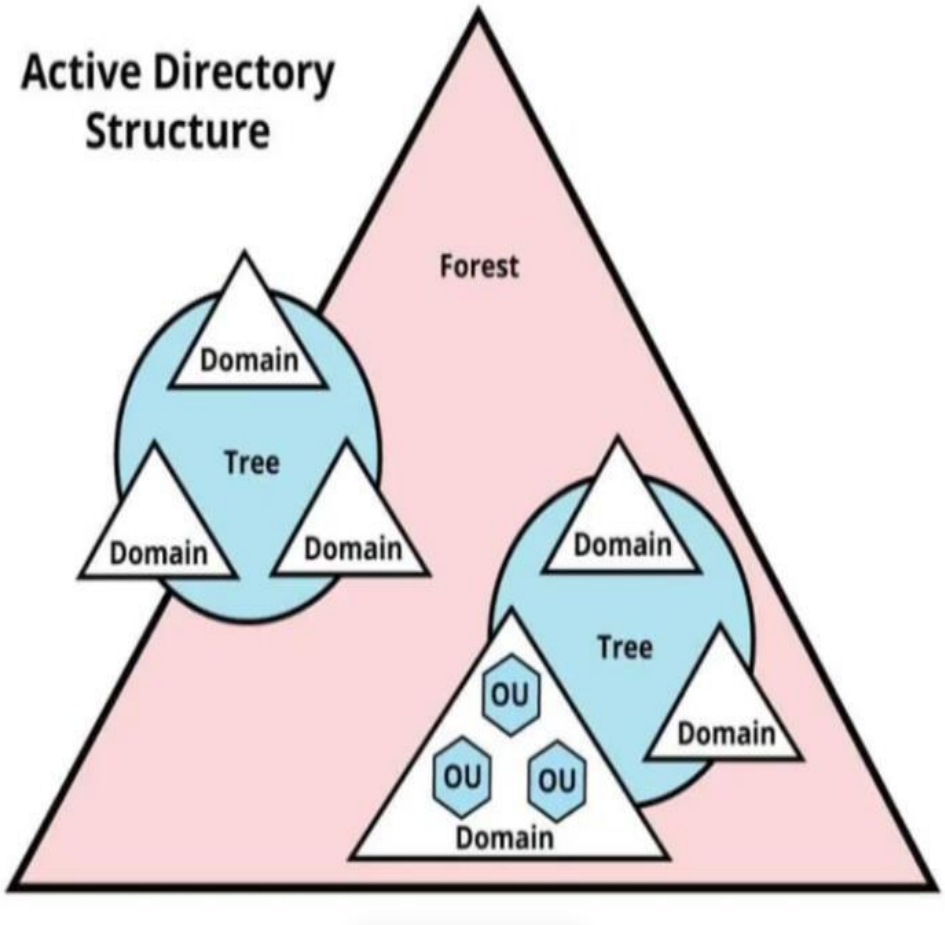
Active Directory Enumeration

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

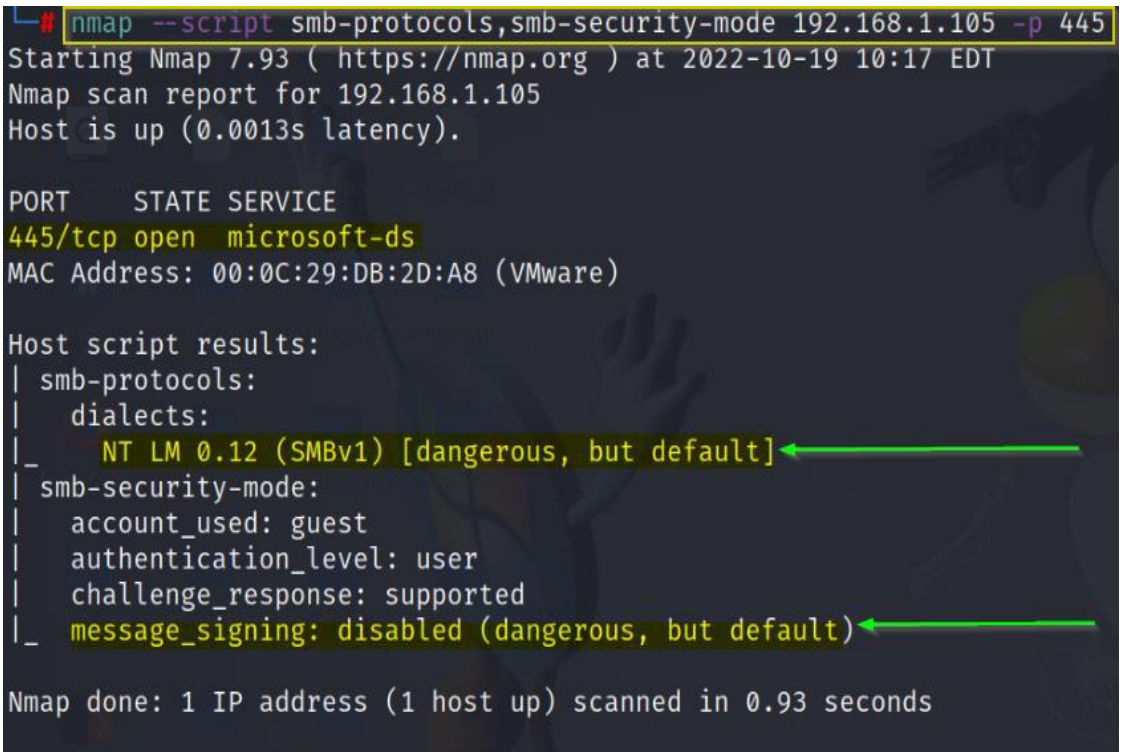
Ports to identify and Attack

