RDP and SOCKS Tunneling with SocksOverRDP

There are often times during an assessment when we may be limited to a Windows network and may not be able to use SSH for pivoting. We would have to use tools available for Windows operating systems in these cases. SocksOverRDP is an example of a tool that uses `Dynamic Virtual Channels` (`DVC`) from the Remote Desktop Service feature of Windows. DVC is responsible for tunneling packets over the RDP connection. Some examples of usage of this feature would be clipboard data transfer and audio sharing. However, this feature can also be used to tunnel arbitrary packets over the network. We can use `SocksOverRDP` to tunnel our custom packets and then proxy through it. We will use the tool Proxifier as our proxy server.

We can start by downloading the appropriate binaries to our attack host to perform this attack. Having the binaries on our attack host will allow us to transfer them to each target where needed. We will need:

1. SocksOverRDP x64 Binaries

2. Proxifier Portable Binary

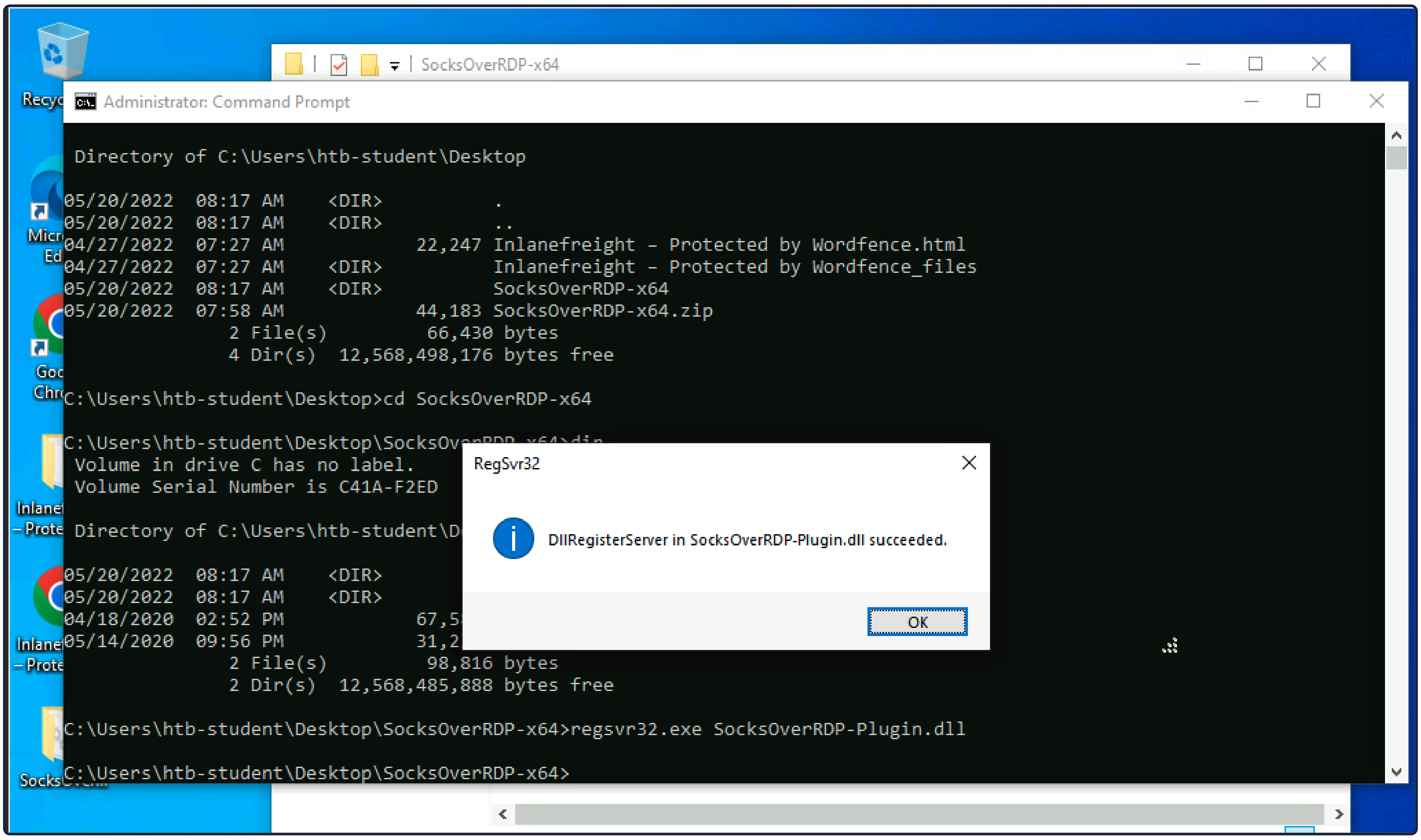
- We can look for `ProxifierPE.zip`

We can then connect to the target using xfreerdp and copy the `SocksOverRDPx64.zip` file to the target. From the Windows target, we will then need to load the SocksOverRDP.dll using regsvr32.exe.

Loading SocksOverRDP.dll using regsvr32.exe

Loading SocksOverRDP.dll using regsvr32.exe

```
C:\Users\htb-student\Desktop\SocksOverRDP-x64> regsvr32.exe SocksOverRDP-Plugin.dll
```



