📚🔭Tools to enumerate NTDS Database With Kali 🐲

Intro

As we saw on the introduction of this section we can enumerate the NTDS Database that the domain controller has, even without an elevated user privs on the domain, through the **LDAP protocol** we just need to use the credentials of a legitim domain user to enumerate remotely all that information.

We can use a lot of tools to enumerate NTDS Databases and in this section we are going to see how to use some tools to do that.

👾Netexec/🐙Crackmapexec

NetExec (formerly known as CrackMapExec) is a post-exploitation and enumeration tool that allows you to interact with common Windows networking services such as SMB, WinRM, RDP, and of course, **LDAP**.

When connected via **LDAP**, NetExec allows us to enumerate key information from the Active Directory domain (**NTDS**) in the ***Domain Controller*** database without using SMB or executing remote commands. Of course we will need credentials of a legitim domain user.

Among the things we can enumerate, specifying the DC IP address, are:

👥 Domain user enumeration (--users)

netexec ldap 10.10.10.5 -u Username -p Password --users

```
netexec ldap 192.168.20.5 -u employer1 -p Password01 --users
SMB         192.168.20.5    445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:corp.local) (signing:True) (SMBv1:False)
LDAP        192.168.20.5    389    DC01            [+] corp.local\employer1:Password01
LDAP        192.168.20.5    389    DC01            [*] Enumerated 156 domain users: corp.local
LDAP        192.168.20.5    389    DC01            -Username-                    -Last PW Set-       -BadPW- -Description-
LDAP        192.168.20.5    389    DC01            Administrator                 2024-12-05 23:51:00 0       Built-in account for administering the computer/domain
LDAP        192.168.20.5    389    DC01            Guest                         <never>             0       Built-in account for guest access to the computer/domain
LDAP        192.168.20.5    389    DC01            krbtgt                        2024-12-06 00:28:46 0       Key Distribution Center Service Account
LDAP        192.168.20.5    389    DC01            employer1                     2024-12-07 01:46:55 0
LDAP        192.168.20.5    389    DC01            employer2                     2024-12-07 01:47:57 0
LDAP        192.168.20.5    389    DC01            faustine.lars                 2024-12-28 02:15:37 0
LDAP        192.168.20.5    389    DC01            ada.jammie                    2024-12-28 02:15:38 0
LDAP        192.168.20.5    389    DC01            aryn.maurita                  2024-12-28 02:15:38 0
LDAP        192.168.20.5    389    DC01            king.pammy                    2024-12-28 02:15:38 0
LDAP        192.168.20.5    389    DC01            leda.raye                     2024-12-28 02:15:38 0
LDAP        192.168.20.5    389    DC01            kendre.dorine                 <never>             2       New User. DefaultPassword
```

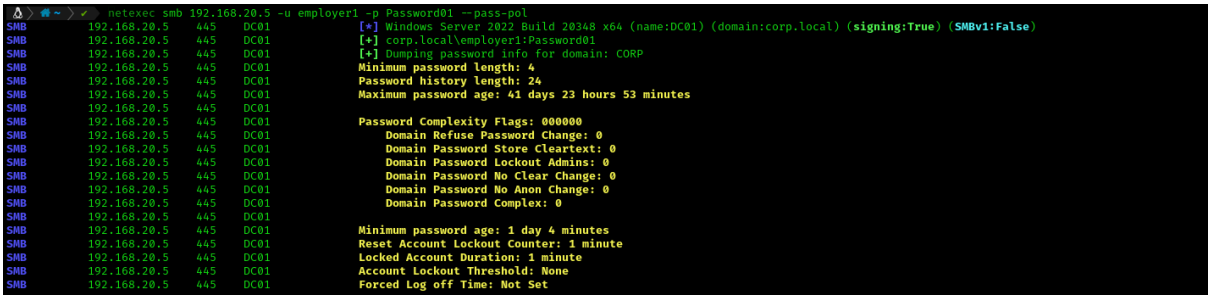
👨‍👨‍👧‍👧 Group enumeration (--groups)

netexec ldap 10.10.10.5 -u Username -p Password --groups

```
netexec ldap 192.168.20.5 -u employer1 -p Password01 --groups
SMB         192.168.20.5    445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:corp.local) (signing:True) (SMBv1:False)
LDAP        192.168.20.5    389    DC01            [+] corp.local\employer1:Password01
LDAP        192.168.20.5    389    DC01            Administrators
LDAP        192.168.20.5    389    DC01            Users
LDAP        192.168.20.5    389    DC01            Guests
LDAP        192.168.20.5    389    DC01            Print Operators
LDAP        192.168.20.5    389    DC01            Backup Operators
LDAP        192.168.20.5    389    DC01            Replicator
LDAP        192.168.20.5    389    DC01            Remote Desktop Users
LDAP        192.168.20.5    389    DC01            Network Configuration Operators
LDAP        192.168.20.5    389    DC01            Performance Monitor Users
LDAP        192.168.20.5    389    DC01            Performance Log Users
```

Something interesting is that we can enumerate that information using **SMB** protocol, in some cases with better results. For example if we enumerate ***groups***, specifying the **SMB** protocol, not only do they show us the groups that are in the domain, but also how ***many members belong to them***.

