Enumeration

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network
- Policies and passwords
- Routing tables
- Audit and service settings
- SNMP and FQDN details

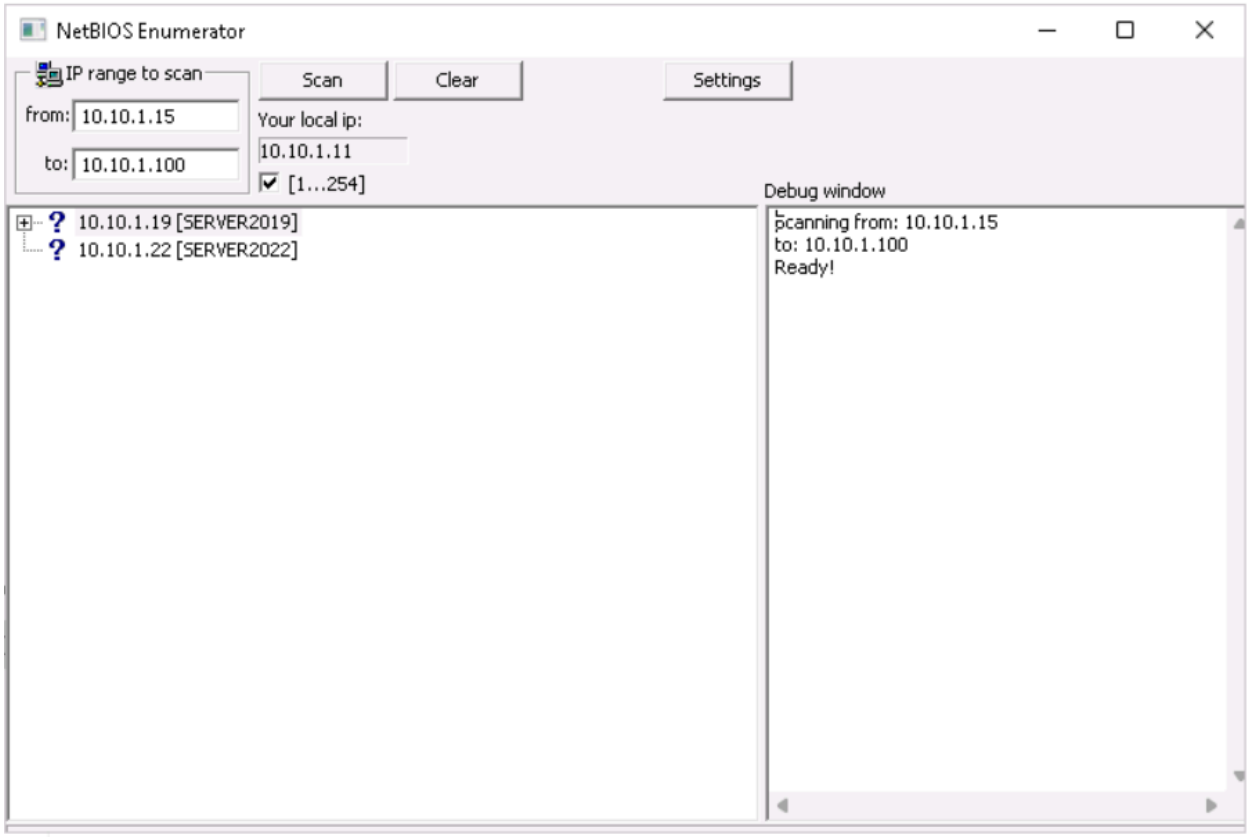
a. Perform NetBIOS enumeration

i. Perform NetBIOS enumeration using Windows command-line utilities

- Using the nbtstat command (***nbtstat -a [target Ip***]) (**-a** displays the NetBIOS name table of a remote computer.)
- ***nbtstat -c*** (**-c** lists the contents of the NetBIOS name cache of the remote computer.)
- ***net use*** (connection status, shared folder/drive and network information)

ii. Perform NetBIOS enumeration using NetBIOS Enumerator

- NetBIOS Enumerator



iii. Perform NetBIOS enumeration using an NSE Script (Parrot Linux)

nbstat script to enumerate information such as the name of the computer and the logged-in user.

