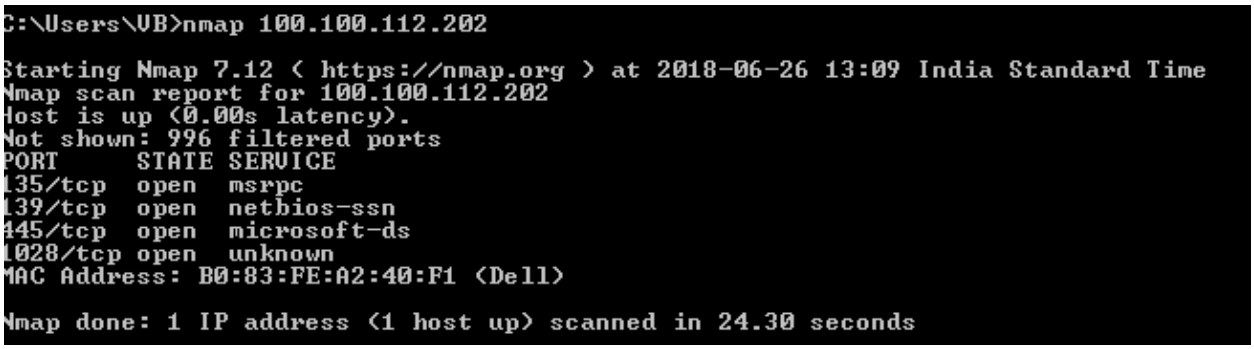
Practical 1

TCP/UDP scanning using NMAP and ZENMAP

Aim: Scan a single IP
Syntax: nmap ip address
It will scan 1 ip address in which it will search for open ports and services foe the MAC address provided.



Aim: Scan a range of IP address
Syntax: nmap ipaddress-ipaddress
EG: nmap 100.100.112.200-210

```
C:\Users\VB>nmap 100.100.112.210-215

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:44 India Standard Tim
Nmap scan report for 100.100.112.213
Host is up (0.0060s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A2:1B:2A (Dell)

Nmap scan report for 100.100.112.214
Host is up (0.00s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1028/tcp open  unknown
2869/tcp open  icslap
MAC Address: B0:83:FE:A5:19:4F (Dell)

Nmap scan report for 100.100.112.215
Host is up (0.0046s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
1031/tcp open  iad2
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A5:92:0B (Dell)

Nmap done: 6 IP addresses (3 hosts up) scanned in 18.16 seconds
```

Aim: Scan a subnet
Syntax: nmap ipaddress/subnet
EG: nmap 100.100.112.202/24

```
C:\Users\VB>nmap 100.100.112.204/50

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:58 India Standard Time
Illegal netmask in "100.100.112.204/50". Assuming /32 (one host)
Nmap scan report for 100.100.112.204
Host is up (0.00s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: B0:83:FE:A5:89:54 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 18.11 seconds
```

Aim: Scan a single port
Syntax: nmap –p portname ipaddress
EG: nmap –p 80 100.100.112.202

```
C:\Users\VB>nmap -p 80 100.100.112.202

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:37 India Standard Time
Nmap scan report for 100.100.112.202
Host is up (0.00s latency).
PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: B0:83:FE:A2:40:F1 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

AIM: To find information about the operating system
Syntax: nmap –O -ipaddress
Nmap –O 100.100.112.202

