Active Information Gathering Module (OSCP)

Direct interaction with target services , to gather information .

1. DNS Enumeration :

DNS is basically that translates domain names to IP addresses.

Interacting with it :

```
┌──(root㉿kali)-[/home/kali]
└─# host www.megacorpone.com
www.megacorpone.com has address 149.56.244.87

┌──(root㉿kali)-[/home/kali]
└─# host -t mx megacorpone.com
megacorpone.com mail is handled by 20 spool.mail.gandi.net.
megacorpone.com mail is handled by 10 fb.mail.gandi.net.
megacorpone.com mail is handled by 50 mail.megacorpone.com.
megacorpone.com mail is handled by 60 mail2.megacorpone.com.

┌──(root㉿kali)-[/home/kali]
└─# host -t txt megacorpone.com
megacorpone.com descriptive text "Try Harder"
megacorpone.com descriptive text "google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA"
```

Host command to see IP addresses .

Specify –t after to give an argument for type of record we want

For example shown above are –t mx for mail server records

And –t txt for text records

2. Forward Lookup Bruteforce :

Trial and error technique to find valid information

We can use common wordlists of hostname . Example :

Our wordlist :

```
File  Actions  Edit  View  Help
  GNU nano 6.0
www
ftp
mail
owa
proxy
router
```

Now our bash one-liner to do the task :

```
┌──(root㉿kali)-[/home/kali]
└─# for i in $(cat list.txt) ; do host $i.megacorpone.com; done
www.megacorpone.com has address 149.56.244.87
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
mail.megacorpone.com has address 51.222.169.212
Host owa.megacorpone.com not found: 3(NXDOMAIN)
Host proxy.megacorpone.com not found: 3(NXDOMAIN)
router.megacorpone.com has address 51.222.169.214
```

3. Reverse Lookup Bruteforce .

Get hostname for each IP:

```
┌──(root㉿kali)-[/home/kali]
└─# for ip in $(seq 50 100); do host 38.100.193.$ip; done | grep -v "not found"
66.193.100.38.in-addr.arpa domain name pointer syslog.megacorpone.com.
69.193.100.38.in-addr.arpa domain name pointer beta.megacorpone.com.
70.193.100.38.in-addr.arpa domain name pointer ns1.megacorpone.com.
72.193.100.38.in-addr.arpa domain name pointer admin.megacorpone.com.
73.193.100.38.in-addr.arpa domain name pointer mail2.megacorpone.com.
76.193.100.38.in-addr.arpa domain name pointer www.megacorpone.com.
77.193.100.38.in-addr.arpa domain name pointer vpn.megacorpone.com.
80.193.100.38.in-addr.arpa domain name pointer ns2.megacorpone.com.
84.193.100.38.in-addr.arpa domain name pointer mail.megacorpone.com.
85.193.100.38.in-addr.arpa domain name pointer snmp.megacorpone.com.
89.193.100.38.in-addr.arpa domain name pointer siem.megacorpone.com.
90.193.100.38.in-addr.arpa domain name pointer ns3.megacorpone.com.
91.193.100.38.in-addr.arpa domain name pointer router.megacorpone.com.
```

4. DNS Zone Transfers :

Is basically database replication between related DNS servers.

In this the “zone” file is copied from a master dns to slave dns ,

Zone file has all the dns names .

We can retrieve that file .

We can have corporate network laid out on a silver platter.

So for this first enumerate name servers :

```
┌──(root㉿kali)-[/home/kali]
└─# host -t ns megacorpone.com
megacorpone.com name server ns3.megacorpone.com.
megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
```

Then perform a zone transfer like this :

```
┌──(root㉿kali)-[/home/kali]
└─# host -l megacorpone.com ns2.megacorpone.com
Using domain server:
Name: ns2.megacorpone.com
Address: 51.222.39.63#53
Aliases:

megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
admin.megacorpone.com has address 51.222.169.208
beta.megacorpone.com has address 51.222.169.209
fs1.megacorpone.com has address 51.222.169.210
intranet.megacorpone.com has address 51.222.169.211
mail.megacorpone.com has address 51.222.169.212
mail2.megacorpone.com has address 51.222.169.213
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
ns3.megacorpone.com has address 66.70.207.180
router.megacorpone.com has address 51.222.169.214
siem.megacorpone.com has address 51.222.169.215
snmp.megacorpone.com has address 51.222.169.216
support.megacorpone.com has address 51.222.169.218
syslog.megacorpone.com has address 51.222.169.217
test.megacorpone.com has address 51.222.169.219
vpn.megacorpone.com has address 51.222.169.220
www.megacorpone.com has address 149.56.244.87
www2.megacorpone.com has address 149.56.244.87
```

Other relevant tools in kali linux :

