Enumeration

Enumeration is the process of systematically probing a target network or system to gather detailed information about its resources, services, and configurations. It involves actively connecting to and interacting with the system to identify usernames, network shares, services, and other sensitive information, which can be leveraged for further attacks or security assessments.

Enumeration typically follows the scanning phase and involves techniques that extract data to build a more detailed picture of the target's structure and weaknesses. It is a crucial step in both offensive security (like penetration testing) and defensive security (like vulnerability assessments). Some common types of enumeration include:

- **Network enumeration**: Discovering hosts, IP addresses, and services.
- **Service enumeration**: Identifying open ports and the services running on them.
- **User enumeration**: Listing user accounts, group memberships, and associated privileges.

Tools used for Enumeration:

- **Nmap**: For network discovery and service enumeration.
- **NetBIOS**: For enumerating resources on a network like shared folders.
- **SNMP enumeration**: To gather data from devices via the Simple Network Management Protocol.
- **LDAP enumeration**: For directory services.

It's an essential phase of an attack where information is collected to plan further exploitation or assess system security.

What and all can be gathered:

1. Network Information

- **Active Hosts**: Identifying live systems in a network.
- **Open Ports**: Finding which ports are open and listening.
- **Running Services**: Identifying services running on open ports (e.g., FTP, SSH, HTTP).
- **Operating Systems**: Determining the type of operating system (e.g., Windows, Linux) and version.
- **IP Addresses and Subnets**: Mapping out the IP address ranges in use.
- **Network Shares**: Discovering shared folders, printers, or resources.

2. User and Group Information

- **Usernames**: Identifying valid user accounts on the system.
- **Groups and Roles**: Enumerating which groups users belong to and their associated privileges.
- **Password Policies**: Discovering password restrictions like length, complexity, and expiration.
- **Authentication Mechanisms**: Identifying how users authenticate, such as LDAP, Kerberos, or RADIUS.

3. System Information

- **System Name**: Hostnames and computer names in the network.
- **Network Topology**: Understanding the network layout, routers, and switches.
- **Domain Information**: Finding domain names and controllers.
- **Services and Processes**: Identifying running processes and their configurations.
- **SNMP Information**: Accessing device information through the Simple Network Management Protocol.

4. Service-Specific Information

- **Banner Grabbing**: Reading system and software version information from banners.
- **Database Information**: Identifying running databases and their configurations (e.g., MySQL, PostgreSQL).
- **DNS Records**: Getting information about domain names, IP addresses, and mail servers.
- **Mail Servers**: Discovering the mail system, including user accounts and configurations.

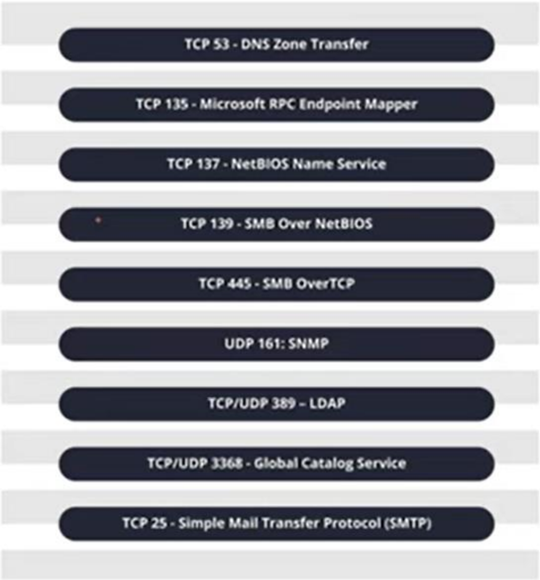
5. Vulnerabilities

- **Weak Configurations**: Detecting default settings or weak service configurations.
- **Weak Passwords**: Identifying accounts with easily guessable or weak passwords.
- **Unpatched Services**: Detecting services running outdated or vulnerable versions of software.

6. Device Information

- **Hardware Details**: Discovering information about network devices (e.g., routers, switches).
- **Network Printers**: Identifying shared network printers and their configurations.
- **VoIP Systems**: Detecting and enumerating VoIP (Voice over IP) systems and devices.

