned ports on 192.168.1.113 are closed

Nmap done: 256 IP addresses (7 hosts up) scanned in 13.29 seconds
root@bt:~#
```

15. Find Nmap version.

nmap -V

Output:

```
root : bash <2>
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -V

Nmap version 6.01 ( http://nmap.org )
Platform: i686-pc-linux-gnu
Compiled with: nmap-liblua-5.1.3 openssl-0.9.8k libpcre-7.8 libpcap-1.0.0 nmap-libdnet-1.12 ipv6
Compiled without:
root@bt:~#
```

16. Scan Ports Consecutively.

nmap -r 192.168.1.101

Output:

```
root : nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -r 192.168.1.101

Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:42 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0017s latency).
Not shown: 982 filtered ports
PORT       STATE  SERVICE
25/tcp     closed smtp
110/tcp    closed pop3
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
554/tcp    open   rtsp
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
1001/tcp   closed unknown
2869/tcp   open   icslap
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
10243/tcp  open   unknown
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.09 seconds
root@bt:~#
```

17. Print Host interfaces and Routes.

nmap -- iflist

Output:

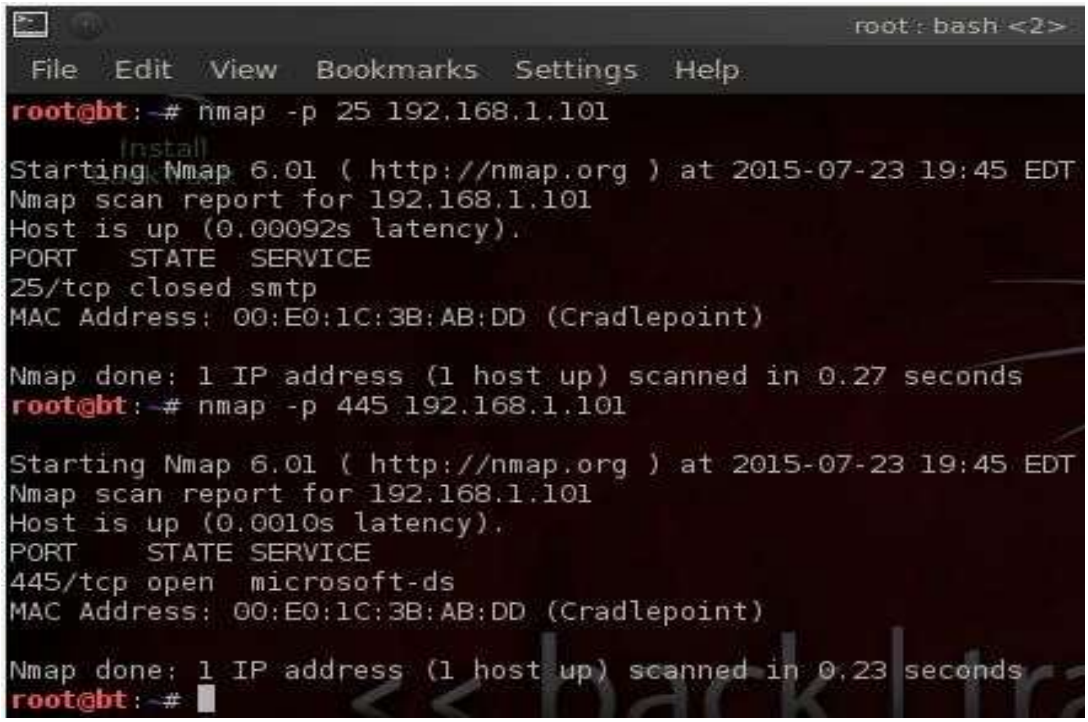
```
root : bash <2>
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap --iflist

Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:43 EDT
************************INTERFACES************************
DEV  (SHORT) IP/MASK                     TYPE     UP MTU   MAC
lo   (lo)    127.0.0.1/8                 loopback up 16436
lo   (lo)    ::1/128                     loopback up 16436
eth0 (eth0)  192.168.1.113/24            ethernet up 1500  08:00:27:8D:63:DD
eth0 (eth0)  fe80::a00:27ff:fe8d:63dd/64 ethernet up 1500  08:00:27:8D:63:DD