```
C:\Users\VB>nmap -O 100.100.112.202

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:35 India Standard Time
Nmap scan report for 100.100.112.202
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1028/tcp open  unknown
MAC Address: B0:83:FE:A2:40:F1 (Dell)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8
osoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7,
crosoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.20 seconds
```

AIM: To find the range of ports
SYNTAX: nmap –p portrange ipaddress

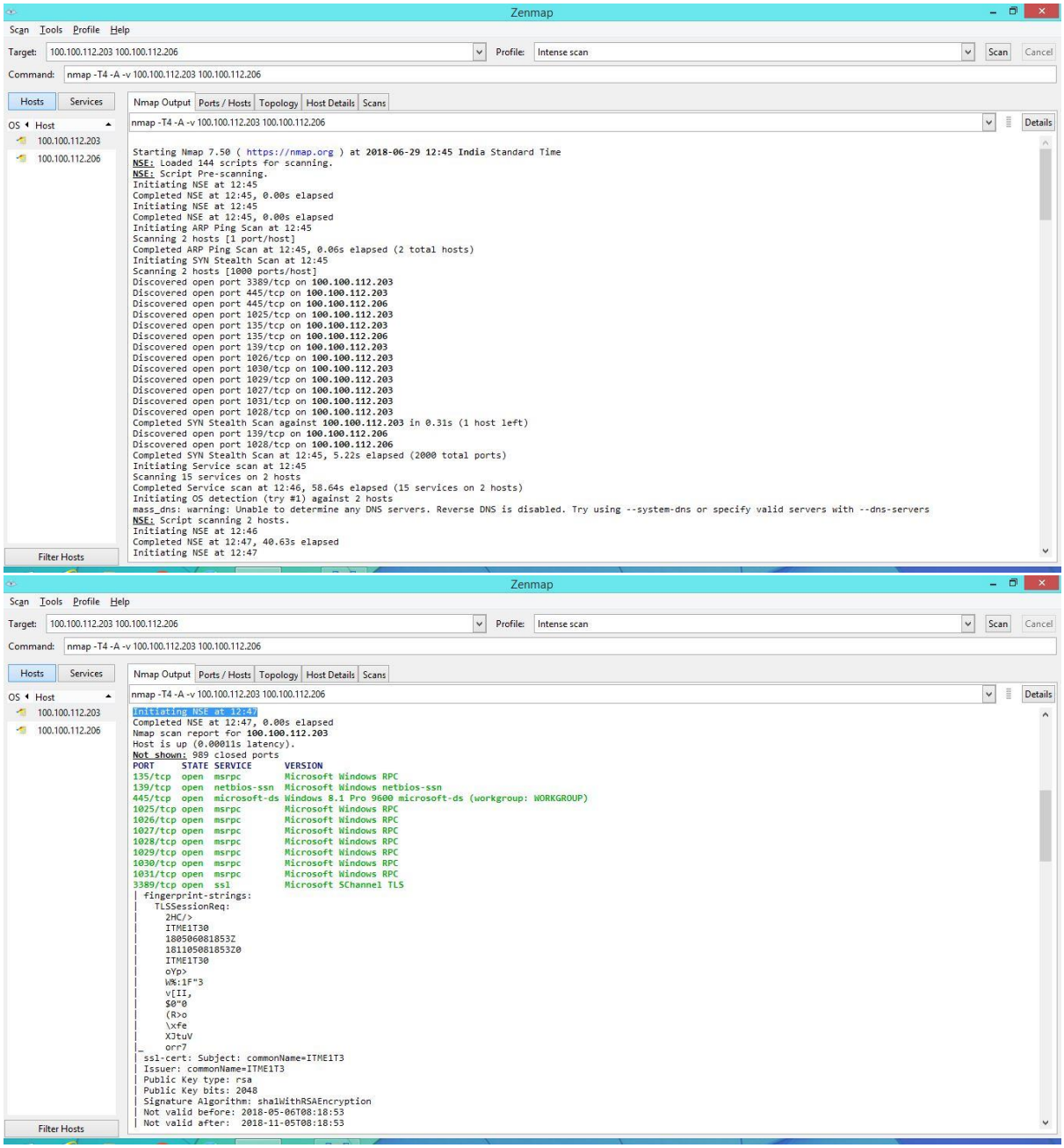
```
C:\Users\VB>nmap -p 80-85 100.100.112.202

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:42 India Standard Time
Nmap scan report for 100.100.112.202
Host is up (0.00s latency).
PORT   STATE    SERVICE
80/tcp filtered http
81/tcp filtered hosts2-ns
82/tcp filtered xfer
83/tcp filtered mit-ml-dev
84/tcp filtered ctf
85/tcp filtered mit-ml-dev
MAC Address: B0:83:FE:A2:40:F1 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