- 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

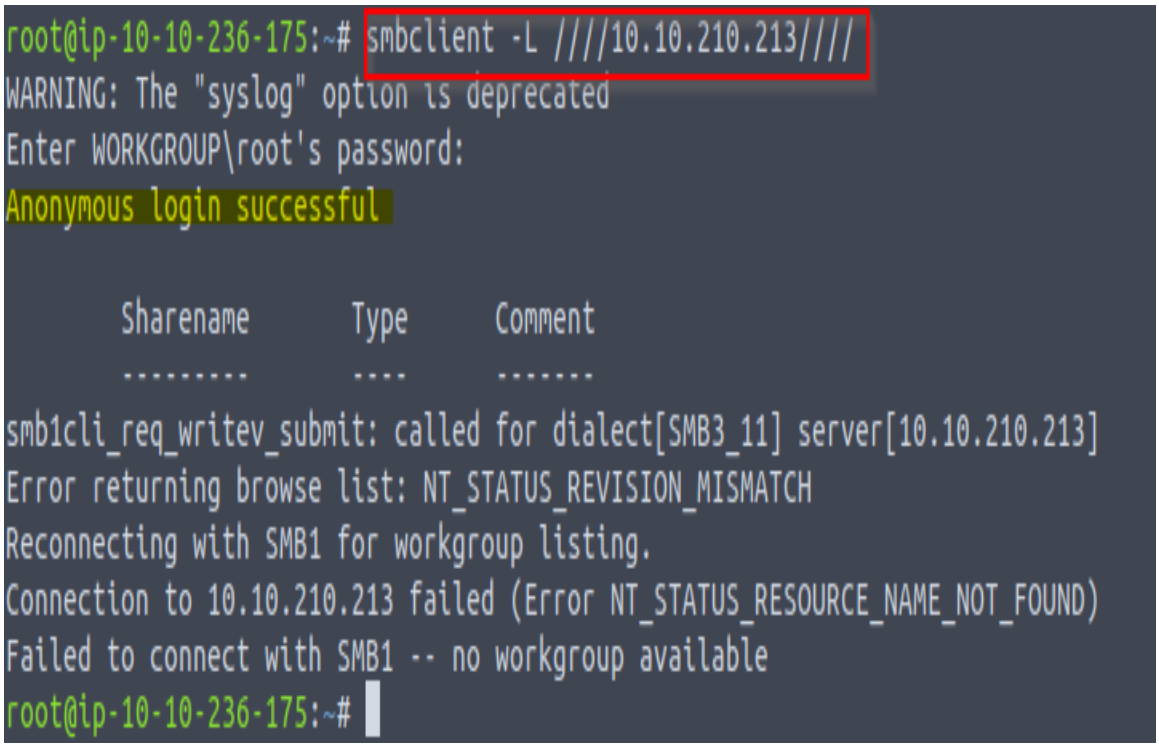


Null Login

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.

