ENUMERATION

> Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

<br>

NetBIOS Enumeration:

> NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

- nbtstat -a [IP address of the remote machine]
  - In this command, -a displays the NetBIOS name table of a remote computer.
- nbtstat -c
  - In this command, -c lists the contents of the NetBIOS name cache of the remote computer.
- nmap -sV -v --script nbstat.nse [Target IP Address]
  - sV detects the service versions, -v enables the verbose output (that is, includes all hosts and ports in the output), and --script nbstat.nse performs the NetBIOS enumeration.
  - nmap -sU -p 137 --script nbstat.nse

Overview of SNMP Enumeration:

> SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

> SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

SNMP uses port 161

- nmap -sU -p 161 [Target IP address]

  > -sU performs a UDP scan and -p specifies the port to be scanned.

snmp-check [Target IP Address]

SnmpWalk:

> SnmpWalk is a command line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network. It is issued to the root node so that the information from all the sub nodes such as routers and switches can be fetched.

- snmpwalk -v1 -c public [target IP]
  - –v: specifies the SNMP version number (1 or 2c or 3) and –c: sets a community string.
- snmpwalk -v2c -c public [Target IP Address]

  - –v: specifies the SNMP version (here, 2c is selected) and –c: sets a community string.
- nmap -sU -p 161 --script=snmp-sysdescr [target IP Address]
  - sU: specifies a UDP scan, -p: specifies the port to be scanned, and -– script: is an argument used to execute a given script (here, snmp-sysdescr).
- nmap -sU -p 161 --script=snmp-processes [target IP Address]
- nmap -sU -p 161 --script=snmp-win32-software [target IP Address]
- nmap -sU -p 161 --script=snmp-interfaces [target IP Address]

LDAP Enumeration:

> LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

- nmap -sU -p 389 [Target IP address]
- nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=CEH,dc=com"' [Target IP Address]
- ldapsearch
  - ldapsearch is a shell-accessible interface to the ldap_search_ext(3) library call. ldapsearch opens a connection to an LDAP server, binds the connection, and performs a search using the specified parameters. The filter should conform to the string representation for search filters as

defined in RFC 4515. If not provided, the default filter, (objectClass=*), is used.

- ldapsearch -h [Target IP Address] -x -s base namingcontexts
  - x: specifies simple authentication, -h: specifies the host, and -s: specifies the scope.
- ldapsearch -h [Target IP Address] -x -b “DC=CEH,DC=com”
  - x: specifies simple authentication, -h: specifies the host, and -b: specifies the base DN for search.
- ldapsearch -x -h [Target IP Address] -b "DC=CEH,DC=com" "objectclass=*"
  - x: specifies simple authentication, -h: specifies the host, and -b: specifies the base DN for search.

NFS Enumeration:

> NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

- nmap -p 2049 [Target IP Address]
- https://github.com/p4pentest/SuperEnum
- https://github.com/hegusung/RPCScan

DNS Enumeration:

> DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization. DNS enumeration can be performed using the following techniques:

- dig ns [Target Domain]
  - In this command, ns returns name servers in the result

- dig @[NameServer] [Target Domain] axfr
  - (in this example, the name server is ns1.bluehost.com and the target domain is www.certifiedhacker.com); press Enter.
  - In this command, axfr retrieves zone information.

DNSSEC Zone Walking:

> DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map.

- ./dnsrecon.py -d [Target domain] -z
  - In this command, -d specifies the target domain and -z specifies that the DNSSEC zone walk be performed with standard enumeration.
- nmap --script=broadcast-dns-service-discovery [Target Domain]
- nmap -T4 -p 53 --script dns-brute [Target Domain]
  - T4: specifies the timing template, -p: specifies the target port.
- nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='[Target Domain]'”

SMTP Enumeration:

> The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

- nmap -p 25 --script=smtp-enum-users [Target IP Address]
- nmap -p 25 --script=smtp-open-relay [Target IP Address]

- nmap -p 25 --script=smtp-commands [Target IP Address]

RPC Enumeration: Enumerating RPC endpoints enables vulnerable services on these service ports to be identified