AIM: To scan all the ports
SYNTAX: nmap –p ipaddress
EG: nmap –p 100.100.112.202

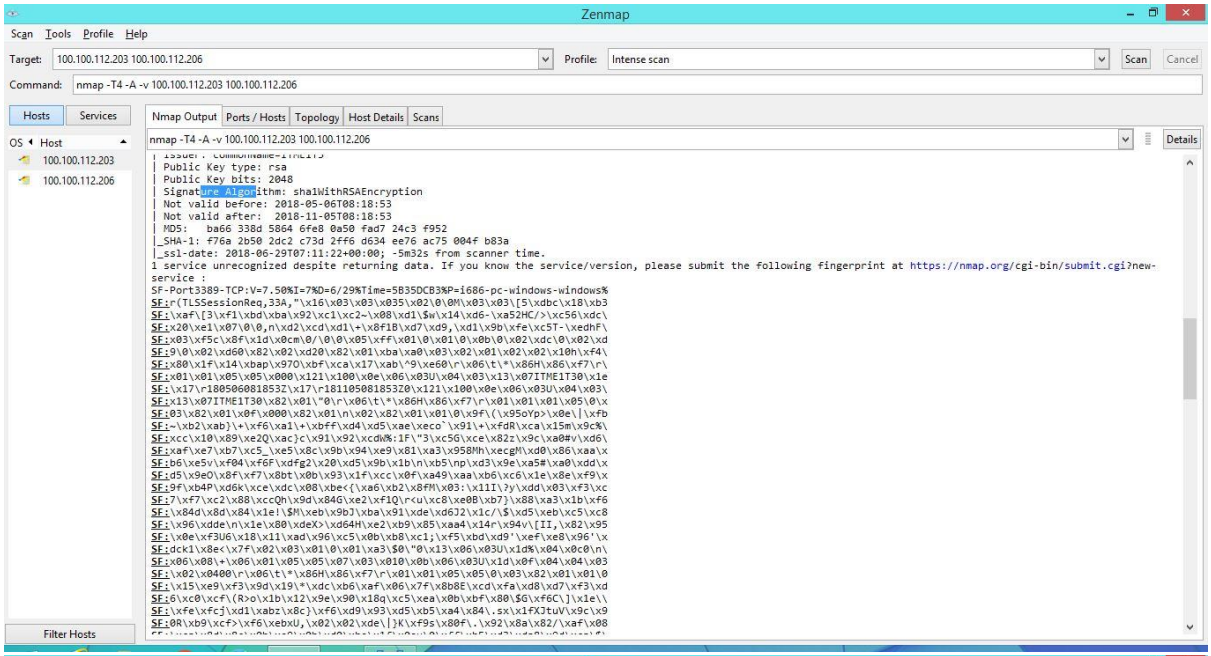
```
C:\Users\VB>nmap -p 100.100.112.202

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:48 India Standard Time
Failed to resolve "ûp".
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Packet Tracing disabled.
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.65% done
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.20% done; ETC: 13:50 (0:01:22 remaining)
Nmap scan report for 100.100.112.202
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1028/tcp open  unknown
MAC Address: B0:83:FE:A2:40:F1 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 20.43 seconds
```

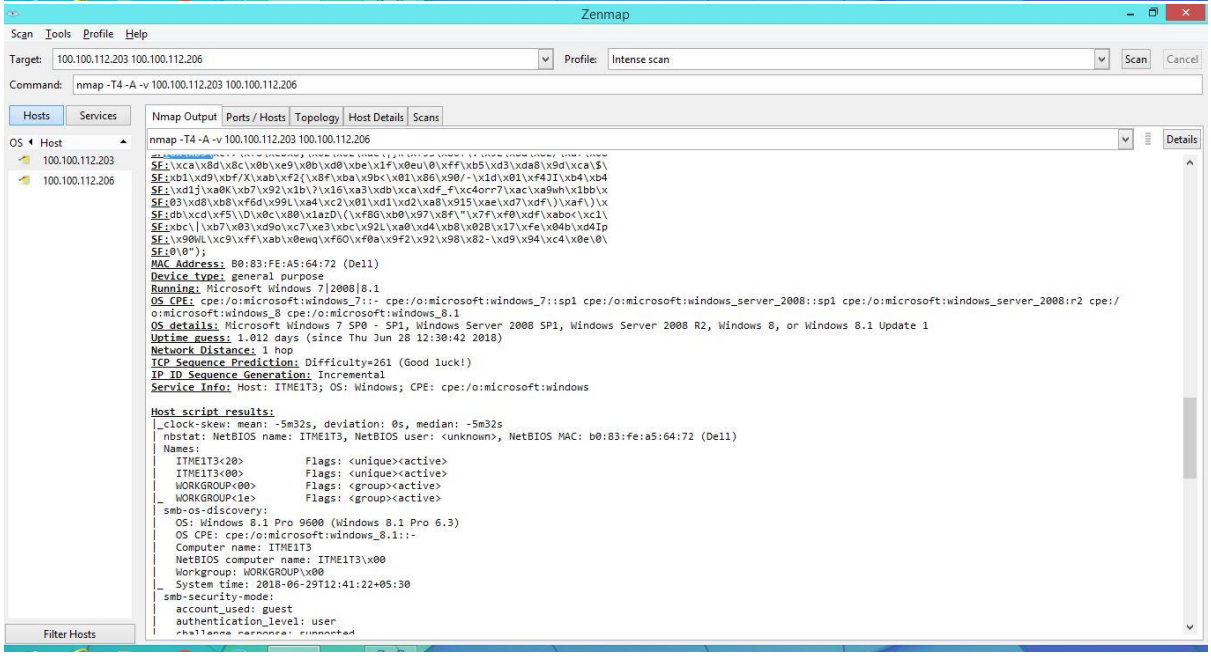
AIM: To find first 100 most common ports
SYNTAX: nmap –f ipaddress
EG: nmap –f 100.100.112.202