-> DNSRecon :

Advanced and modern , written in python :

Lets perform a DNS zone transfer using this :

```
┌──(root㉿kali)-[/home/kali]
└─# dnsrecon -d megacorpone.com -t axfr
[*] Checking for Zone Transfer for megacorpone.com name servers
```

Results :

```
[*]      TXT Try Harder
[*]      TXT google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA
[*]      MX @.megacorpone.com fb.mail.gandi.net 217.70.178.217
[*]      MX @.megacorpone.com fb.mail.gandi.net 217.70.178.215
[*]      MX @.megacorpone.com fb.mail.gandi.net 217.70.178.216
[*]      MX @.megacorpone.com spool.mail.gandi.net 217.70.178.1
[*]      A admin.megacorpone.com 51.222.169.208
[*]      A beta.megacorpone.com 51.222.169.209
[*]      A fs1.megacorpone.com 51.222.169.210
[*]      A intranet.megacorpone.com 51.222.169.211
[*]      A mail.megacorpone.com 51.222.169.212
[*]      A mail2.megacorpone.com 51.222.169.213
[*]      A ns1.megacorpone.com 51.79.37.18
[*]      A ns2.megacorpone.com 51.222.39.63
[*]      A ns3.megacorpone.com 66.70.207.180
[*]      A router.megacorpone.com 51.222.169.214
[*]      A siem.megacorpone.com 51.222.169.215
[*]      A snmp.megacorpone.com 51.222.169.216
[*]      A support.megacorpone.com 51.222.169.218
[*]      A syslog.megacorpone.com 51.222.169.217
[*]      A test.megacorpone.com 51.222.169.219
```

Bruteforce subdomains using dnsrecon :

We will use the previously created wordlist here:

```
┌──(root㉿kali)-[/home/kali]
└─# dnsrecon -d megacorpone.com -D /home/kali/list.txt -t brt
[*] Using the dictionary file: /home/kali/list.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorpone.com...
[+]      A www.megacorpone.com 149.56.244.87
[+]      A mail.megacorpone.com 51.222.169.212
[+]      A router.megacorpone.com 51.222.169.214
[+] 3 Records Found
```

-> DNSenum : it basically does all the above things in one command and give us data we can use .

```
┌──(root㉿kali)-[/home/kali]
└─# dnsenum zonetransfer.me
dnsenum VERSION:1.2.6

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         7200     IN    A        5.196.105.14


Name Servers:
______________

nsztm2.digi.ninja.                       10800    IN    A        34.225.33.2
nsztm1.digi.ninja.                       10799    IN    A        81.4.108.41


Mail (MX) Servers:
___________________
```

Port Scanning :

Inspecting running TCP and UDP ports on a target system and what services are running and other data .

We can use netcat to do some small or basic TCP scan like this ,

For this module i will be using metasploitable .

TCP scanning :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nv -w 1 -z 192.168.1.8 20-30
(UNKNOWN) [192.168.1.8] 25 (smtp) open
(UNKNOWN) [192.168.1.8] 23 (telnet) open
(UNKNOWN) [192.168.1.8] 22 (ssh) open
(UNKNOWN) [192.168.1.8] 21 (ftp) open
```

Here i used –nv for verbosity –w for timeout which i set to 1 and –z for empty requests.

And we found 4 open ports .

UDP scanning :

Syntax is same as above just add –u option for UDP .

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nv -u -w 1 -z 192.168.1.8 160-162
```

Port Scanning with NMAP :

Most popular tool .

Basic scan of top 1000 ports:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 06:35 EDT
Nmap scan report for 192.168.1.8
Host is up (0.0041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:BC:ED:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Syn scan : it has incomplete TCP handshake .

Basic stealth scan

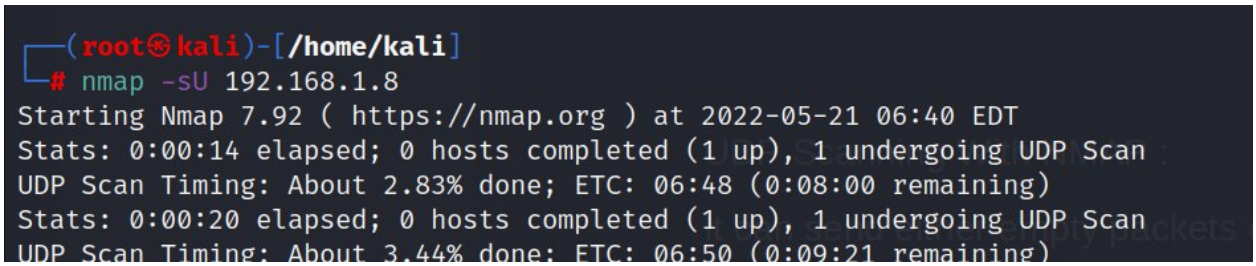
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 06:37 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00058s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

TCP connect scan :

Full 3 way handshake , takes extra time .