SMB Enumeration: Enumerating SMB services enables banner grabbing, which obtains information such as OS details and versions of services running

FTP Enumeration: Enumerating FTP services yields information about port 21 and any running FTP services; this information can be used to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing

Enumerate Information from Windows and Samba Hosts using Enum4linux:

- Enum4linux is a tool for enumerating information from Windows and Samba systems. It is used for share enumeration, password policy retrieval, identification of remote OSes, detecting if hosts are in a workgroup or a domain, user listing on hosts, listing group membership information, etc.
- enum4linux -u martin -p apple -n [Target IP Address]
- enum4linux -u martin -p apple -U [Target IP Address]
    - In this command, -u user specifies the username to use, -p pass specifies the password and -U retrieves the userlist.
    - P retrieves the password policy information.
    - o retrieves the OS information.
    - G retrieves group and member list.
    - S retrieves sharelist.

Below is an in-depth exploration of common enumeration techniques, including detailed examples and explanations for each. These techniques are widely used in penetration testing and ethical hacking to gather critical information about a target.

---

1. Banner Grabbing

Purpose: Retrieve service banners to identify software names, versions, and configurations. This helps in fingerprinting the target and identifying potential vulnerabilities.

Methods and Tools:

- **Netcat (nc)**:

```
bashCopy
nc -nv <target_ip> 80
GET / HTTP/1.1
```

  - This sends a basic HTTP request to the web server, which often responds with server details (e.g., `Apache/2.4.29`).

- **Telnet**:

```
bashCopy
telnet <target_ip> 25
```

  - For SMTP servers, this might return a banner like `220 mail.example.com ESMTP Postfix`.

- **Nmap**:

```
bashCopy
nmap -sV --script=banner <target_ip>
```

  - The `sV` flag probes services to determine versions, while the `banner` script extracts banners.

Use Case:

- Identifying outdated software (e.g., an old Apache version with known exploits).

---

2. Null Session Enumeration (SMB)

Purpose: Exploit misconfigured SMB shares to enumerate users, groups, and shares without authentication.

Steps:

1. **Check for Null Session Vulnerability**:

```
bashCopy
smbclient -L //<target_ip> -N
```

- If successful, this lists available shares (e.g., `IPC$`, `ADMIN$`).

2. **Enumerate Users**:

   ```
   bashCopy
   rpcclient -U "" -N <target_ip>
   ```

   - Inside the `rpcclient` shell, commands like `enumdomusers` list domain users.

Mitigation:

- Disable null sessions in SMB configuration (`restrict anonymous = 2` in `smb.conf`).

3. DNS Enumeration

Purpose: Extract DNS records to map the target's domain infrastructure, including subdomains and mail servers.

Techniques:

- **Zone Transfer**:

  ```
  bashCopy
  dig axfr @<dns_server> <domain>
  ```

  - If the DNS server allows zone transfers, this returns all records (A, MX, TXT, etc.).

- **Subdomain Bruteforcing**:

  ```
  bashCopy
  gobuster dns -d example.com -w subdomains.txt
  ```

  - Uses a wordlist (`subdomains.txt`) to discover subdomains like `admin.example.com`.

Use Case:

- Discovering hidden subdomains (e.g., `dev.example.com`) that may expose test environments.

4. SNMP Enumeration

Purpose: Retrieve system details (e.g., OS, processes, interfaces) via SNMP if community strings are weak or default.

Steps:

1. **Identify SNMP Ports**:

    ```
    bashCopy
    nmap -sU -p 161 <target_ip>
    ```

    - Checks if UDP port 161 (SNMP) is open.

2. **Brute-Force Community Strings**:

    ```
    bashCopy
    onesixtyone -c community.txt <target_ip>
    ```

    - Tries common strings like `public`, `private`.

3. **Query MIBs**:

    ```
    bashCopy
    snmpwalk -c public -v1 <target_ip> 1.3.6.1.2.1.1.1
    ```

    - Retrieves system description (e.g., `Linux server 4.15.0-20-generic`).

Mitigation:

- Use SNMPv3 with authentication and encryption.