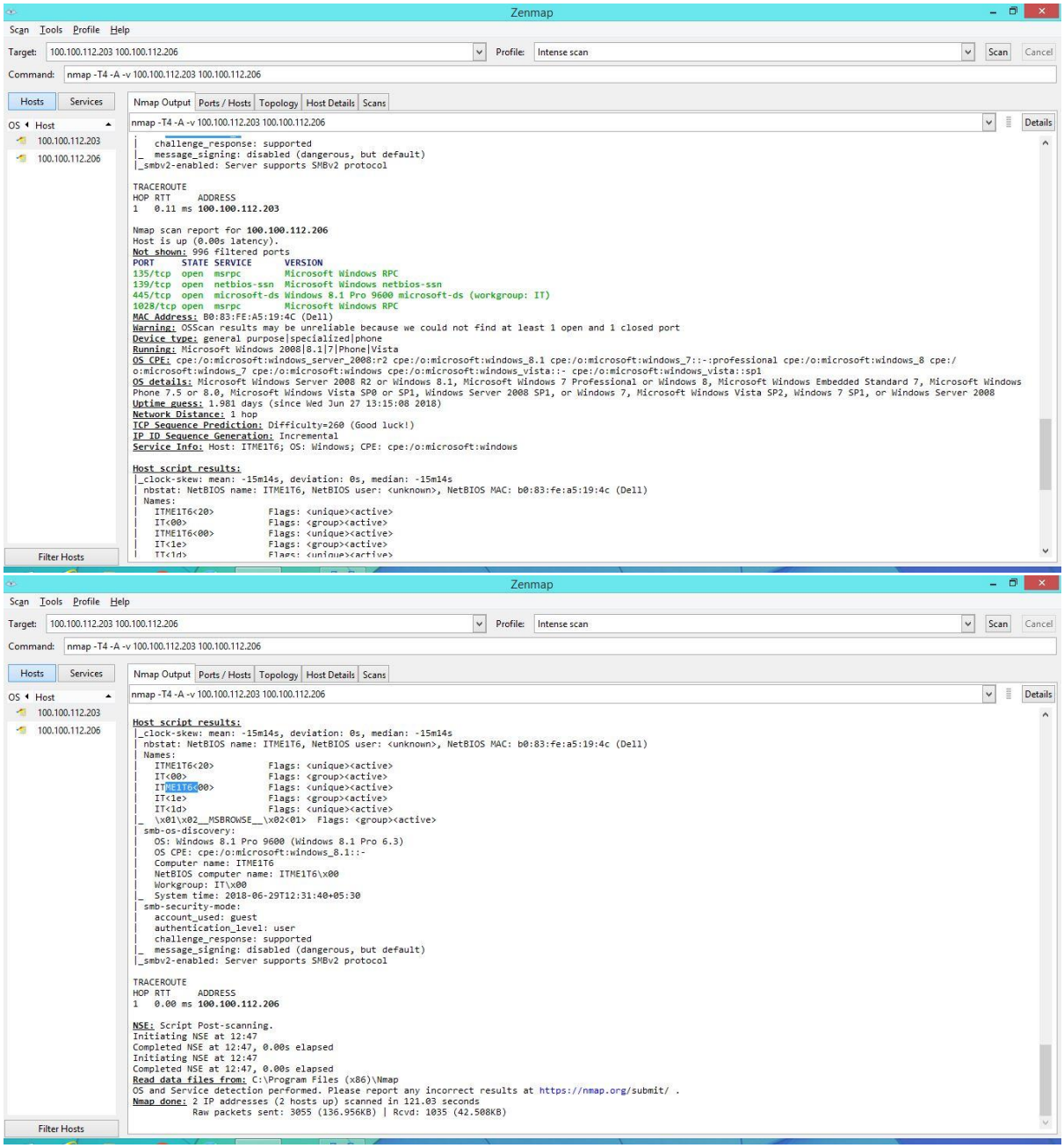
```
C:\Users\VB>nmap -f 100.100.112.202

Starting Nmap 7.12 ( https://nmap.org ) at 2018-06-26 13:50 India Standard Time
Failed to resolve "ûf".
Nmap scan report for 100.100.112.202
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1028/tcp open  unknown
MAC Address: B0:83:FE:A2:40:F1 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds
```