UDP Scanning With NMAP :

It can send either empty packets or specified protocol packets for well known UDP ports,



These UDP scans can take a lot of time

Can be mixed with a SYN scan :

Network Sweeping :

To deal with large volume of hosts , use this technique ,

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.1-254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 06:45 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 253 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 34.19% done; ETC: 06:46 (0:00:12 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 253 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 44.07% done; ETC: 06:46 (0:00:15 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
MAC Address: BC:62:D2:1A:2A:18 (Genexis International)
Nmap scan report for 192.168.1.2
Host is up (0.020s latency).
MAC Address: 64:A2:00:C5:34:CF (Xiaomi Communications)
Nmap scan report for 192.168.1.5
Host is up (0.036s latency).
MAC Address: 8C:AA:CE:54:0C:3B (Xiaomi Communications)
Nmap scan report for 192.168.1.7
Host is up (0.034s latency).
MAC Address: 46:47:0D:75:5B:D3 (Unknown)
Nmap scan report for 192.168.1.8
```

I have comprehensive notes for NMAP in github repository so i won't be giving this section much time .

Masscan :

Cam scan entire subnet easily as it is fasttt af .

Good for Class A and B subnet .

```
┌──(root㉿kali)-[/home/kali]
└─# masscan -p80 192.168.1.0/24 --rate=1000 -e eth0 --router-ip 192.168.1.1
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-05-21 10:55:18 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.1.8
Discovered open port 80/tcp on 192.168.1.10
```

SMB Enumeration :

It is quite vulnerable ,

Refers to as server message block

Netbios service scan – listens on port 139

And smb runs on 445

Nmap scan :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 139,445 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:25 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00030s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BC:ED:E4 (VMware)
```

NBTSCAN :

```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan -r 192.168.1.8
Doing NBT name scan for addresses from 192.168.1.8

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------
192.168.1.8      METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

Using nmap nse scripts : to run some common scripts

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 139,445 -sC 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:27 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.09% done; ETC: 07:28 (0:00:01 remaining)
Nmap scan report for 192.168.1.8
Host is up (0.00020s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BC:ED:E4 (VMware)

Host script results:
|_clock-skew: mean: 1h35m44s, deviation: 2h49m43s, median: -24m16s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-05-21T07:03:33-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

To see scripts for smb :

```
┌──(root㉿kali)-[/home/kali]
└─# ls -l /usr/share/nmap/scripts/smb*
-rw-r--r-- 1 root root  3753 Jan 18 09:54 /usr/share/nmap/scripts/smb2-capabilities.nse
-rw-r--r-- 1 root root  2689 Jan 18 09:54 /usr/share/nmap/scripts/smb2-security-mode.nse
-rw-r--r-- 1 root root  1408 Jan 18 09:54 /usr/share/nmap/scripts/smb2-time.nse
-rw-r--r-- 1 root root  5269 Jan 18 09:54 /usr/share/nmap/scripts/smb2-vuln-uptime.nse
-rw-r--r-- 1 root root 45138 Jan 18 09:54 /usr/share/nmap/scripts/smb-brute.nse
-rw-r--r-- 1 root root  5289 Jan 18 09:54 /usr/share/nmap/scripts/smb-double-pulsar-backdoor.nse
-rw-r--r-- 1 root root  4840 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-domains.nse
-rw-r--r-- 1 root root  5971 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-groups.nse
-rw-r--r-- 1 root root  8043 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-processes.nse
-rw-r--r-- 1 root root 27274 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-services.nse
-rw-r--r-- 1 root root 12097 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-sessions.nse
-rw-r--r-- 1 root root  6923 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-shares.nse
-rw-r--r-- 1 root root 12527 Jan 18 09:54 /usr/share/nmap/scripts/smb-enum-users.nse
-rw-r--r-- 1 root root  1706 Jan 18 09:54 /usr/share/nmap/scripts/smb-flood.nse
-rw-r--r-- 1 root root  7471 Jan 18 09:54 /usr/share/nmap/scripts/smb-ls.nse
-rw-r--r-- 1 root root  8758 Jan 18 09:54 /usr/share/nmap/scripts/smb-mbenum.nse
```

Smb-os-discovery script :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 139,445 --script=smb-os-discovery 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:30 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00027s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BC:ED:E4 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-05-21T07:06:31-04:00
```