- Nmap -sV -v –script nbstat.nse [target IP]
- Nmap -sU -v -p 137 –script nbstat.nse [target IP]
- **Global Network Inventory (http://www.magnetosoft.com)**
- **Advanced IP Scanner (https://www.advanced-ip-scanner.com)**
- **Hyena (https://www.systemtools.com)**
- **Nsauditor Network Security Auditor (https://www.nsauditor.com)**

b. Perform SNMP enumeration

i. **SNMP-check** [snmp-check 10.10.1.22]

ii. **SoftPerfect Network Scanner**
Network Performance Monitor (https://www.solarwinds.com)
OpUtils (https://www.manageengine.com)
PRTG Network Monitor (https://www.paessler.com)
Engineer's Toolset (https://www.solarwinds.com)

iii. **Snmp Walk** [snmpwalk -v1 -c public 10.10.1.22]

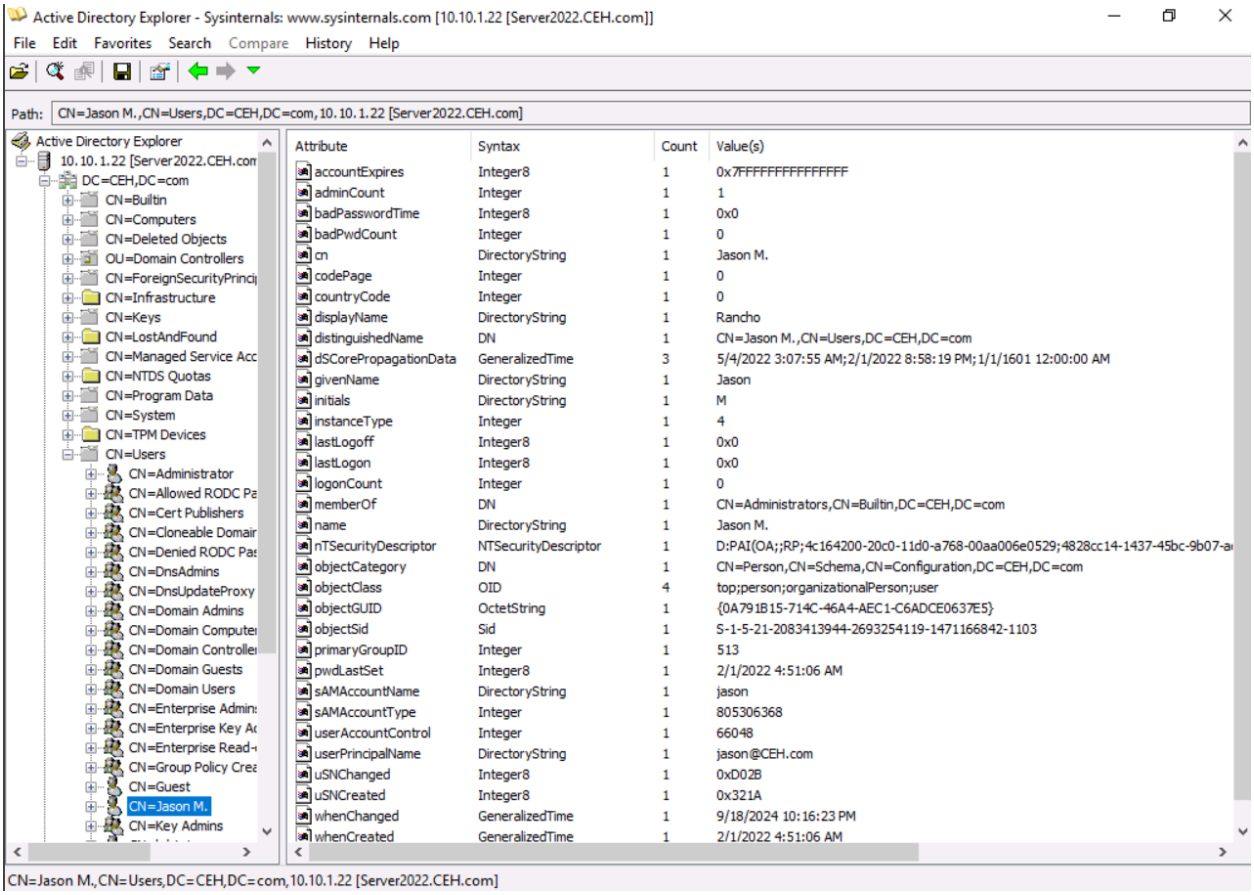
- This is a command-line tool used to retrieve a subtree of management values from a target system via SNMP.
- `-v1`: Specifies the SNMP version. In this case, it's using SNMP version 1. Others are v2c and v3.
- `-c public`: This is the community string, which acts like a password. "public" is a common default string for read-only access.