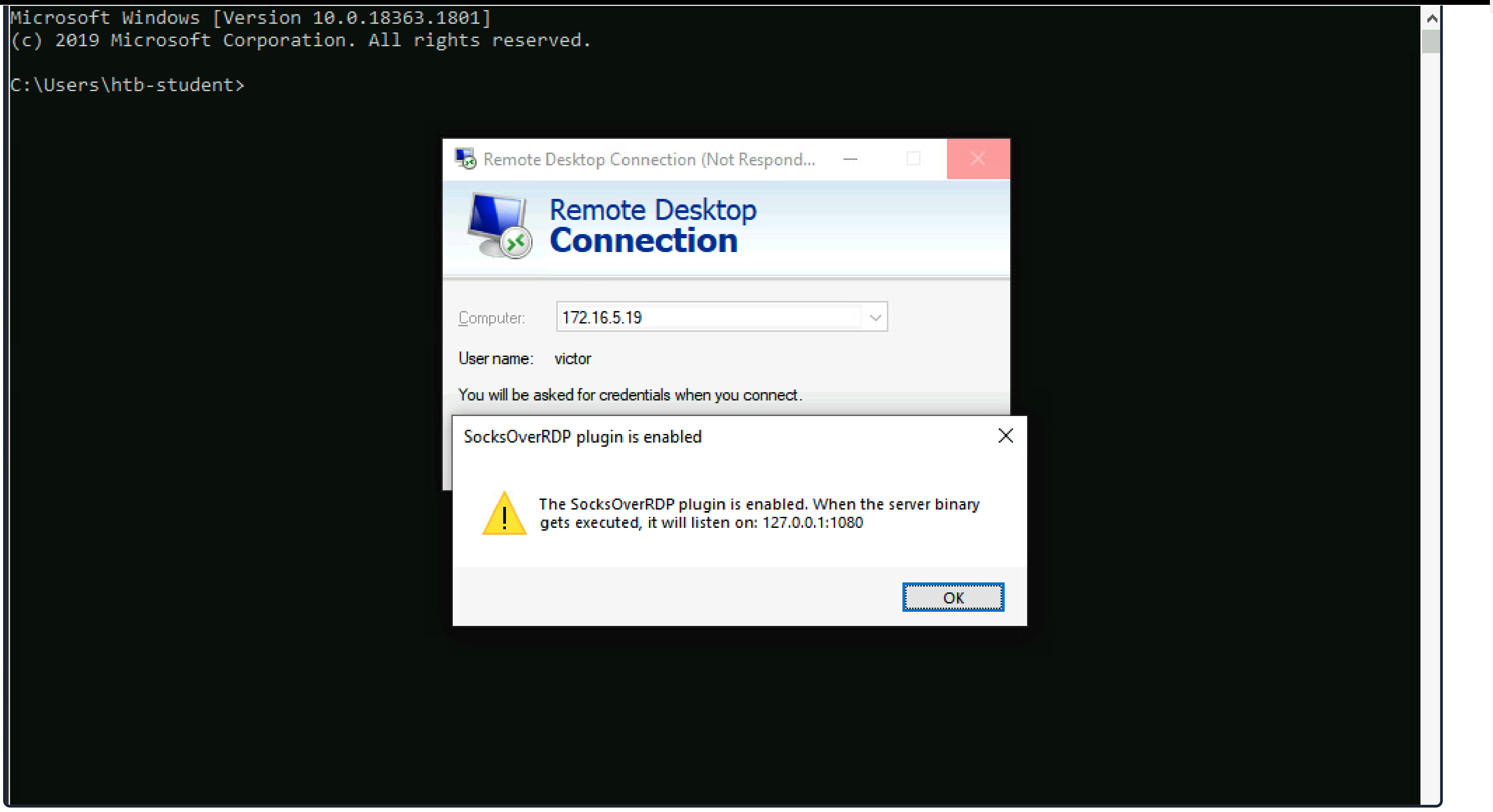
```
 Directory of C:\Users\htb-student\Desktop

05/20/2022  08:17 AM    <DIR>          .
05/20/2022  08:17 AM    <DIR>          ..
04/27/2022  07:27 AM            22,247 Inlanefreight - Protected by Wordfence.html
04/27/2022  07:27 AM    <DIR>          Inlanefreight - Protected by Wordfence_files
05/20/2022  08:17 AM    <DIR>          SocksOverRDP-x64
05/20/2022  07:58 AM            44,183 SocksOverRDP-x64.zip
               2 File(s)         66,430 bytes
               4 Dir(s)  12,568,498,176 bytes free

C:\Users\htb-student\Desktop>cd SocksOverRDP-x64

C:\Users\htb-student\Desktop\SocksOv
 Volume in drive C has no label.
 Volume Serial Number is C41A-F2ED

 Directory of C:\Users\htb-student\D

05/20/2022  08:17 AM    <DIR>
05/20/2022  08:17 AM    <DIR>
04/18/2020  02:52 PM            67,5
05/14/2020  09:56 PM            31,2
               2 File(s)         98,816 bytes
               2 Dir(s)  12,568,485,888 bytes free

C:\Users\htb-student\Desktop\SocksOverRDP-x64>regsvr32.exe SocksOverRDP-Plugin.dll

C:\Users\htb-student\Desktop\SocksOverRDP-x64>
```

RegSvr32

DllRegisterServer in SocksOverRDP-Plugin.dll succeeded.

Now we can connect to 172.16.5.19 over RDP using `mstsc.exe`, and we should receive a prompt that the SocksOverRDP plugin is enabled, and it will listen on 127.0.0.1:1080. We can use the credentials `victor:pass@123` to connect to 172.16.5.19.

Integrated Terminal



```
Microsoft Windows [Version 10.0.18363.1801]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\htb-student>
```