SERVICE & PORT ENUMERATE



TCP 53 - DNS Zone Transfer

TCP 135 - Microsoft RPC Endpoint Mapper

TCP 137 - NetBIOS Name Service

TCP 139 - SMB Over NetBIOS

TCP 445 - SMB OverTCP

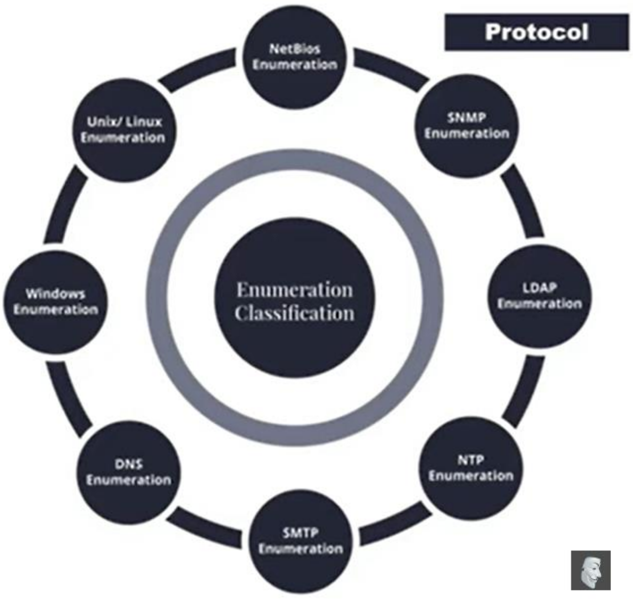
UDP 161: SNMP

TCP/UDP 389 – LDAP

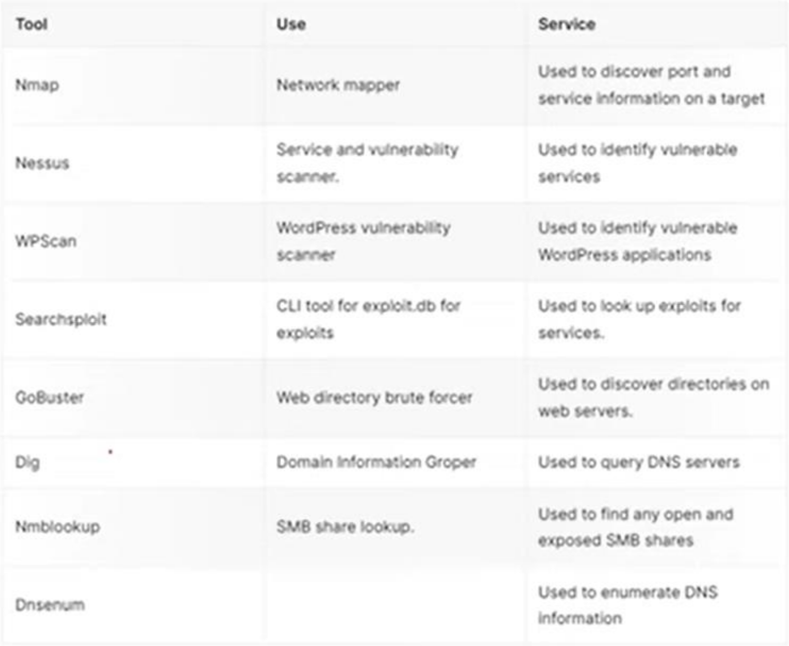
TCP/UDP 3368 - Global Catalog Service

TCP 25 - Simple Mail Transfer Protocol (SMTP)