---

5. LDAP Enumeration

Purpose: Extract user, group, and policy details from Active Directory or LDAP services.

Steps:

1. **Connect to LDAP**:

    ```
    bashCopy
    ldapsearch -x -h <target_ip> -b "dc=example,dc=com"
    ```

- Lists all objects in the LDAP directory.

2. **Filter for Users**:

```
bashCopy
ldapsearch -x -h <target_ip> -b "dc=example,dc=com" "(objectClass=user)"
```

- Returns user accounts with attributes like `sAMAccountName`.

Use Case:

- Mapping organizational structure for targeted phishing.

---

6. Web Application Enumeration

Purpose: Discover hidden directories, files, and parameters in web apps.

Techniques:

- **Directory Bruteforcing**:

  ```
  bashCopy
  gobuster dir -u http://example.com -w /path/to/wordlist.txt
  ```

  - Finds paths like `/admin/` or `/backup/`.

- **Parameter Fuzzing**:

  ```
  bashCopy
  ffuf -u http://example.com?FUZZ=test -w params.txt
  ```

  - Identifies vulnerable parameters (e.g., `?id=1` for SQLi).

Use Case:

- Locating unprotected admin panels (`/admin/login.php`).

---

7. RPC Enumeration

Purpose: Gather information about remote procedures (e.g., NFS, RPCbind).

Steps:

1. **List RPC Services**:

   ```
   bashCopy
   rpcinfo -p <target_ip>
   ```

   - Shows programs like `mountd` (NFS) or `nfs`.

2. **NFS Share Enumeration**:

   ```
   bashCopy
   showmount -e <target_ip>
   ```

   - Lists exported shares (e.g., `/home`).

Mitigation:

- Restrict RPC services to trusted networks.

---

8. SMTP Enumeration

Purpose: Identify valid email addresses via SMTP commands.

Steps:

1. **Connect to SMTP**:

   ```
   bashCopy
   nc <target_ip> 25
   ```

2. **Verify Users**:

   ```
   bashCopy
   VRFY root
   ```

   - If the server responds `250 2.1.5`, the user exists.

Use Case:

- Building a list of targets for phishing campaigns.

---

9. FTP Enumeration

Purpose: Discover files, directories, and misconfigurations in FTP servers.

Steps:

1. **Anonymous Login**:

   ```
   bashCopy
   ftp <target_ip>
   ```

   - Try username `anonymous` with any password.

2. **List Files**:

   ```
   bashCopy
   ls -la
   ```

   - Check for sensitive files like `passwords.txt`.

Mitigation:

- Disable anonymous logins.

---

10. Database Enumeration

Purpose: Extract schema, tables, and data from databases (e.g., MySQL, MSSQL).

Techniques:

- **MySQL**:

  ```
  bashCopy
  mysql -h <target_ip> -u root -p
  SHOW DATABASES;
  ```

- **MSSQL**:

  ```
  bashCopy
  sqsh -S <target_ip> -U sa
  SELECT name FROM sys.databases;
  ```

Use Case:

- Dumping credentials from a poorly secured database.

Summary Table of Tools and Commands

Technique	Tool/Command	Example Output
Banner Grabbing	`nc`, `telnet`, `nmap -sV`	`Apache/2.4.29`
Null Session	`smbclient -L`, `rpcclient`	List of SMB shares
DNS Enumeration	`dig axfr`, `gobuster dns`	Subdomains (`admin.example.com`)
SNMP Enumeration	`snmpwalk`, `onesixtyone`	System OS, processes
LDAP Enumeration	`ldapsearch`	User accounts, groups
Web Dir Bruteforcing	`gobuster dir`, `ffuf`	Hidden paths (`/backup/`)
SMTP User Enum	`VRFY`, `EXPN`	Valid email addresses
FTP Enumeration	`ftp`, `anonymous login`	Exposed files (`config.php`)

Ethical Considerations

- Always obtain explicit authorization before enumeration.
- Avoid aggressive scanning that could disrupt services.
- Document findings securely and report responsibly.

Enumeration is a powerful phase that lays the groundwork for exploitation. Mastering these techniques ensures thorough assessments and robust defenses.