**************************ROUTES**************************
DST/MASK       DEV  GATEWAY
192.168.1.0/24 eth0
0.0.0.0/0      eth0 192.168.1.1

root@bt:~#
```

18. Scan for specific Port.

There are various options to discover ports on remote machine with Nmap. We can specify the port we want nmap to scan with **-p** option, by default nmap scans only TCP ports.

namp –p 25 192.168.1.101

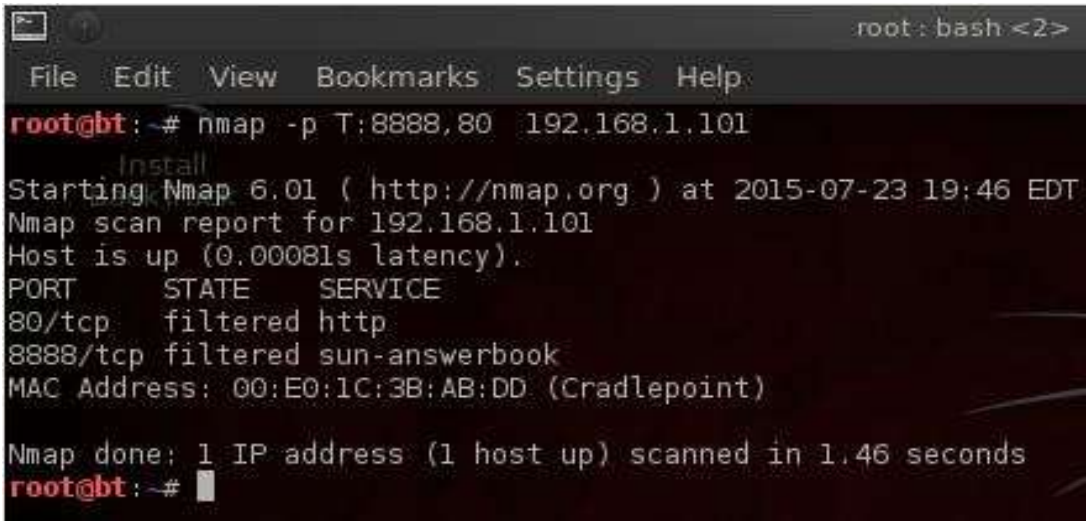
Output:



19. Scan a TCP Port.

nmap –p T:8080,80 192.168.1.101

Output:



20. Scan a UDP Port.

nmap –sU 192.168.1.101

Output:

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -sU 137  192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:50 EDT
Invalid target host specification: 137
Nmap scan report for 192.168.1.101
Host is up (0.0010s latency).
Not shown: 995 open|filtered ports
PORT       STATE  SERVICE
135/udp    closed msrpc
137/udp    open   netbios-ns
443/udp    closed https
49156/udp closed unknown
49185/udp closed unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds
root@bt:~#
```

21. Scan Multiple Ports.

nmap –p 25,80,117,115 192.168.1.101

Output:

```
root:bash
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -p 25,80,117,115 192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:51 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0014s latency).
PORT     STATE    SERVICE
25/tcp   closed   smtp
80/tcp   filtered http
115/tcp  filtered sftp
117/tcp  filtered uucp-path
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
root@bt:~#
```

22. Scan Ports by Network Range.

nmap –p 1-300 192.168.1.101

Output:

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -p 1-300  192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:52 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0011s latency).
Not shown: 296 filtered ports
PORT     STATE  SERVICE
25/tcp   closed smtp
110/tcp  closed pop3
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
root@bt:~#
```

23. Scan remote hosts using TCP ACK (PA) and TCP Syn (PS).

nmap –PS 192.168.1.101

Output:

```
root:nmap <2>
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -PS 192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:54 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0014s latency).
Not shown: 982 filtered ports
PORT       STATE  SERVICE
25/tcp     closed smtp
110/tcp    closed pop3
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
554/tcp    open   rtsp
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
1001/tcp   closed unknown
2869/tcp   open   icslap
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
10243/tcp  open   unknown
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds
root@bt:~#
```

24. Scan Remote host for specific ports with TCP ACK.

nmap –PA –p 80 192.168.1.101

Output:

```
root:bash
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -PA -p 80 192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:56 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0012s latency).
PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@bt:~#
```

25. Scan Remote host for specific ports with TCP Syn.

nmap –PA –p 80 192.168.1.101

Output:

```
root@bt:~# nmap -PS -p 445 192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:57 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0018s latency).
PORT     STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
root@bt:~#
```

26. Perform a stealthy Scan.

nmap –sS 192.168.1.101

Output:

```
root@bt:~# nmap -sS 192.168.1.101
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:57 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00074s latency).
Not shown: 982 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
110/tcp   closed pop3
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
554/tcp   closed rtsp
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1001/tcp  closed unknown
2869/tcp  open   icslap
5357/tcp  open   wsdapi
5432/tcp  closed postgresql
10243/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp closed unknown
49156/tcp open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.44 seconds
root@bt:~#
```

27. Check most commonly used Ports with TCP Syn

nmap –sT 192.168.1.101

Output:

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# nmap -sT 192.168.1.101

Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:58 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0011s latency).
Not shown: 982 filtered ports
PORT       STATE  SERVICE
25/tcp     closed smtp
110/tcp    closed pop3
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
554/tcp    closed rtsp
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
1001/tcp   closed unknown
2869/tcp   open   icslap
5357/tcp   open   wsdapi
5432/tcp   closed postgresql
10243/tcp  open   unknown
49153/tcp  open   unknown
49154/tcp  open   unknown
49155/tcp  closed unknown
49156/tcp  open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds
root@bt:~# nmap -sN 192.168.1.101

Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:59 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00071s latency).
```