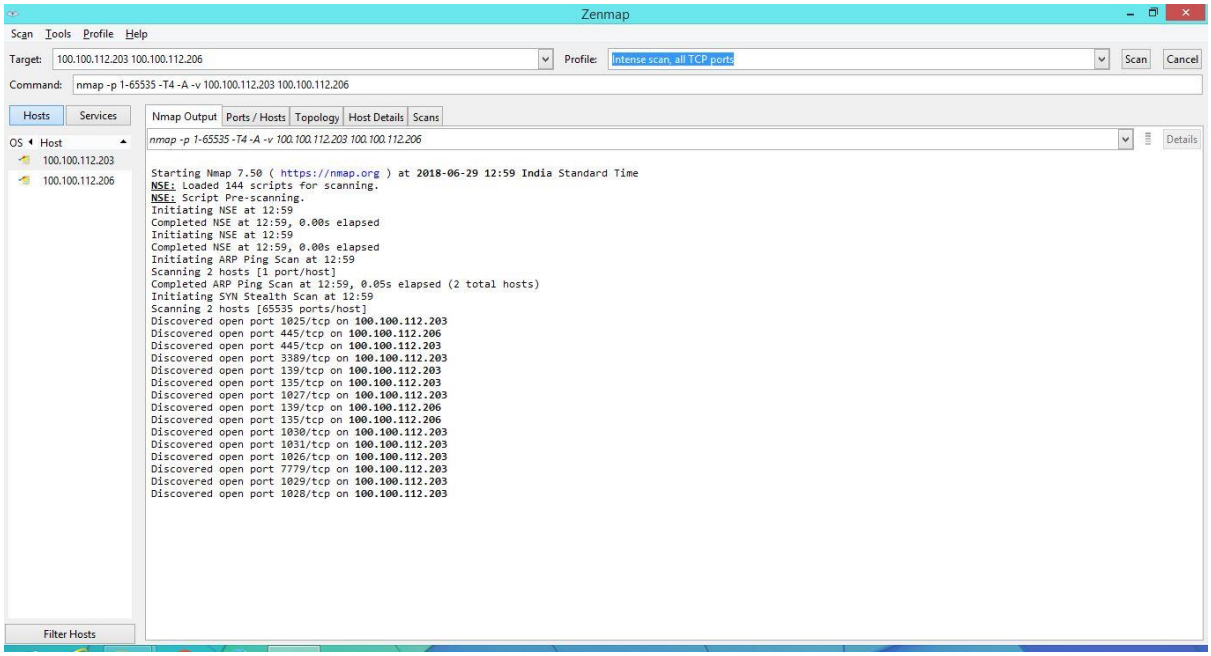

Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 100.100.112.203 100.100.112.206
Hosts
Services
OS Host
100.100.112.203
100.100.112.206
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 100.100.112.203 100.100.112.206
Details
Starting Nmap 7.50 (https://nmap.org) at 2018-06-29 12:45 India Standard Time
NSE: Loaded 144 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating ARP Ping Scan at 12:45
Scanning 2 hosts [1 port/host]
Completed ARP Ping Scan at 12:45, 0.06s elapsed (2 total hosts)
Initiating SYN Stealth Scan at 12:45
Scanning 2 hosts [1000 ports/host]
Discovered open port 3389/tcp on 100.100.112.203
Discovered open port 445/tcp on 100.100.112.203
Discovered open port 445/tcp on 100.100.112.206
Discovered open port 1025/tcp on 100.100.112.203
Discovered open port 135/tcp on 100.100.112.203
Discovered open port 135/tcp on 100.100.112.206
Discovered open port 139/tcp on 100.100.112.203
Discovered open port 1026/tcp on 100.100.112.203
Discovered open port 1030/tcp on 100.100.112.203
Discovered open port 1029/tcp on 100.100.112.203
Discovered open port 1027/tcp on 100.100.112.203
Discovered open port 1031/tcp on 100.100.112.203
Discovered open port 1028/tcp on 100.100.112.203
Completed SYN Stealth Scan against 100.100.112.203 in 0.31s (1 host left)
Discovered open port 139/tcp on 100.100.112.206
Discovered open port 1028/tcp on 100.100.112.206
Completed SYN Stealth Scan at 12:45, 5.22s elapsed (2000 total ports)
Initiating Service scan at 12:45
Scanning 15 services on 2 hosts
Completed Service scan at 12:46, 58.64s elapsed (15 services on 2 hosts)
Initiating OS detection (try #1) against 2 hosts
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
NSE: Script scanning 2 hosts.
Initiating NSE at 12:46
Completed NSE at 12:47, 40.63s elapsed
Initiating NSE at 12:47
Filter Hosts

Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 100.100.112.203 100.100.112.206
Hosts
Services
OS Host
100.100.112.203
100.100.112.206
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 100.100.112.203 100.100.112.206
Details
Initiating NSE at 12:47
Completed NSE at 12:47, 0.00s elapsed
Nmap scan report for 100.100.112.203
Host is up (0.00011s latency).
Not shown: 989 closed ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 8.1 Pro 9600 microsoft-ds (workgroup: WORKGROUP)
1025/tcp open msrpc Microsoft Windows RPC
1026/tcp open msrpc Microsoft Windows RPC
1027/tcp open msrpc Microsoft Windows RPC
1028/tcp open msrpc Microsoft Windows RPC
1029/tcp open msrpc Microsoft Windows RPC
1030/tcp open msrpc Microsoft Windows RPC
1031/tcp open msrpc Microsoft Windows RPC
3389/tcp open ssl Microsoft SChannel TLS
| fingerprint-strings:
| TLSSessionReq:
| 2HC/>
| ITME1T30
| 180506081853Z
| 181105081853Z0
| ITME1T30
| oYp>
| W%:1F"3
| v[II,
| $0"0
| (R>o
| \xfe
| XJtuV
|_ orr7
| ssl-cert: Subject: commonName=ITME1T3
| Issuer: commonName=ITME1T3
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2018-05-06T08:18:53
| Not valid after: 2018-11-05T08:18:53
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 100.100.112.203 100.100.112.206
Hosts Services
OS Host
100.100.112.203
100.100.112.206
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 100.100.112.203 100.100.112.206
Details
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2018-05-06T08:18:53
| Not valid after: 2018-11-05T08:18:53
| MD5: ba66 338d 5864 6fe8 0a50 fad7 24c3 f952
|_SHA-1: f76a 2b50 2dc2 c73d 2ff6 d634 ee76 ac75 004f b83a
