**📚🔭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, we just need to use the credentials of a legitim domain user and we can enumerate remotely all that info.

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.

**📟 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**.

**Anonymous enumeration**

**ldapsearch -x -h 192.168.20.5 -D ' ' -w ' ' -b "DC=corp,DC=local"**

We can perform this command to see if the domain allows enumeration by an Anonymous user

**🖥️⚡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

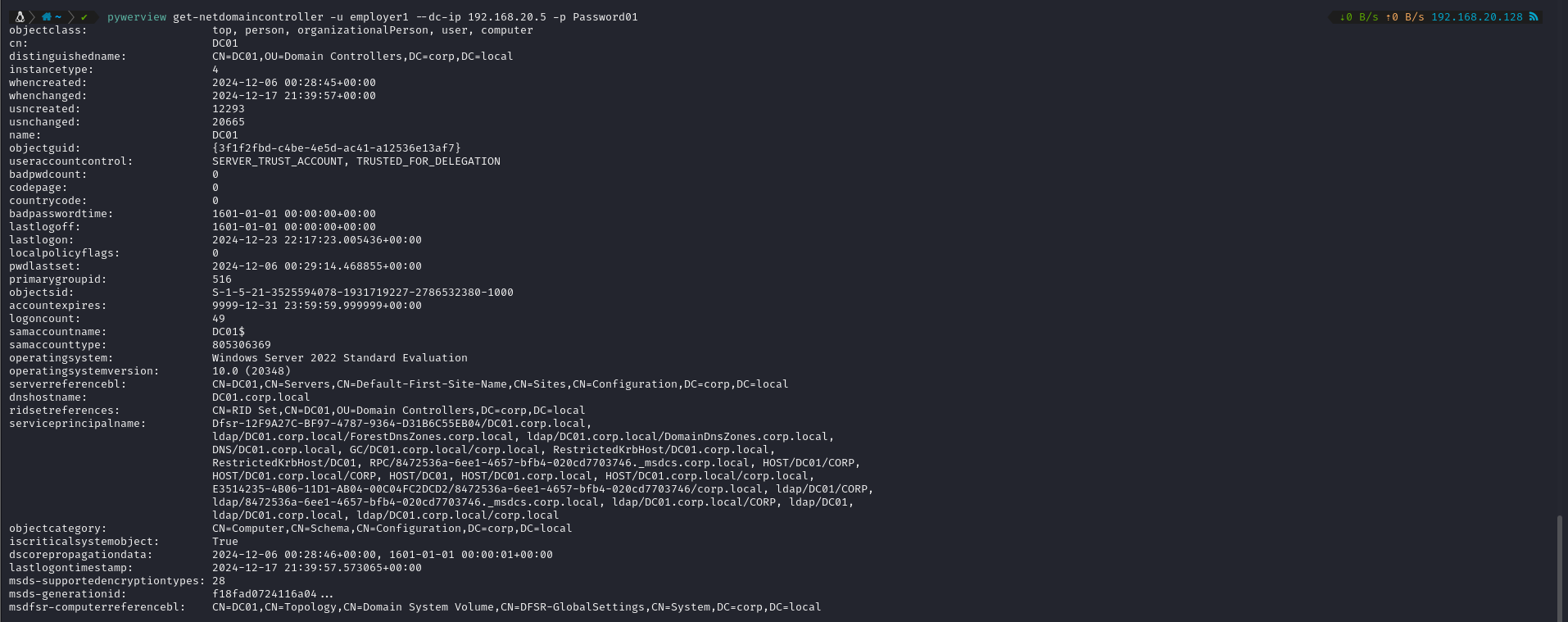
**pywerview get-netuser -u user --dc-ip 192.0.0.5 -p password:D**

This command will dump information about all domain users



**pywerview get-netdomaincontroller -u employer1 --dc-ip 192.168.20.5 -p Password01**

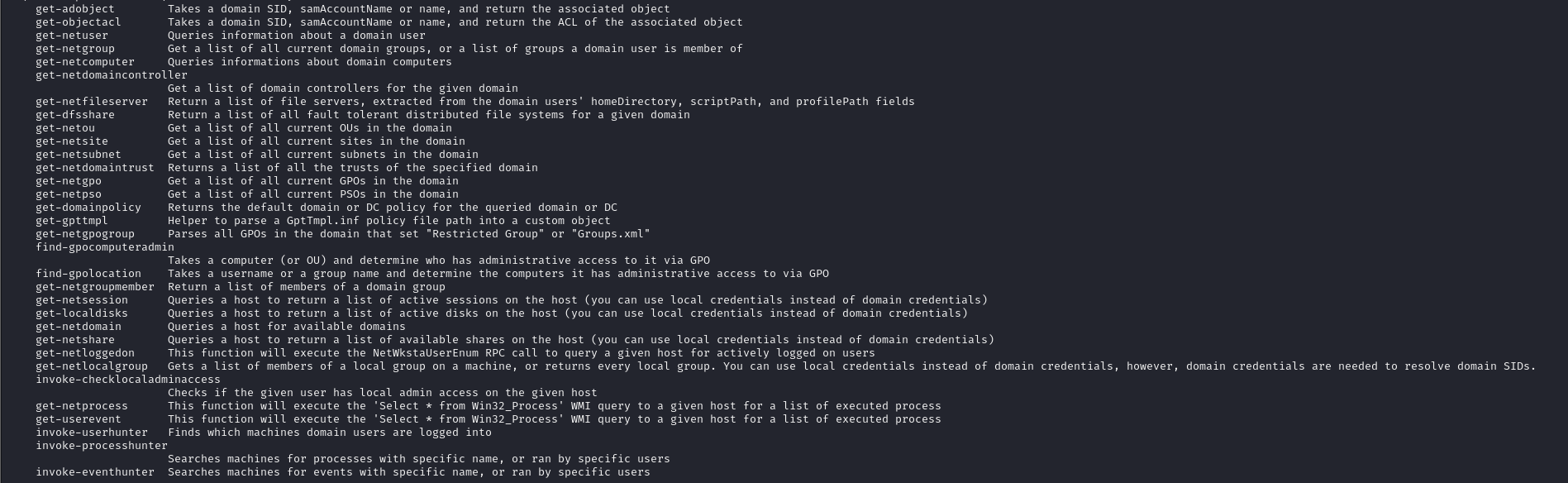
This command allows us gather information about the domain controller



**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**

****