To check for known smb vulnerabilities :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 139,445 --script=smb-vuln* 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:32 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00028s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BC:ED:E4 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
```

NFS Enumeration :

Basically network shared folders and files .

Scanning for NFS shares ,

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 111 --script=rpcinfo 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:37 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00023s latency).

PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      49332/udp   mountd
|   100005  1,2,3      51610/tcp   mountd
|   100021  1,3,4      33217/udp   nlockmgr
|   100021  1,3,4      40630/tcp   nlockmgr
|   100024  1          35437/udp   status
|_  100024  1          38184/tcp   status
MAC Address: 00:0C:29:BC:ED:E4 (VMware)
```

Now we will use nmap nse scripts for NFS further enumeration

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 111 --script=nfs* 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:39 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00025s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-statfs:
|   Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /           7282168.0  1498176.0  5416992.0  22%   2.0T         32000
| nfs-showmount:
|_  / *
| nfs-ls: Volume /
|   access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION  UID  GID  SIZE   TIME                 FILENAME
| drwxr-xr-x  0    0    4096   2012-05-14T03:35:33  bin
| drwxr-xr-x  0    0    4096   2010-04-16T06:16:02  home
| drwxr-xr-x  0    0    4096   2010-03-16T22:57:40  initrd
| lrwxrwxrwx  0    0    32     2010-04-28T20:26:18  initrd.img
| drwxr-xr-x  0    0    4096   2012-05-14T03:35:22  lib
| drwx------  0    0    16384  2010-03-16T22:55:15  lost+found
| drwxr-xr-x  0    0    4096   2010-03-16T22:55:52  media
| drwxr-xr-x  0    0    4096   2010-04-28T20:16:56  mnt
| drwxr-xr-x  0    0    4096   2012-05-14T01:54:53  sbin
| drwxr-xr-x  0    0    4096   2010-04-28T04:06:37  usr
|_
MAC Address: 00:0C:29:BC:ED:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

Lets mount these shares :

```
┌──(root㉿kali)-[/home/kali]
└─# mount -o nolock 192.168.1.8:/home /home/kali/mounted

┌──(root㉿kali)-[/home/kali]
└─# ls
active-directory  Desktop      final.txt              LinEnum   oscp                Pictures          shell.aspx          Videos
base64.txt        Documents    fsocity.dic            list.txt  output.txt          PowerSploit       shell.php           wget.exe
bind_shell.crt    Downloads    fsocity.dic.3          mona      pass.txt            printspoofer      sorted.txt          Windows-Exploit-Suggester
bind_shell.key    encoded.txt  gatekeeper.exe         mounted   passwords.txt       PrintSpoofer.exe  ssh-backdoor        wordlists
bind_shell.pem    enum4linux   hello_world.c          Music     paused.conf         Public            stuff
chatserver.exe    essfunc.dll  instagram-hacking-tool  nfs      PEASS-ng            SecLists          tcp_22_ssh_nmap.txt
CMSmap            evil-winrm   joomlavs               nishang   Pentest-Cheatsheets secretfile.txt    Templates
cred              fela.txt     key-1-of-3.txt         notes     php-reverse-shell.php seeker          thesecret.txt

┌──(root㉿kali)-[/home/kali]
└─# cd mounted

┌──(root㉿kali)-[/home/kali/mounted]
└─# ls
ftp  msfadmin  service  user
```

SMTP –Simple Mail Transfer Protocol – Enumeration

Can be good to gain some usernames

Runs on port 25 . Use VRFY to verify if a user exist on the system or not

```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.8 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VRFY kalra
550 5.1.1 <kalra>: Recipient address rejected: User unknown in local recipient table
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
```

SNMP –simple network management protocol –Enumeration .

Is based on UDP .

Is somehow vulnerable .

MIB tree concept – it is basically management information base that is a database for information related to network management .

To scan for it :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 161 -sU 192.168.1.8
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 07:54 EDT
```

Using onesixtyone tool :

To bruteforce attack against list of IP :

Generating community strings :

```
┌──(root㉿kali)-[/home
└─# cat > community <<
heredoc> public
heredoc> private
heredoc> manager
heredoc> EOF

┌──(root㉿kali)-[/home
└─# ls
active-directory  Desk
base64.txt        Docu
bind_shell.crt    Down
bind_shell.key    encc
bind_shell.pem    enur
chatserver.exe    essi
CMSmap            evil
community         fela
cred              fina

┌──(root㉿kali)-[/home
└─# cat community
public
private
manager
```

Generating a list of ip :

```
┌──(root㉿kali)-[/home/kali]
└─# for ip in $(seq 1 254); do echo 192.168.1.$ip; done > ips

┌──(root㉿kali)-[/home/kali]
└─# cat ips
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.4
```

Then usage of tool :

```
┌──(root㉿kali)-[/home/kali]
└─# onesixtyone -c community -i ips
Scanning 254 hosts, 4 communities
^C
```

Now we can query MIB data .

Enumerating the Entire MIB tree :