|_ssl-date: 2018-06-29T07:11:22+00:00; -5m32s from scanner time.
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 100.100.112.203 100.100.112.206
Hosts Services
OS Host
100.100.112.203
100.100.112.206
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 100.100.112.203 100.100.112.206
Details
MAC Address: B0:83:FE:A5:64:72 (Dell)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 1.012 days (since Thu Jun 28 12:30:42 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: ITME1T3; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
|_clock-skew: mean: -5m32s, deviation: 0s, median: -5m32s
| nbstat: NetBIOS name: ITME1T3, NetBIOS user: <unknown>, NetBIOS MAC: b0:83:fe:a5:64:72 (Dell)
| Names:
| ITME1T3<20> Flags: <unique><active>
| ITME1T3<00> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
|_ WORKGROUP<1e> Flags: <group><active>
| smb-os-discovery:
| OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
| OS CPE: cpe:/o:microsoft:windows_8.1::-
| Computer name: ITME1T3
| NetBIOS computer name: ITME1T3\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2018-06-29T12:41:22+05:30
| smb-security-mode:
| account_used: guest
| authentication_level: user
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 100.100.112.203 100.100.112.206
Hosts Services
OS Host
100.100.112.203
100.100.112.206
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 100.100.112.203 100.100.112.206
Details
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
TRACEROUTE
HOP RTT ADDRESS
1 0.11 ms 100.100.112.203
Nmap scan report for 100.100.112.206
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 8.1 Pro 9600 microsoft-ds (workgroup: IT)
1028/tcp open msrpc Microsoft Windows RPC
MAC Address: B0:83:FE:A5:19:4C (Dell)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 1.981 days (since Wed Jun 27 13:15:08 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: ITME1T6; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
|_clock-skew: mean: -15m14s, deviation: 0s, median: -15m14s
| nbstat: NetBIOS name: ITME1T6, NetBIOS user: <unknown>, NetBIOS MAC: b0:83:fe:a5:19:4c (Dell)
| Names:
| ITME1T6<20> Flags: <unique><active>
| IT<00> Flags: <group><active>
| ITME1T6<00> Flags: <unique><active>
| IT<1e> Flags: <group><active>
| IT<1d> Flags: <unique><active>
Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 100.100.112.203 100.100.112.206
Hosts Services
OS Host
100.100.112.203
100.100.112.206
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 100.100.112.203 100.100.112.206
Details
Host script results:
|_clock-skew: mean: -15m14s, deviation: 0s, median: -15m14s
| nbstat: NetBIOS name: ITME1T6, NetBIOS user: <unknown>, NetBIOS MAC: b0:83:fe:a5:19:4c (Dell)
| Names:
| ITME1T6<20> Flags: <unique><active>
| IT<00> Flags: <group><active>
| ITME1T6<00> Flags: <unique><active>
| IT<1e> Flags: <group><active>
| IT<1d> Flags: <unique><active>
|_ \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| smb-os-discovery:
| OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
| OS CPE: cpe:/o:microsoft:windows_8.1::-
| Computer name: ITME1T6
| NetBIOS computer name: ITME1T6\x00
| Workgroup: IT\x00
|_ System time: 2018-06-29T12:31:40+05:30
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 100.100.112.206
NSE: Script Post-scanning.
Initiating NSE at 12:47
Completed NSE at 12:47, 0.00s elapsed
Initiating NSE at 12:47
Completed NSE at 12:47, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 121.03 seconds
Raw packets sent: 3055 (136.956KB) | Rcvd: 1035 (42.508KB)