We can also list **the domain's password policy** with the **--pass-pol** flag.



With this information we can design more realistic brute force attacks that do not endanger the productivity of the environment we are auditing.

🖥️⚡Pywerview

Intro

Pywerview is a tool writing in python for enumeration using LDAP protocol. This tool is very similar to Power View, in that it will allow us to enumerate the NTDS database with one big difference : that we can use **Pywerview** to enumerate from our attacker machine.

To use **Pywerview** we will need credentials from a domain user.

This tool cames pre install on Kali Linux 🐉and Parrot 🦜systems and it will be use it by terminal command line.

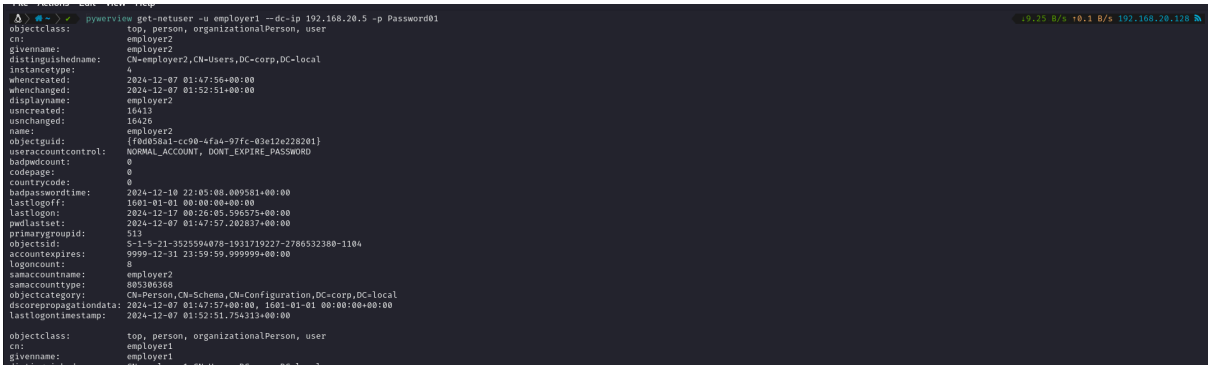
🖥️🔨⚡ Pywerview on action

The command to use pywerview will consist of calling the tool "**pywerview**" then the command that we will use to enumerate, for example **"get-netuser"**, next we have to use the **username** with the parameter **"-u user"**. The next step is put the **DC** IP address "**--dc-ip 192.0.0.5"** and finally the password with **"-p password:D"**

There some examples of commands that we can use to enumerate NTDS database

pywerview get-netuser -u Username --dc-ip 192.0.0.5 -p Password

This command will dump information about all domain users



pywerview get-netdomaincontroller -u Username --dc-ip 192.0.0.5 -p Password

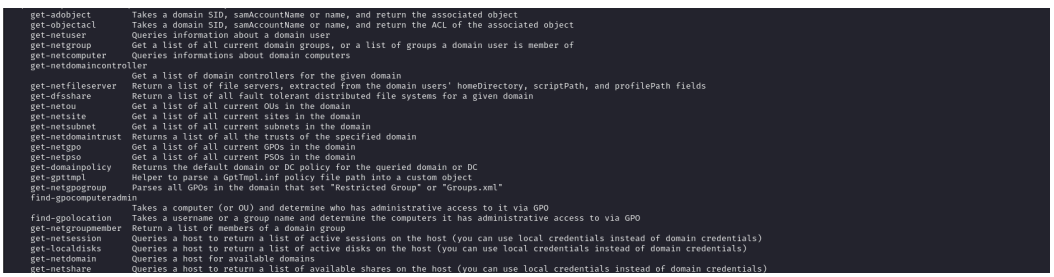
This command allows us gather information about the domain controller

There are just two examples of what we can do with **pywerview**. Of course, it has a lot of functionality that we can use to enumerate a domain and that we can use according to what we want to enumerate in the domain

Conclusions

As we have seen, **pywerview** is a very interesting tool that we can use if we don't have access to a domain computer or if we just want to use an alternative tool.

If we want more info about all commands that we can use, we just have to use the the command **pywerview -h**



📟 Ldapsearch

Intro

Ldapsearch is a tool that allows us to interact with a database using the LDAP **protocol** and we use it to interact with the **NTDS Database** that DC has.

