

Enumeration

Like, Reconnaissance is the method of collecting information about a target system without alerting it, also known as Footprinting, it is the first step in any form of hacking that helps in understanding the target system and identify potential attack vectors & vulnerabilities followed by network scanning to identify hosts, ports and services in the network.

Enumeration is when you try and connect to the system and do deliberate actions to gather more information.

“Enumeration is the process of actively connecting to and gathering detailed information about systems and services on a network. It goes beyond scanning and focuses on extracting specific details like usernames, shared resources, network shares, and system roles.”

To Gain access to the inner workings of a network, identify vulnerabilities, and understand the structure of the target system.

Scanning vs Enumeration

While scanning involves finding open ports and services, enumeration digs deeper to obtain actual data from these services.

My Network for this Activity

Windows Server 2022 – DC – 192.168.1.1/24

Windows Client 10 – Dmember – DHCP from Server

Debian 13 – 192.168.1.240/24

Kali – 192.168.1.250/24

NetBIOS Enumeration

Confirm the target Windows machine has file and printer sharing enabled and NetBIOS over TCP/IP running.

From your Kali Linux:

```
nbtscan -r 192.168.1.0/24
```

+ This command scans the specified network range for NetBIOS names.

Enumeration

- + The output typically shows computer names, MAC addresses, and workgroup information
- + This kind of information is valuable for attackers trying to understand the network structure.

Outcome

```
(nitheesh@kali)~$  
$ smbclient -L 192.168.1.240  
Password for [WORKGROUP\nitheesh]:  
  
Sharename      Type           Comment  
-----  
print$         Disk          Printer Drivers  
shared         Disk          IPC Service (Debian Samba Server)  
IPC$           IPC           Home Directories  
nobody         Disk          Home Directories  
Reconnecting with SMB1 for workgroup listing.  
smbcli_negprot_smb1_done: No compatible protocol selected by server.  
Protocol negotiation to server 192.168.1.240 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE  
Unable to connect with SMB1 -- no workgroup available
```

```
(nitheesh@kali)~$  
$ smbclient -L //192.168.1.240  
Password for [WORKGROUP\nitheesh]:  
  
Sharename      Type           Comment  
-----  
print$         Disk          Printer Drivers  
shared         Disk          IPC Service (Debian Samba Server)  
IPC$           IPC           Home Directories  
nobody         Disk          Home Directories  
Reconnecting with SMB1 for workgroup listing.  
smbcli_negprot_smb1_done: No compatible protocol selected by server.  
Protocol negotiation to server 192.168.1.240 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE  
Unable to connect with SMB1 -- no workgroup available  
  
(nitheesh@kali)~$  
$ smbclient -L //192.168.1.1  
Password for [WORKGROUP\nitheesh]:  
Anonymous login successful  
  
Sharename      Type           Comment  
-----  
print$         Disk          Printer Drivers  
shared         Disk          IPC Service (Debian Samba Server)  
IPC$           IPC           Home Directories  
nobody         Disk          Home Directories  
Reconnecting with SMB1 for workgroup listing.  
do_connect: Connection to 192.168.1.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)  
Unable to connect with SMB1 -- no workgroup available
```

```
(nitheesh@kali)~$  
$ nbtscan -r 192.168.1.0/24  
Doing NBT name scan for addresses from 192.168.1.0/24  
  
IP address    NetBIOS Name  Server  User      MAC address  
-----  
192.168.1.1   SWANSEA-DC    <server> <unknown> 00:0c:29:77:d4:b7  
192.168.1.240 SWANSEA-DC    <server> DEBIAN-NETBIOS 00:00:00:00:00:00  
192.168.1.250 <unknown>     <unknown> <unknown>  
192.168.1.235 Sendto failed: Permission denied  
  
(nitheesh@kali)~$  
$ enum4linux -a 192.168.1.1  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov 11 09:35:14 2024  
  
===== ( Target Information ) =====  
Target ..... 192.168.1.1  
RID Range ..... 500-550,1000-1050  
Username ..... ''  
Password ..... ''  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
  
===== ( Enumerating Workgroup/Domain on 192.168.1.1 ) =====  
[+] Got domain/workgroup name: NITHEESH  
  
===== ( Nbtstat Information for 192.168.1.1 ) =====  
Looking up status of 192.168.1.1  
SWANSEA-DC    <00> - M <ACTIVE> Workstation Service  
NITHEESH      <00> - <GROUP> M <ACTIVE> Domain/Workgroup Name  
NITHEESH      <1c> - <GROUP> M <ACTIVE> Domain Controllers  
NITHEESH      <1b> - M <ACTIVE> Domain Master Browser  
SWANSEA-DC    <20> - M <ACTIVE> File Server Service  
  
MAC Address = 00-0C-29-77-D4-B7
```

Enumeration

```
(nitheesh@kali)~$ ping 192.168.1.240
PING 192.168.1.240 (192.168.1.240) 56(84) bytes of data:
64 bytes from 192.168.1.240: icmp_seq=1 ttl=64 time=0.936 ms
64 bytes from 192.168.1.240: icmp_seq=2 ttl=64 time=1.51 ms
64 bytes from 192.168.1.240: icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from 192.168.1.240: icmp_seq=4 ttl=64 time=1.92 ms
64 bytes from 192.168.1.240: icmp_seq=5 ttl=64 time=0.919 ms
64 bytes from 192.168.1.240: icmp_seq=6 ttl=64 time=0.815 ms
64 bytes from 192.168.1.240: icmp_seq=7 ttl=64 time=0.755 ms
^C
--- 192.168.1.240 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 0.755/1.133/1.919/0.395 ms

(nitheesh@kali)~$ nmblookup -A 192.168.1.240
Looking up status of 192.168.1.240
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE>
               <00> - B <ACTIVE>
               <03> - B <ACTIVE>
               <20> - B <ACTIVE>
NITHEESH.NOSS <00> - <GROUP> B <ACTIVE>
NITHEESH.NOSS <1d> - B <ACTIVE>
NITHEESH.NOSS <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-00-00-00-00-00
```

Discussion: Discuss the risks of leaving NetBIOS enabled and how this can expose sensitive network information, such as usernames and shared resources.

If you are not getting the desired outcome as shown in the screenshot (example), you need to check if NETBIOS/ SAMBA Service is enabled.

To Check that, in your Windows Command Prompt, type:

nbtstat -n

If not enabled, follow the instructions from your lecturer (This is why it is important to attend the lecture sessions!!!)

Similarly for other Services to Enumerate, Check if the Services are enabled and running.

In Windows Server – Powershell

NetBIOS: nbtstat -n

should show active NetBIOS names.

SNMP: Get-Service -Name SNMP

DNS: nslookup

SMTP: telnet localhost 25 should connect to the SMTP service.

RPC: Run rpcinfo -p on the server

check Services for Remote Procedure Call status.

If SNMP Service is not installed, If not enabled, follow the instructions from your lecturer (This is why it is important to attend the lecture sessions!!!)

Enumeration

```
snmpwalk -v 2c -c public 192.168.1.1
```

Commands for other Services like:

For DNS

```
dig @192.168.1.1 nitheesh.noss any
```

For SMTP

```
telnet 192.168.1.1 25
```

For RPC

```
rpcclient -U "" 192.168.1.1
```