iv. **Nmap**

- Nmap -sU -p 161 –script=snmp-sysdescr 10.10.1.22
  → (Information regarding SNMP server type and operating system details)
- Nmap -sU -p 161 –script=snmp-processes 10.10.1.22
  → (list of all the running SNMP processes along with the associated ports on the target machine)
- Nmap -sU -p 161 –script=snmp-win32-software 10.10.1.22
  → (list of all the applications running on the target machine)
- Nmap -sU -p 161 –script=snmp-interfaces 10.10.1.22
  → (information about the Operating system, network interfaces, and applications that are installed on the target machine)

c. Perform LDAP enumeration Port :- 389

i. Perform LDAP enumeration using Active Directory Explorer (AD Explorer)



- Softerra LDAP Administrator (https://www.ldapadministrator.com)
- LDAP Admin Tool (https://www.ldapsoft.com)
- LDAP Account Manager (https://www.ldap-account-manager.org)
- LDAP Search (https://securityxploded.com)

ii. Perform LDAP enumeration using Python and Nmap

[nmap -p 389 –script ldap-brute –script-args ldap.base=’”cn=users,dc=CEH,dc=com”’ 10.10.1.22**]**

-p:- specifies the port to be scanned

ldap-brute:- to perform brute-force LDAP authentication

ldap.base:- *if set, the script will use it as a base for the password guessing attempts.*

iii. **Perform LDAP enumeration using ldapsearch**

- Ldapsearch -h 10.10.1.22 -x -s base namingcontexts
- Ldapsearch -h 10.10.1.22 -x -b “DC=CEH,DC=com”
- Ldapsearch -x -h 10.10.1.22 -b “DC=CEH,DC=com” “objectclass=*”
- **-x**: specifies simple authentication
- **-h**: specifies the host
- **-s**: specifies the scope.
- **-b**: specifies the base DN for search.

d. Perform NFS enumeration

i. **Using SuperEnum**

- cd SuperEnum
- echo “10.10.1.19” >> Target.txt
- ./superenum

ii. **Using RPCScan**

- cd RPCScan
- python3 rpc-scan.py 10.10.1.19 --rpc
- **--rpc**: lists the RPC (portmapper).

e. Perform DNS enumeration

i. **Zone Transfer**

- **(In Parrot)**
- dig ns [domain]
- dig @[nameserver] [target domain] axfr (axfr retrieves zone information)
- **(In Windows CMD)**
- nslookup
- set querytype=soa [SOA – Start of Authority]
- www.certifiedhacker.com
- In nslookup, ls -d [Name Server] (**ls -d** requests a zone transfer of the specified name server)

ii. **DNSSEC zone walking**
- DNSRecon [./dnsrecon.py -d www.target.com -z] (-d = domain, -z = DNSSEC zone walk)
- **LDNS** (https://www.nlnetlabs.nl)
- **nsec3map** (https://github.com)
- **nsec3walker** (https://dnscurve.org)
- **DNSwalk** (https://github.com)

iii. **DNS Enumeration Using Nmap**
- nmap --script=broadcast-dns-service-discovery [domain]
- nmap -T4 -p 53 --script dns-brute [Target Domain]
- nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'"

f. Perform SMTP Enumeration

i. **Using nmap**
- nmap -p 25 --script=smtp-enum-users [Target IP]
- nmap -p 25 --script=smtp-open-relay [Target IP]
- The attackers can perform password spraying attacks to gain unauthorized access to the user accounts.

g. Perform RPC, SMB, and FTP enumeration

i. **Perform SMB and RPC enumeration using NetScanTools Pro**
- Using NetScanTools Pro
- →Manual > smb scanner > put Ip addresses > put credentials > Get smb shares

ii. **Perform RPC, SMB, and FTP enumeration using Nmap**
- Using Nmap
- First start the FTP service in target machine
- Using IIS (Internet Information Services)
- nmap -p 21 [Target Ip]
- nmap -T4 -A [Target IP]

- nmap -p 445 -A [Target Ip]
- nmap -p 21 -A [Target Ip]

h. Perform enumeration using various enumeration tools

i. **Global Network Inventory**
   - Download GNI (Global Network Inventory)

ii. **Advanced IP Scanner**
   - Download Advance Ip Scanner

iii. **Windows and Samba hosts using Enum4linux**
   - enum4linux -u martin -p apple -n [Target IP]
     (-u – username, -p – password, -n – NetBIOS)
   - enum4linux -u martin -p apple -U [Target IP] (-U – userlist)
   - -o → OS information
   - -P → Password Policy
   - -G → Group Policy (retrieves group and member list.)
   - -S → Shared List