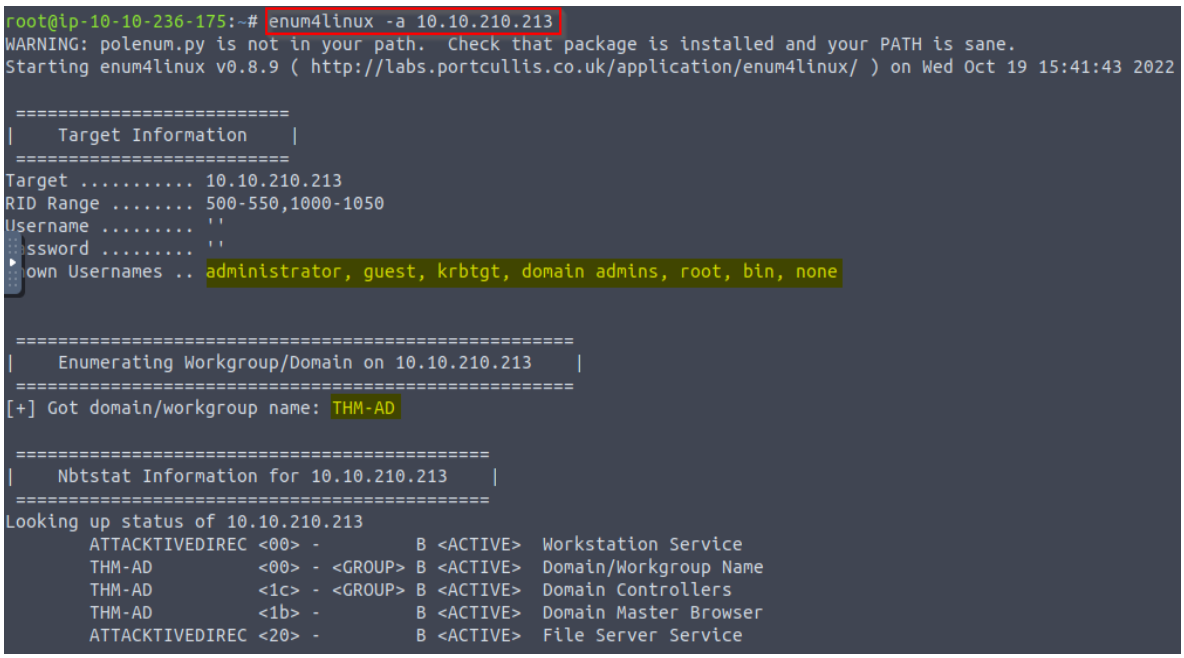


SMBMap allows users to enumerate samba share drives across an entire domain. List share drives,drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands.

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.