TYPES OF ENUMERATION



TOOLS SUPPORTING ENUMERATION



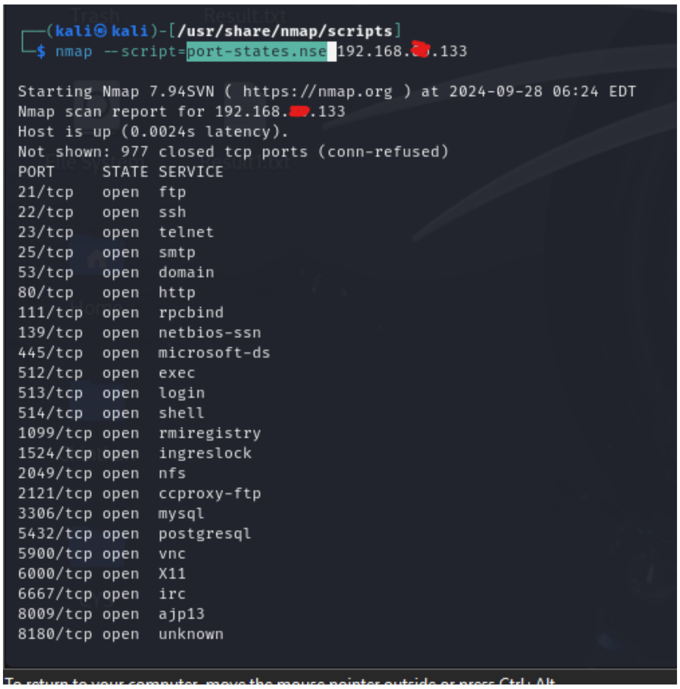
Tool	Use	Service
Nmap	Network mapper	Used to discover port and service information on a target
Nessus	Service and vulnerability scanner.	Used to identify vulnerable services
WPScan	WordPress vulnerability scanner	Used to identify vulnerable WordPress applications
Searchsploit	CLI tool for exploit.db for exploits	Used to look up exploits for services.
GoBuster	Web directory brute forcer	Used to discover directories on web servers.
Dig	Domain Information Groper	Used to query DNS servers
Nmblookup	SMB share lookup.	Used to find any open and exposed SMB shares
Dnsenum		Used to enumerate DNS information

Scripts

Home → usr →share →nmap → scripts

- All Nmap scripts are present in this folder. U can execute by using the target ip-address.
- nmap --script=<File Name> <ip-address>
- ip-address: Target ip-address
- File name: Name of the file in that folder.

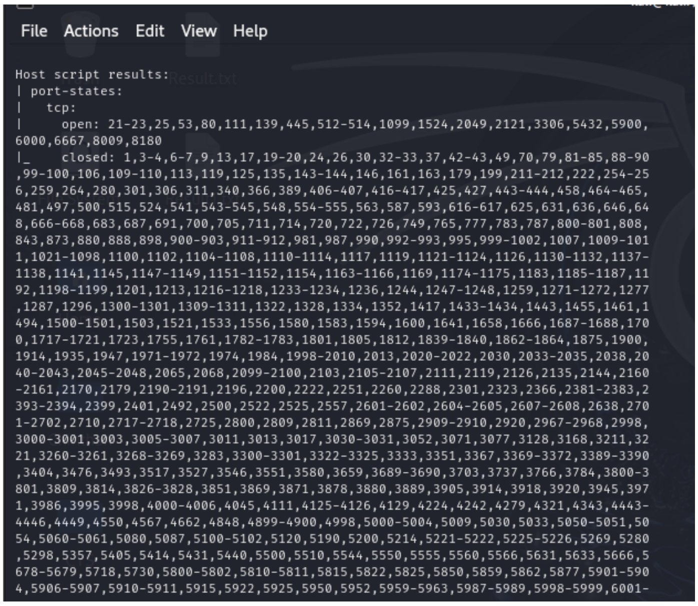
1. **nmap –script= port-states.nse <ip-address>**
   shows the state of Ports (open or close).



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=port-states.nse 192.168.[redacted].133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 06:24 EDT
Nmap scan report for 192.168.[redacted].133
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt



```
Host script results:
| port-states:
|   tcp:
|     open: 21-23,25,53,80,111,139,445,512-514,1099,1524,2049,2121,3306,5432,5900,
6000,6667,8009,8180
|_    closed: 1,3-4,6-7,9,13,17,19-20,24,26,30,32-33,37,42-43,49,70,79,81-85,88-90
,99-100,106,109-110,113,119,125,135,143-144,146,161,163,179,199,211-212,222,254-25
6,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-444,458,464-465,
481,497,500,515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,64
8,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,
843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-101
1,1021-1098,1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-
1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,11
92,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277
,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1
494,1500-1501,1503,1521,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,170
0,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,
1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,20
40-2043,2045-2048,2065,2068,2099-2100,2103,2105-2107,2111,2119,2126,2135,2144,2160
-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2
393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,270
1-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,
3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,32
21,3260-3261,3268-3269,3283,3300-3301,3322-3325,3333,3351,3367,3369-3372,3389-3390
,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3
801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,397
1,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-
4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,50
54,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280
,5298,5357,5405,5414,5431,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5
678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5901-590
4,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-5999,6001-
```

There are many more scripts for various services and Ports. Use the above syntax to excecute script.

THANK YOU