

## Table of Contents

Introduction .....	2
Lab Results .....	2
1. Port Scanning with Netcat .....	2
1.1 Kali virtual machine terminal window .....	2
1.2 Ports .....	2
2. Establishing Connections with Netcat .....	3
2.1 OpenSUSE Virtual machine. ....	3
2.2 Terminal application. ....	3
2.3 Root user. ....	3
2.4 Port 53 .....	3
2.5 Back to the Kali virtual machine terminal .....	4
2.6 Confirmation .....	4
2.6 OpenSUSE virtual machine terminal .....	4
3. Transferring Files with Netcat .....	5
3.1 OpenSUSE virtual machine terminal .....	5
3.2 Back to the Kali virtual machine terminal .....	5
3.3 File write out .....	6
3.4 File name to write .....	6
3.5 Exiting out of editor .....	6
3.6 testfile to OpenSUSE virtual machine .....	7
3.7 Back to the OpenSUSE virtual machine terminal .....	7
3.8 Current files .....	7
3.9 testfile .....	7

## Introduction

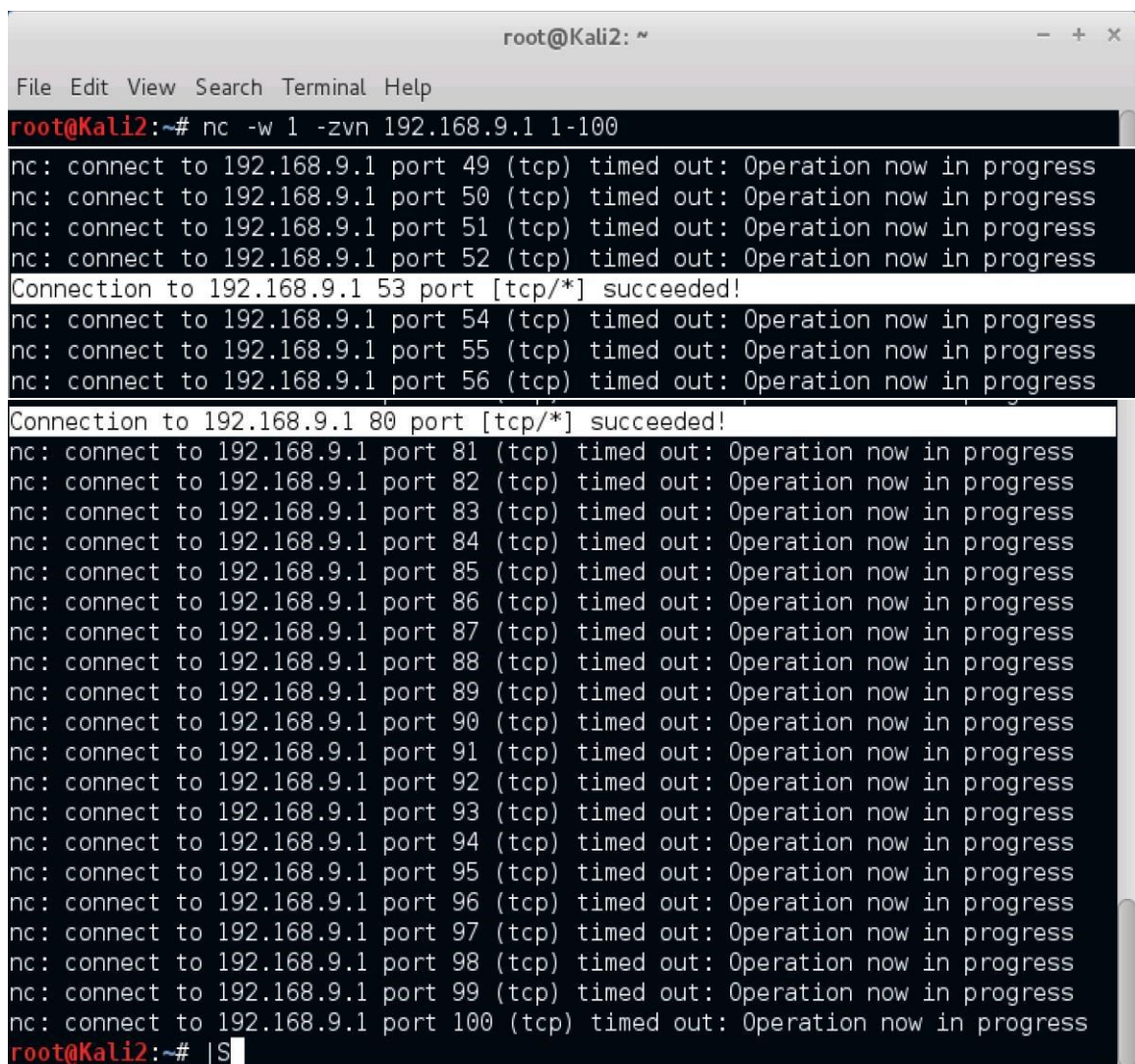
In most Linux distributions, Netcat is pre-installed. It may be used to execute different operations at the TCP/IP level. I'll use a variety of tools in this lab to undertake ethical hacking methods. Netcat port scanning, netcat connection establishment, and netcat File transferring.