28. Perform a tcp null scan to fool a firewall.

nmap –sN 192.168.1.101

Output:

```
root:nmap
File  Edit  View  Bookmarks  Settings  Help
49156/tcp open   unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds
root@bt:~# nmap -sN 192.168.1.101

Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-23 19:59 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00071s latency).
Not shown: 982 open|filtered ports
PORT       STATE  SERVICE
25/tcp     closed smtp
110/tcp    closed pop3
135/tcp    closed msrpc
139/tcp    closed netbios-ssn
443/tcp    closed https
445/tcp    closed microsoft-ds
554/tcp    closed rtsp
902/tcp    closed iss-realsecure
912/tcp    closed apex-mesh
1001/tcp   closed unknown
2869/tcp   closed icslap
5357/tcp   closed wsdapi
5432/tcp   closed postgresql
10243/tcp  closed unknown
49153/tcp  closed unknown
49154/tcp  closed unknown
49155/tcp  closed unknown
49156/tcp  closed unknown
MAC Address: 00:E0:1C:3B:AB:DD (Cradlepoint)

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
root@bt:~#
```

Port no.	Services	Application	Vulnerability	Exploit
80: TCP, UDP	HTTP, WWW	Hyper Text Transfer Protocol (HTTP) - port used for web traffic. Hypertext Transfer Protocol (HTTP) (official)	Weak	Trojan(711 trojan, AckCmd BlueFire Cafeini Duddie Executor, God Message Seeker Slapper WebServerCT (WebDownloader)
25: TCP, UDP	SMTP	SMTP (Simple Mail Transfer Protocol). Many worms contain their own SMTP engine and use it to propagate by mass- mailing the payload, often also spoofing the "From: ..." field in emails.	Weak	Antigen Barok BSE EmailPasswordSender EPSII Gip Gris Happy99 Hpteammail Hybris Iloveyou Kuang2 MagicHorse MBTMailBombingTrojan
110: TCP, UDP	POP3	POP3 (Post Office Protocol - Version 3) Re-usable cleartext password, no auditing of connections & attempts thus subject to grinding. Some POP3 server versions have had buffer overflow problems.	Weak	Trojan Pro-MailTrojan Bancos Civcat
135: TCP, UDP	Loc-srv Msrpc Epmap	Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software.	weak	W32.Kiman Femot W32.Blaster.Worm W32.Francette.Worm W32.Mytob
139: TCP, UDP	Net-Bios ss	NetBIOS is a protocol used for File and Print Sharing under all current versions of Windows. While this in itself is not a problem, the way that the protocol is implemented can be. There are a number of vulnerabilities associated with leaving this port open. **NetBios services:** NETBIOS Session	Weak	Trojan: Chode, God Message Worm Msinit Network Qaz Sadmind SMB Relay
443: TCP, SCTP	HTTPS Games Application (AIMVIDEIM ,Battlefieldetc)	HTTPS / SSL - encrypted web traffic. ASUS AiCloud routers file sharing service uses ports 443 and 8082.	Weak	Civcat Tabdim W32.Kelvir

Port no.	Services	Application	Vulnerability	Exploit
445	Microsoft- ds	TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. This service is only implemented in the more recent verions of Windows (e.g. Windows 2K / XP). The SMB (Server Message Block) protocol is used among other things for file sharing in Windows NT/2K/XP.	weak	Otinet Rtkit Secefa W32.Aizu W32.Bobax W32.Bolgi.Worm W32.Cissi W32.Cycle W32.Explet W32.HLLW.Deborms W32.HLLW.Deloder W32.HLLW.Gaobot W32.HLLW.Lioten W32.HLLW.Moega W32.HLLW.Nebiwo W32.HLLW.Polybot
902	ideafarm-door ideafarm-chat iss-realsecure	self-documenting Telnet Door self-documenting Door: send 0x00 for info IDEAFARM-CHAT ISS RealSecure Sensor	Weak	Trojan(Net Devil Pest)
903 Tcp,udp	ideafarm-door ideafarm-chat iss-realsecure	self documenting Telnet Door self documenting Door: send 0x00 for info IDEAFARM-CHAT ISS RealSecure Sensor	Weak	Trojan(Net Devil Pest)