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



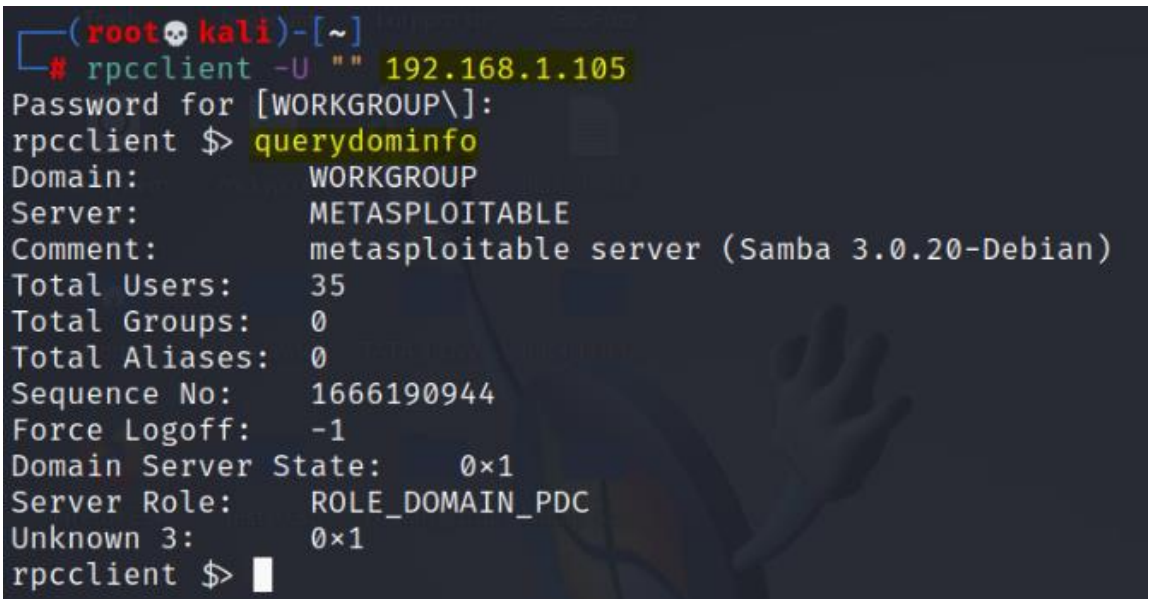
User enumeration using Rpcclient

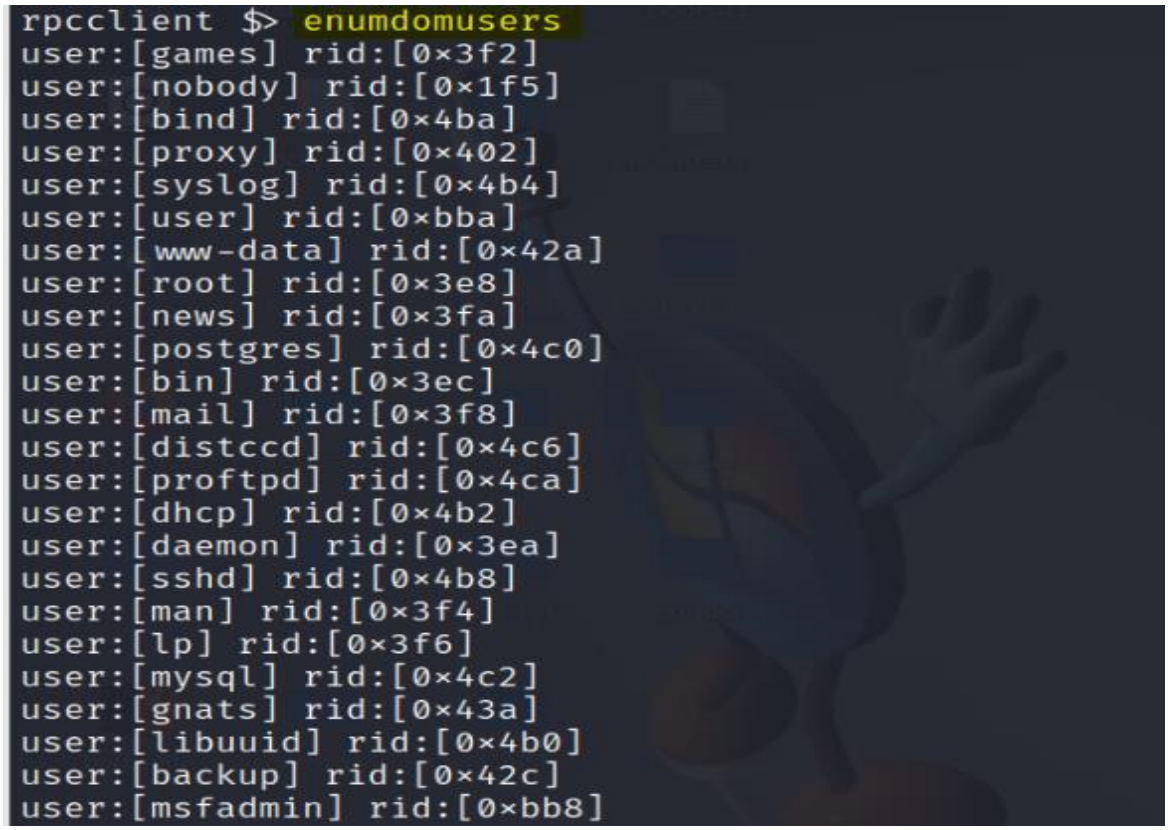
What is Rpcclient used for?