Zenmap
Scan Tools Profile Help
Target: 100.100.112.203 100.100.112.206
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 100.100.112.203 100.100.112.206
Hosts
Services
OS Host
100.100.112.203
100.100.112.206
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v 100.100.112.203 100.100.112.206
Details
Starting Nmap 7.50 (https://nmap.org) at 2018-06-29 12:59 India Standard Time
NSE: Loaded 144 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:59
Completed NSE at 12:59, 0.00s elapsed
Initiating NSE at 12:59
Completed NSE at 12:59, 0.00s elapsed
Initiating ARP Ping Scan at 12:59
Scanning 2 hosts [1 port/host]
Completed ARP Ping Scan at 12:59, 0.05s elapsed (2 total hosts)
Initiating SYN Stealth Scan at 12:59
Scanning 2 hosts [65535 ports/host]
Discovered open port 1025/tcp on 100.100.112.203
Discovered open port 445/tcp on 100.100.112.206
Discovered open port 445/tcp on 100.100.112.203
Discovered open port 3389/tcp on 100.100.112.203
Discovered open port 139/tcp on 100.100.112.203
Discovered open port 135/tcp on 100.100.112.203
Discovered open port 1027/tcp on 100.100.112.203
Discovered open port 139/tcp on 100.100.112.206
Discovered open port 135/tcp on 100.100.112.206
Discovered open port 1030/tcp on 100.100.112.203
Discovered open port 1031/tcp on 100.100.112.203
Discovered open port 1026/tcp on 100.100.112.203
Discovered open port 7779/tcp on 100.100.112.203
Discovered open port 1029/tcp on 100.100.112.203
Discovered open port 1028/tcp on 100.100.112.203