Remote Desktop Connection (Not Respond...
Remote Desktop
Connection

Computer: 172.16.5.19

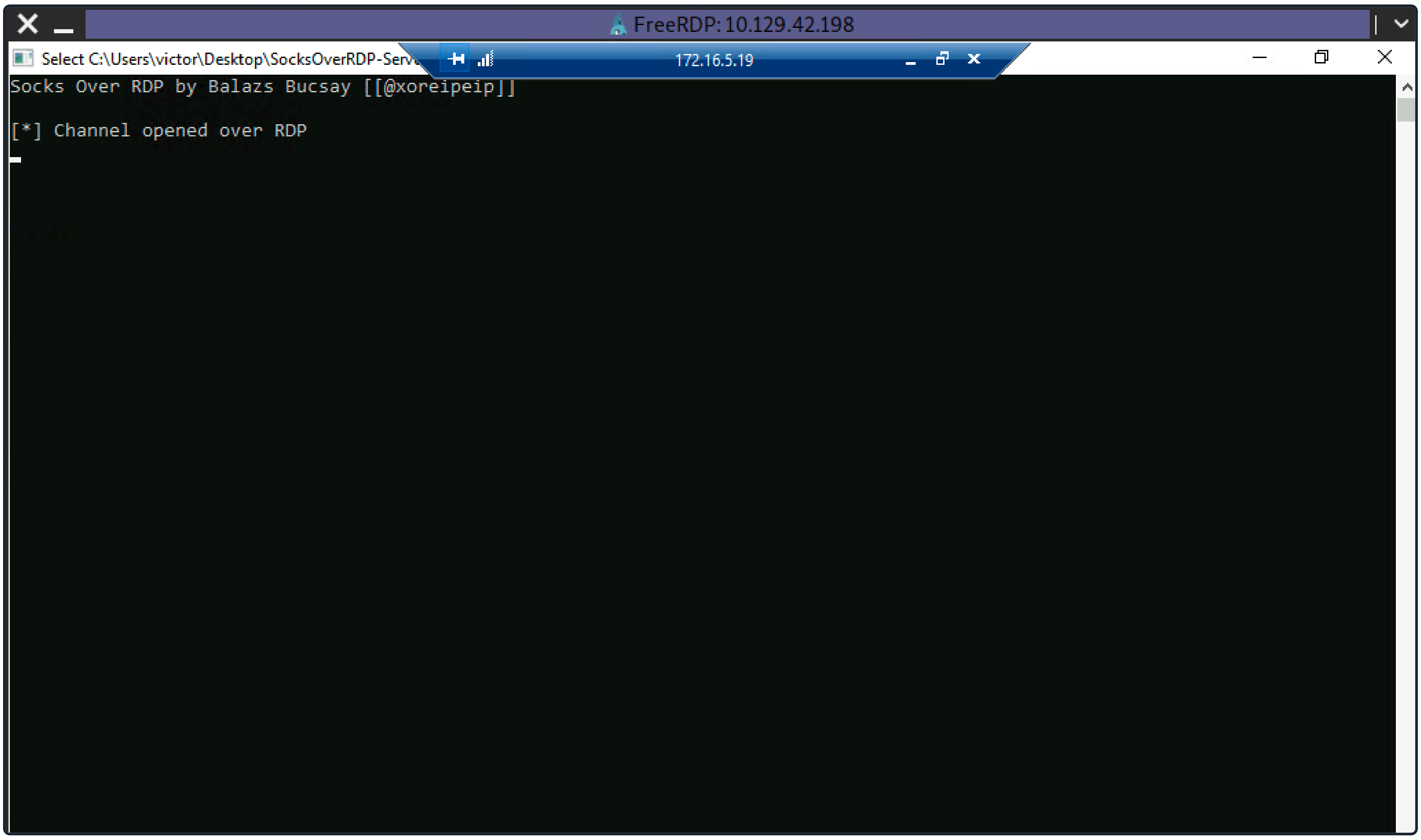
User name: victor

You will be asked for credentials when you connect.

SocksOverRDP plugin is enabled

The SocksOverRDP plugin is enabled. When the server binary gets executed, it will listen on: 127.0.0.1:1080

We will need to transfer SocksOverRDPx64.zip or just the SocksOverRDP-Server.exe to 172.16.5.19. We can then start SocksOverRDP-Server.exe with Admin privileges.



```
Socks Over RDP by Balazs Bucsay [[@xoreipeip]]

[*] Channel opened over RDP
```

When we go back to our foothold target and check with Netstat, we should see our SOCKS listener started on 127.0.0.1:1080.