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.

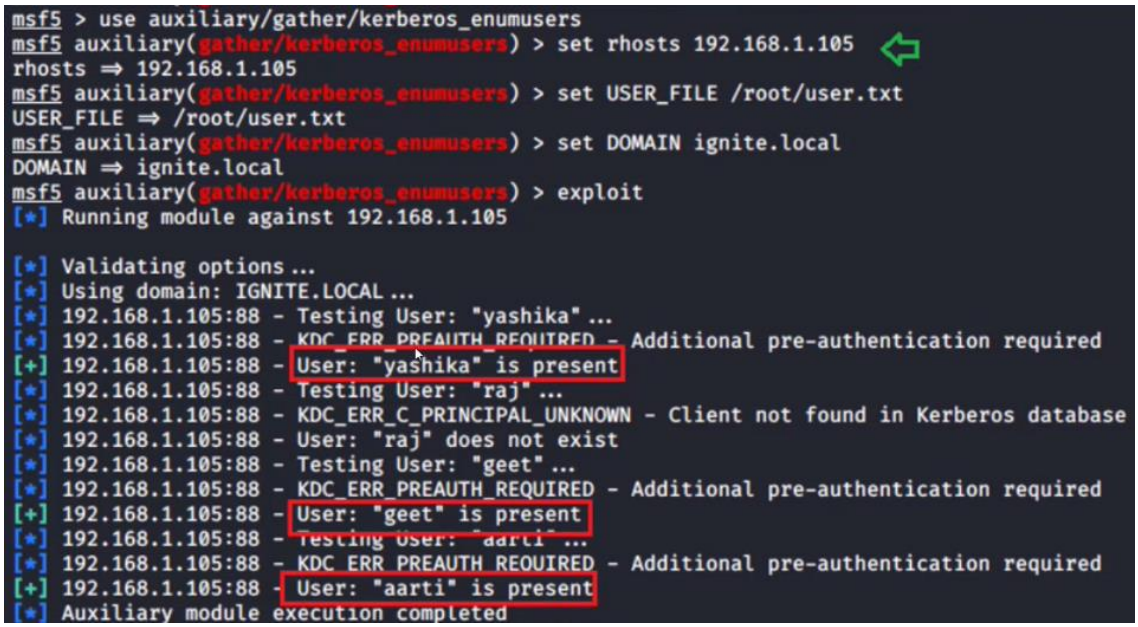




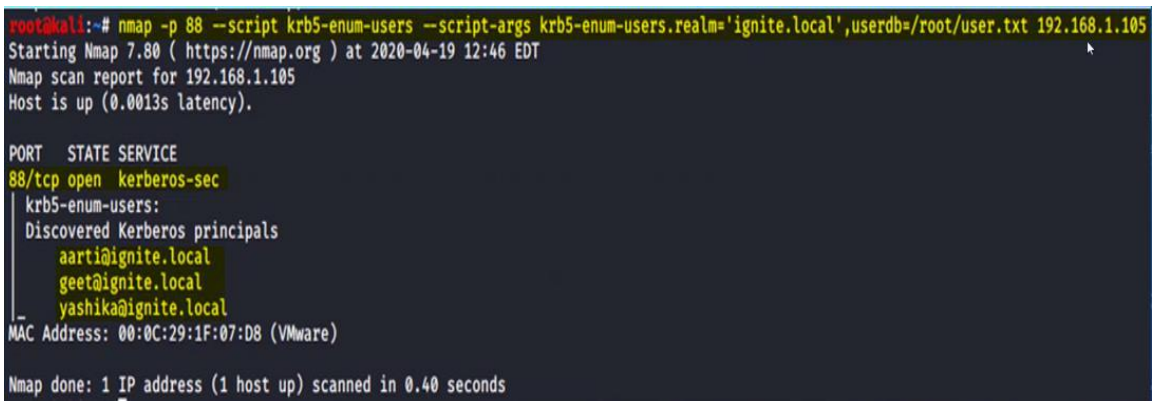
Attacking Port 88 Kerberos

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.

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



Nmap –script krb5-enum-users



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.