Network Scanning Practicals:

Open a blank terminal in kali linux, and type the follows:

netdiscover

Or

netdiscover –i <interface name>

Or

netdiscover –r <network range you want to scan>

Ex:

netdiscover

netdiscover –i eth0

netdiscover –r 192.168.0.0/24

Ping Sweeping techniques for Network Scanning with nmap

Open a blank terminal and type

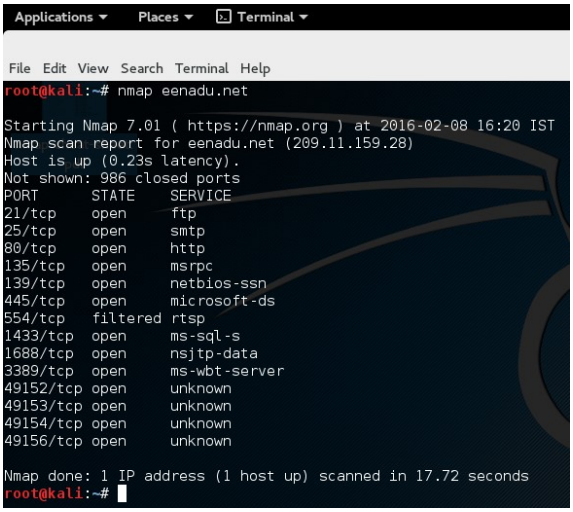
nmap –sn 192.168.0.0/24

Port Scanning Practical:

Regular Scan (syn stealth scan or half open scan):

nmap <target ip or domain>

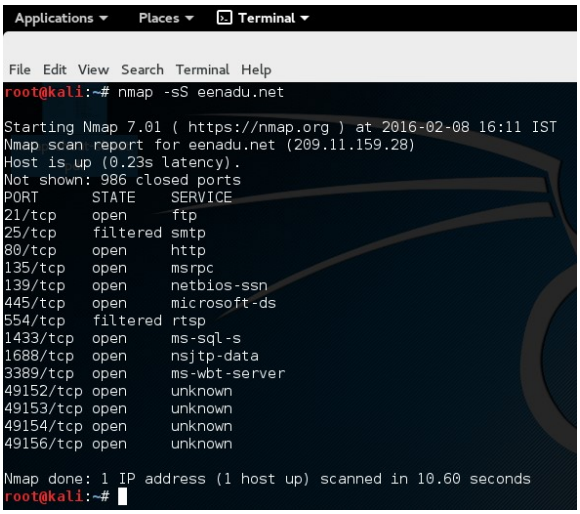
Ex: nmap 192.168.0.100 or nmap –sS example.com or nmap –sS 192.168.0.100 or nmap –sS example.com



```
Applications  Places  Terminal
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap eenadu.net

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 16:20 IST
Nmap scan report for eenadu.net (209.11.159.28)
Host is up (0.23s latency).
Not shown: 986 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
25/tcp    open     smtp
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   filtered rtsp
1433/tcp  open     ms-sql-s
1688/tcp  open     nsjtp-data
3389/tcp  open     ms-wbt-server
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49156/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
root@kali:~#
```



```
Applications  Places  Terminal
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sS eenadu.net

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 16:11 IST
Nmap scan report for eenadu.net (209.11.159.28)
Host is up (0.23s latency).
Not shown: 986 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   filtered rtsp
1433/tcp  open     ms-sql-s
1688/tcp  open     nsjtp-data
3389/tcp  open     ms-wbt-server
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49156/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 10.60 seconds
root@kali:~#
```

Note: Even if you take a domain name nmap won't scan the website it will scan the computer (server) hosting that website.

TCP connect scan (Full Connect Scan):

nmap –sT <target ip or domain>

Ex: nmap –sT example.com or nmap –sT 192.168.0.100

```
Applications  Places  Terminal                Mon 17:15
                                              root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sT todaypk.com

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:06 IST
Stats: 0:02:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.85% done; ETC: 17:10 (0:01:22 remaining)
Nmap scan report for todaypk.com (192.124.249.3)
Host is up (0.074s latency).
rDNS record for 192.124.249.3: cloudproxy10003.sucuri.net
Not shown: 997 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 526.36 seconds
root@kali:~#
```

OS Detection Scan:

Nmap –O <target ip or domain>

Ex: nmap –O example.com or nmap –O 192.168.0.100

```
Applications  Places  Terminal                Mon 16:23
                                              root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -O eenadu.net

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 16:22 IST
Nmap scan report for eenadu.net (209.11.159.28)
Host is up (0.24s latency).
Not shown: 986 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
25/tcp    open     smtp
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   filtered rtsp
1433/tcp  open     ms-sql-s
1688/tcp  open     nsjtp-data
3389/tcp  open     ms-wbt-server
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49156/tcp open     unknown
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|7|Vista|2012 (96%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::sp2 cp
e:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows Server 2008 R2 or Windows 8 (96%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (96%), Microso
ft Windows Server 2008 R2 (95%), Microsoft Windows 7 (93%), Windows Server 2008 R2 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Win
dows Server 2008 (93%), Windows Server 2012 (92%), Microsoft Windows Server 2008 R2 SP1 (90%), Microsoft Windows 7 SP1 (90%), Microsoft Wind
ows Server 2008 or 2008 Beta 3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.54 seconds
```

Service detection scan or version detection scan:

Ex: nmap –sV example.com or nmap –sV 192.168.0.100

```
Applications  Places  Terminal                Mon 16:16
                                              root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sV eenadu.net

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 16:14 IST
Nmap scan report for eenadu.net (209.11.159.28)
Host is up (0.26s latency).
Not shown: 986 closed ports
PORT      STATE    SERVICE            VERSION
21/tcp    open     ftp                FileZilla ftpd 0.9.41 beta
25/tcp    filtered smtp
80/tcp    open     http               Microsoft IIS httpd 7.5
135/tcp   open     msrpc              Microsoft Windows RPC
139/tcp   open     netbios-ssn        Microsoft Windows 98 netbios-ssn
445/tcp   open     microsoft-ds       Microsoft Windows Server 2008 R2 microsoft-ds
554/tcp   filtered rtsp
1433/tcp  open     ms-sql-s           Microsoft SQL Server 2008 R2 10.50.1600; RTM
1688/tcp  open     msrpc              Microsoft Windows RPC
3389/tcp  open     ssl/ms-wbt-server?
49152/tcp open     msrpc              Microsoft Windows RPC
49153/tcp open     msrpc              Microsoft Windows RPC
49154/tcp open     msrpc              Microsoft Windows RPC
49156/tcp open     msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows 98, Windows Server 2008 R2; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft
:windows_server_2008:r2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.14 seconds
```

UDP port scan:

Nmap –sU <target ip or domain>

Ex: nmap –sU example.com or nmap –sU 192.168.0.100

Custom port scanning:

Nmap –p <port range> <target ip or domain>

Ex: nmap –p 80 example.com or nmap –p 80-85 192.168.0.100 or

nmap –p 80,81,85,21,443 49.204.90.43

You can add –v at the end of any command to see the verbose (in detailed) information.

Aggressive scan:

Nmap –A <target ip of domain>

Ex: nmap –A example.com or nmap –A 192.168.0.100 –v

```
Applications ▾  Places ▾  Terminal ▾        Mon 16:09
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -A eenadu.net

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 16:01 IST
Nmap scan report for eenadu.net (209.11.159.28)
Host is up (0.24s latency).
Not shown: 986 closed ports
PORT      STATE    SERVICE           VERSION
21/tcp    open     ftp               FileZilla ftpd 0.9.41 beta
25/tcp    filtered smtp
80/tcp    open     http              Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 12 disallowed entries
| /AbinandhanaMandaraMala/ /adimages/ /App_Code/
| /App_Data/ /Bin/ /css/ /galleryjs/ /images/ /PE/ /sIFR/ /Taja-News/
|_/tickerbyks/
|_http-server-header: Microsoft-IIS/7.5
|_http-title: EENADU Online Edition - Telugu news paper
135/tcp   open     msrpc             Microsoft Windows RPC
139/tcp   open     netbios-ssn       Microsoft Windows 98 netbios-ssn
445/tcp   open     microsoft-ds      Microsoft Windows Server 2008 R2 microsoft-ds
554/tcp   filtered rtsp
1433/tcp  open     ms-sql-s          Microsoft SQL Server 2008 R2 10.50.1600.00; RTM
1688/tcp  open     msrpc             Microsoft Windows RPC
3389/tcp  open     ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=EENADUSECONDARY
| Not valid before: 2015-10-28T19:30:19
|_Not valid after:  2016-04-28T19:30:19
|_ssl-date: 2016-02-08T10:31:51+00:00; -1m19s from scanner time.
49152/tcp open     msrpc             Microsoft Windows RPC
49153/tcp open     msrpc             Microsoft Windows RPC
49154/tcp open     msrpc             Microsoft Windows RPC
49156/tcp open     msrpc             Microsoft Windows RPC
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|7|2012|Vista (96%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 c
pe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 R2 or Windows 8 (96%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (96%), Microso
ft Windows Server 2008 R2 (95%), Windows Server 2008 R2 (93%), Microsoft Windows 7 (92%), Windows Server 2012 (91%), Microsoft Windows Serve
```

```
Applications ▾  Places ▾  Terminal ▾        Mon 16:10
root@kali: ~
File  Edit  View  Search  Terminal  Help
Network Distance: 15 hops
Service Info: OSs: Windows, Windows 98, Windows Server 2008 R2; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft
:windows_server_2008:r2

Host script results:
| ms-sql-info:
|   Windows server name: EENADUSECONDARY
|   209.11.159.28\MSSQLSERVER:
|     Instance name: MSSQLSERVER
|     Version:
|       Service pack level: RTM
|       number: 10.50.1600.00
|       Product: Microsoft SQL Server 2008 R2
|       name: Microsoft SQL Server 2008 R2 RTM
|       Post-SP patches applied: false
|     TCP port: 1433
|     Named pipe: \\209.11.159.28\pipe\sql\query
|_    Clustered: false
|_nbstat: NetBIOS name: EENADUSECONDARY, NetBIOS user: <unknown>, NetBIOS MAC: a4:ba:db:37:f2:5e (Dell)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: EENADUSECONDARY
|   NetBIOS computer name: EENADUSECONDARY
|   Workgroup: WORKGROUP
|_  System time: 2016-02-08T16:01:52+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 (using port 1720/tcp)
HOP RTT       ADDRESS
1   19.65 ms  192.168.0.1
2   19.74 ms  49.204.0.1
3   25.63 ms  ras.beamtele.net (183.82.14.153)
4   16.36 ms  14.141.24.169.static-hyderabad.tcl.net.in (14.141.24.169)
```

```
5   ...
6   21.00 ms  ix-4-2.tcore1.CXR-Chennai.as6453.net (180.87.36.9)
7   57.58 ms  if-5-2.tcore1.SVW-Singapore.as6453.net (180.87.12.53)
8   57.58 ms  if-11-2.thar1.SVQ-Singapore.as6453.net (180.87.98.37)
9   57.58 ms  ae-6.r00.sngpsi05.sg.bb.gin.ntt.net (129.250.8.241)
10  57.61 ms  ae-10.r20.sngpsi05.sg.bb.gin.ntt.net (129.250.7.18)
11  229.50 ms ae-8.r22.snjsca04.us.bb.gin.ntt.net (129.250.3.48)
12  233.90 ms ae-40.r02.snjsca04.us.bb.gin.ntt.net (129.250.3.121)
13  233.91 ms xe-0-7-0-3.r02.snjsca04.us.ce.gin.ntt.net (128.241.219.186)
14  229.58 ms 205.234.0.170
15  234.42 ms 209.11.159.28

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 136.33 seconds
root@kali:~#
```

XMAS scan (FIN, PSH, URG Flags):

Nmap –sX <target ip or domain>

Ex: nmap –sX example.com or nmap –sX 192.168.0.100 –v

```
Applications ▾   Places ▾   Terminal ▾

File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sX 192.168.0.112

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.112
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 00:E0:4C:62:0A:BA (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
root@kali:~# nmap -sX 192.168.0.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.102
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.0.102 are closed
MAC Address: 74:DE:2B:90:31:D4 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
root@kali:~#
```

FIN scan (FIN Flag):

Nmap –sF <target ip or domain>

Ex: nmap –sF example.com or nmap –sF 192.168.0.100 –v

```
Applications ▾   Places ▾   Terminal ▾

File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sF 192.168.0.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.102
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.0.102 are closed
MAC Address: 74:DE:2B:90:31:D4 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
root@kali:~# nmap -sF 192.168.0.112

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.112
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 00:E0:4C:62:0A:BA (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

NULL scan (No Flags)

Nmap –sN <target ip or domain>

Ex: nmap –sN example.com or nmap –sN 192.168.0.100 –v