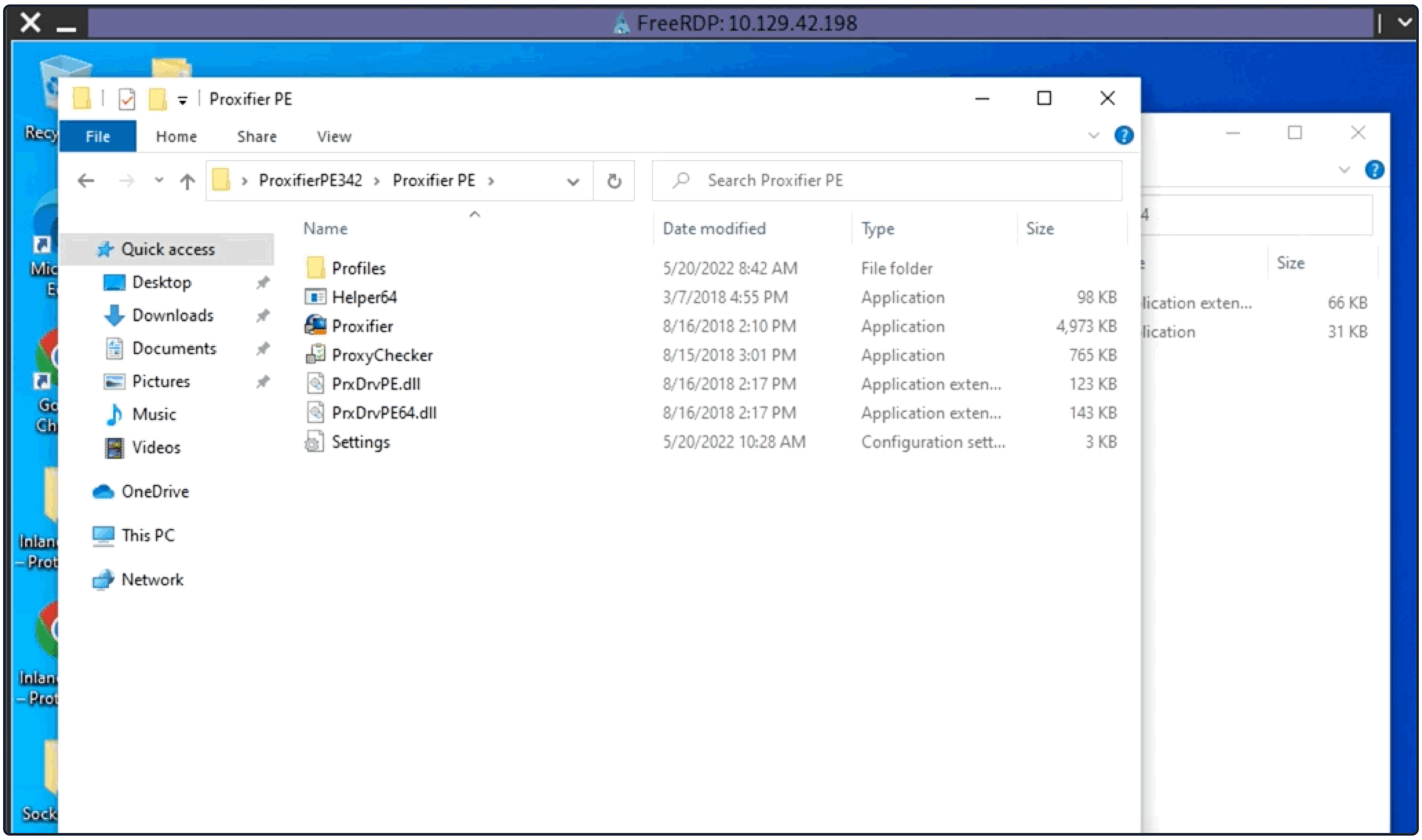
Confirming the SOCKS Listener is Started