This tool cames pre install on Kali Linux 🐉and Parrot 🦜systems and it will be use it by terminal command line

📟👨‍👩‍👧‍👦 Ldapsearch on action

Ok, let's see some commands that we can perform with **LDAP search**.

ldapsearch -x -H ldap://10.10.10.5 -D 'DOMAIN\Username' -w 'Password' -b "DC=domain,DC=local"

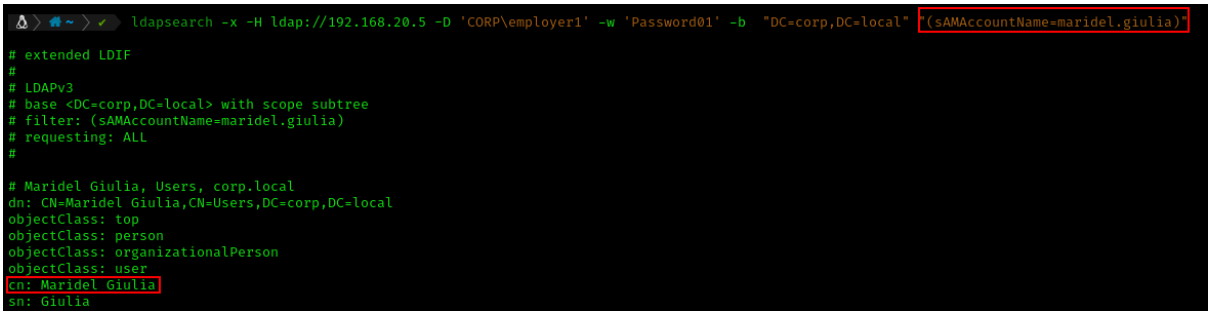
```
ldapsearch -x -H ldap://192.168.20.5 -D 'CORP\employer1' -w 'Password01' -b  "DC=corp,DC=local"
# extended LDIF
#
# LDAPv3
# base <DC=corp,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# corp.local
dn: DC=corp,DC=local
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=corp,DC=local
instanceType: 5
```

When we successfully perform this command we will see that we received an enormous output, because **ldapsearch** is dumping all the information that this NTDS database has, user, groups, gpos, computers… etc.

But if we just receive a specific information we just have to add the flag **CN=** on the **-b** part followed by that information that interests us. For example, if we are interested of dump all domain user will be something like:
-b "CD=UsersDC=domain,DC=local".

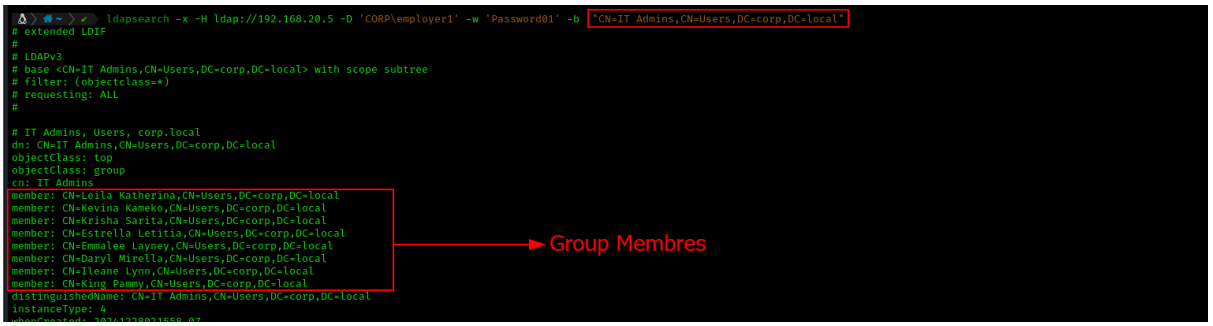
```
ldapsearch -x -H ldap://192.168.20.5 -D 'CORP\employer1' -w 'Password01' -b  "CN=Users,DC=corp,DC=local"
# extended LDIF
#
# LDAPv3
# base <CN=Users,DC=corp,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# Users, corp.local
dn: CN=Users,DC=corp,DC=local
objectClass: top
objectClass: container
cn: Users
description: Default container for upgraded user accounts
distinguishedName: CN=Users,DC=corp,DC=local
instanceType: 4
whenCreated: 20241206002752.0Z
whenChanged: 20241206002752.0Z
uSNCreated: 5660
```

And if we are interested on a particular user we can add that username adding **"(sAMAccountName=user.name)"**



If we what enumerate de computes on the domain we can add **"CD=Computer"**:

And if we what to enumerate a particular group and its members, we can do it adding the flag **"CD=GroupName,CD=Users,"**



And we can more

Anonymous enumeration

ldapsearch -x -H ldap://10.10.10.5 -D ' ' -w ' ' -b "DC=domain,DC=local"

We can perform this command to see if the domain allows enumeration by an Anonymous user. An anonymous enumeration is unlikely to be carried out, but it never hurts to try.

Conclusion

There are some information tools that we can use to enumerate a domain via **NTDS database** through **LDAP** and other protocols from our attacker Machine.