```
Applications ▾   Places ▾   Terminal ▾

File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sN 192.168.0.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.102
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.0.102 are closed
MAC Address: 74:DE:2B:90:31:D4 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
root@kali:~# nmap -sN 192.168.0.112

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:18 IST
Nmap scan report for 192.168.0.112
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE          SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 00:E0:4C:62:0A:BA (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
root@kali:~#
```

If you get any error saying host may be down or disabled icmp try adding –Pn to the command

Ex: nmap –sT –Pn example.com

You can also perform traceroute scan with nmap

Nmap --traceroute <target ip or domain>

Ex: nmap --traceroute example.com or nmap --traceroute 192.168.0.100 –v

```
Applications ▾   Places ▾   Terminal ▾   Mon 16:1
                                        root@kal
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap --traceroute eenadu.net

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 16:12 IST
Nmap scan report for eenadu.net (209.11.159.28)
Host is up (0.23s latency).
Not shown: 986 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   filtered rtsp
1433/tcp  open     ms-sql-s
1688/tcp  open     nsjtp-data
3389/tcp  open     ms-wbt-server
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49156/tcp open     unknown

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   5.23 ms   192.168.0.1
2   6.52 ms   49.204.0.1
3   5.50 ms   ras.beamtele.net (183.82.14.153)
4   6.26 ms   14.141.24.169.static-hyderabad.tcl.net.in (14.141.24.169)
5   ...
6   20.74 ms  ix-4-2.tcore1.CXR-Chennai.as6453.net (180.87.36.9)
7   47.06 ms  if-5-2.tcore1.SVW-Singapore.as6453.net (180.87.12.53)
8   49.72 ms  if-11-2.thar1.SVQ-Singapore.as6453.net (180.87.98.37)
9   48.81 ms  ae-6.r00.sngpsi05.sg.bb.gin.ntt.net (129.250.8.241)
10  48.74 ms  ae-10.r20.sngpsi05.sg.bb.gin.ntt.net (129.250.7.18)
11  230.68 ms ae-8.r22.snjsca04.us.bb.gin.ntt.net (129.250.3.48)
12  227.48 ms ae-40.r02.snjsca04.us.bb.gin.ntt.net (129.250.3.121)
13  231.00 ms xe-0-7-0-3.r02.snjsca04.us.ce.gin.ntt.net (128.241.219.186)
14  227.40 ms 205.234.0.170
15  221.57 ms 209.11.159.28
```

Installing Nessus Vulnerability Scanner In Kali Linux

Step 1: search for "obtain an activation code" in google

Step 2: click on the first link

Step 3: Go for home license and register.

Step 4: After registering download linux nessus version .deb package(32 or 64bit)

Step 5: Go to download location and execute

dpkg -i <filename.deb>

Configuring Nessus IN kali linux

Step 1: execute

/etc/init.d/nessusd start

and then go to your favorite browser and open

https://127.0.0.1:8834/

Step 2: enter Activation Code if it is asking you.

Step 3: Create username and password in the next prompt.

Step 4: Download nessus plugins by clicking the button.

Step 5: wait till the process completes (completion depends on your internet speed) once completed your nessus in ready to go.

Enumeration Practicals:

Netbios Enumeration:

In windows execute the following command in terminal

nbtstat –A

```
G:\Users\SAM>nbtstat -A 192.168.1.7

Ethernet:
Node IpAddress: [169.254.185.160] Scope Id: []

    Host not found.

Ethernet 2:
Node IpAddress: [169.254.123.0] Scope Id: []

    Host not found.