Confirming the SOCKS Listener is Started

```
C:\Users\htb-student\Desktop\SocksOverRDP-x64> netstat -antb | findstr 1080

  TCP    127.0.0.1:1080         0.0.0.0:0              LISTENING
```

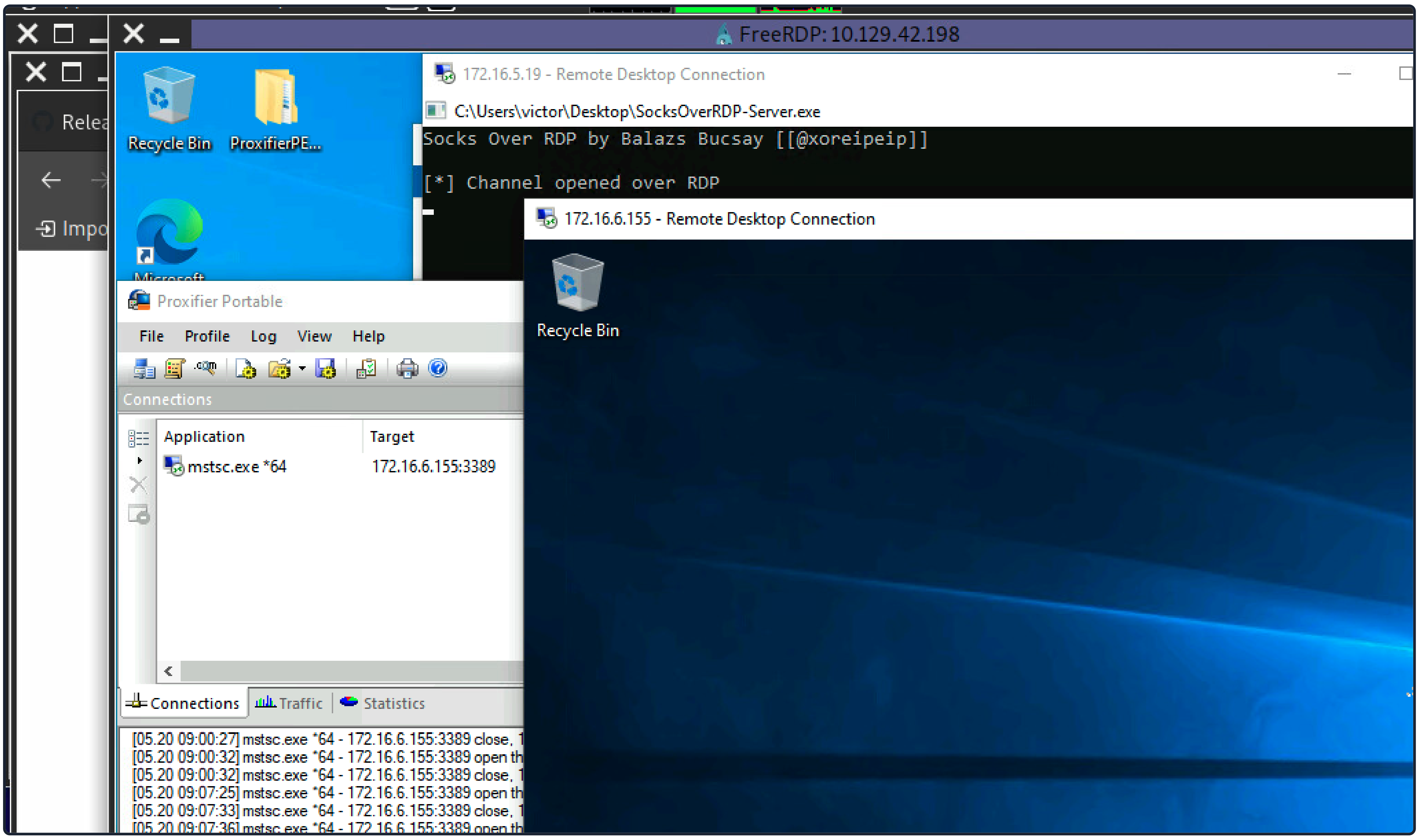
packets to 127.0.0.1:1080. Proxifier will route traffic through the given host and port. See the clip below for a quick walkthrough of configuring Proxifier.

Configuring Proxifier



Name	Date modified	Type	Size
Profiles	5/20/2022 8:42 AM	File folder	
Helper64	3/7/2018 4:55 PM	Application	98 KB
Proxifier	8/16/2018 2:10 PM	Application	4,973 KB
ProxyChecker	8/15/2018 3:01 PM	Application	765 KB
PrxDrvPE.dll	8/16/2018 2:17 PM	Application exten...	123 KB
PrxDrvPE64.dll	8/16/2018 2:17 PM	Application exten...	143 KB
Settings	5/20/2022 10:28 AM	Configuration sett...	3 KB

With Proxifier configured and running, we can start mstsc.exe, and it will use Proxifier to pivot all our traffic via 127.0.0.1:1080, which will tunnel it over RDP to 172.16.5.19, which will then route it to 172.16.6.155 using SocksOverRDP-server.exe.



FreeRDP: 10.129.42.198
Recycle Bin
ProxifierPE...
172.16.5.19 - Remote Desktop Connection
C:\Users\victor\Desktop\SocksOverRDP-Server.exe
172.16.6.155 - Remote Desktop Connection
Recycle Bin
Proxifier Portable
File
Profile
Log
View
Help
Connections
Traffic
Statistics

```
Socks Over RDP by Balazs Bucsay [[@xoreipeip]]

[*] Channel opened over RDP
```