Local Area Connection:
Node IpAddress: [192.168.1.4] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    KUMAR           <00>  UNIQUE      Registered
    KUMAR           <20>  UNIQUE      Registered
    KUMAR7          <00>  GROUP       Registered
    KUMAR7          <1C>  GROUP       Registered
    KUMAR7          <1E>  GROUP       Registered
    KUMAR7          <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
    KUMAR7          <1B>  UNIQUE      Registered

    MAC Address = 08-00-27-82-FF-00


G:\Users\SAM>
```

The above command will disclose the connected devices NETBIOS names to the attacker

nbtstat –c

```
G:\Users\SAM>nbtstat -c

Ethernet:
Node IpAddress: [169.254.185.160] Scope Id: []

    No names in cache

Ethernet 2:
Node IpAddress: [169.254.123.0] Scope Id: []

    No names in cache

Local Area Connection:
Node IpAddress: [192.168.1.4] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name             Type       Host Address    Life [sec]
    ------------------------------------------------------------
    KUMAR          <20>  UNIQUE          192.168.1.7         444
    KUMAR7         <00>  GROUP           192.168.1.7         389

G:\Users\SAM>
```

To see the cached information of NETBIOS

SMB Enumeration with SMBCLIENT TOOL

smbclient –L <target ip> -N

```
root@kali:~# smbclient -L 192.168.1.16 -N
Domain=[KUMAR7] OS=[Windows Server 2003 R2 3790 Service Pack 2] Server=[Windows Server 2003 R2 5.2]

        Sharename       Type      Comment
        ---------       ----      -------
        C$              Disk      Default share
        Share           Disk
        IPC$            IPC       Remote IPC
        ADMIN$          Disk      Remote Admin
        SYSVOL          Disk      Logon server share
        NETLOGON        Disk      Logon server share
Domain=[KUMAR7] OS=[Windows Server 2003 R2 3790 Service Pack 2] Server=[Windows Server 2003 R2 5.2]

        Server               Comment
        ---------            -------
        KUMAR

        Workgroup            Master
        ---------            -------
        KUMAR7               KUMAR
```

For Linux Enumeration:

enum4linux -v <target ip>

Nmap enumeration commands:

Execute locate *.nse|grep enum

To findout the enumeration scripts of nmap and use them as enumerator like below example

nmap --script=<script name> --script-args=unsafe=1 <target ip>

```
root@kali:~# nmap -p445 192.168.0.132 --script=smb-mbenum.nse

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:17 IST
Nmap scan report for 192.168.0.132
Host is up (0.00025s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:82:FF:00 (Cadmus Computer Systems)

Host script results:
| smb-mbenum:
|   DFS Root
|     KUMAR  5.2
|   Domain Controller
|     KUMAR  5.2
|   Master Browser
|     KUMAR  5.2
|   Server service
|     KUMAR  5.2
|   Time Source
|     KUMAR  5.2
|   Windows NT/2000/XP/2003 server
|     KUMAR  5.2
|   Workstation
|_    KUMAR  5.2

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

SMB Protocol Logged On users Enumeration With NMAP Scripts

```
root@kali:~# nmap -p445 192.168.0.132 --script=smb-enum-sessions.nse

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:10 IST
Nmap scan report for 192.168.0.132
Host is up (0.00020s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:82:FF:00 (Cadmus Computer Systems)

Host script results:
| smb-enum-sessions:
|   Users logged in
|_    KUMAR7\Administrator since <unknown>

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

SMB Protocol Shares Enumeration With NMAP Script

```
root@kali:~# nmap --script=smb-enum-shares.nse 192.168.0.132 -p445,139

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:07 IST
Nmap scan report for 192.168.0.132
Host is up (0.00028s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:82:FF:00 (Cadmus Computer Systems)

Host script results:
| smb-enum-shares:
|   ADMIN$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   C$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   IPC$
|     Anonymous access: READ <not a file share>
|     Current user ('guest') access: READ <not a file share>
|   NETLOGON
|     Anonymous access: <none>
|     Current user ('guest') access: READ
|   SYSVOL
|     Anonymous access: <none>
|     Current user ('guest') access: READ
|   Share
|     Anonymous access: <none>
|_    Current user ('guest') access: READ

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

SSH Protocol Algorithms Enumeration With NMAP script

```
root@kali:~# nmap --script=ssh2-enum-algos.nse 192.168.0.131 --open -p22

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:05 IST
Nmap scan report for 192.168.0.131
Host is up (0.00021s latency).
PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (7)
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (3)
|       ssh-rsa
|       ssh-dss
|       ecdsa-sha2-nistp256
|   encryption_algorithms: (13)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       aes192-cbc
|       aes256-cbc
|       arcfour
|       rijndael-cbc@lysator.liu.se
|   mac_algorithms: (11)
```