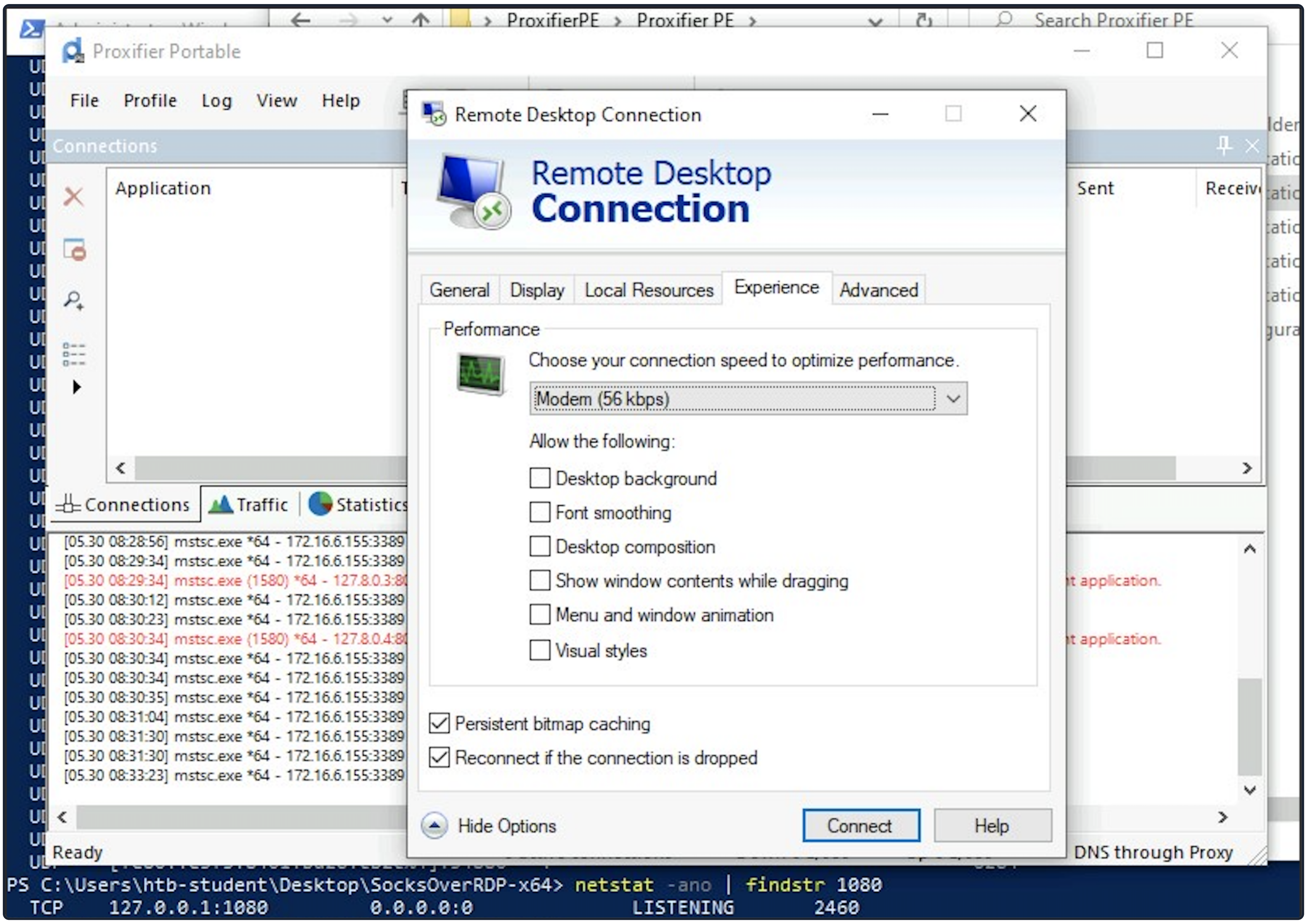
Application	Target
mstsc.exe *64	172.16.6.155:3389

```
[05.20 09:00:27] mstsc.exe *64 - 172.16.6.155:3389 close, 1
[05.20 09:00:32] mstsc.exe *64 - 172.16.6.155:3389 open th
[05.20 09:00:32] mstsc.exe *64 - 172.16.6.155:3389 close, 1
[05.20 09:07:25] mstsc.exe *64 - 172.16.6.155:3389 open th
[05.20 09:07:33] mstsc.exe *64 - 172.16.6.155:3389 close, 1
[05.20 09:07:36] mstsc.exe *64 - 172.16.6.155:3389 open th
```

RDP Performance Considerations

Integrated Terminal

especially if we are managing multiple RDP sessions simultaneously. If this is the case, we can access the `Experience` tab in mstsc.exe and set `Performance` to `Modem`.



Performance

Choose your connection speed to optimize performance.

Modem (56 kbps)

Allow the following:

- □ Desktop background
- □ Font smoothing
- □ Desktop composition
- □ Show window contents while dragging
- □ Menu and window animation
- □ Visual styles

☑ Persistent bitmap caching

☑ Reconnect if the connection is dropped

```
[05.30 08:28:56] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:29:34] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:29:34] mstsc.exe (1580) *64 - 127.8.0.3:8
[05.30 08:30:12] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:30:23] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:30:34] mstsc.exe (1580) *64 - 127.8.0.4:8
[05.30 08:30:34] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:30:34] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:30:35] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:31:04] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:31:30] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:31:30] mstsc.exe *64 - 172.16.6.155:3389
[05.30 08:33:23] mstsc.exe *64 - 172.16.6.155:3389
```

```
PS C:\Users\htb-student\Desktop\SocksOverRDP-x64> netstat -ano | findstr 1080
  TCP    127.0.0.1:1080         0.0.0.0:0              LISTENING       2460
```

Note: When spawning your target, we ask you to wait for 3 - 5 minutes until the whole lab with all the configurations is set up so that the connection to your target works flawlessly.

VPN Servers

⚠ Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

us-academy-1

PROTOCOL

UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Integrated Terminal