## Lab Results

### 1. Port Scanning with Netcat

#### 1.1 Kali virtual machine terminal window

#### 1.2 Ports



```
root@Kali2: ~  
File Edit View Search Terminal Help  
root@Kali2:~# nc -w 1 -zvn 192.168.9.1 1-100  
nc: connect to 192.168.9.1 port 49 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 50 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 51 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 52 (tcp) timed out: Operation now in progress  
Connection to 192.168.9.1 53 port [tcp/*] succeeded!  
nc: connect to 192.168.9.1 port 54 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 55 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 56 (tcp) timed out: Operation now in progress  
Connection to 192.168.9.1 80 port [tcp/*] succeeded!  
nc: connect to 192.168.9.1 port 81 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 82 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 83 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 84 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 85 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 86 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 87 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 88 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 89 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 90 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 91 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 92 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 93 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 94 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 95 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 96 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 97 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 98 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 99 (tcp) timed out: Operation now in progress  
nc: connect to 192.168.9.1 port 100 (tcp) timed out: Operation now in progress  
root@Kali2:~# |$
```

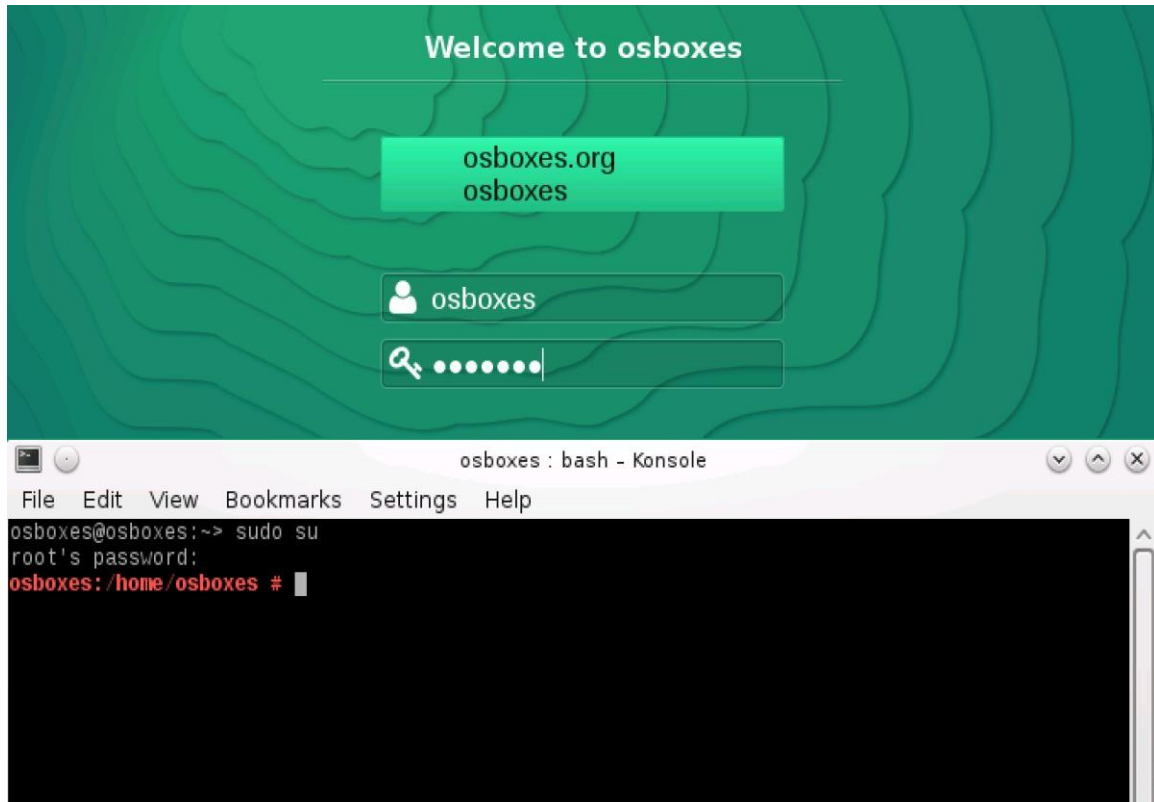
Command: `nc -w 1 -zvn 192.168.9.1 1-100` was used to scan for which outward facing ports were open on the firewall. The results shows that Ports 53 and 80 are open.

## 2. Establishing Connections with Netcat

### 2.1 OpenSUSE Virtual machine.

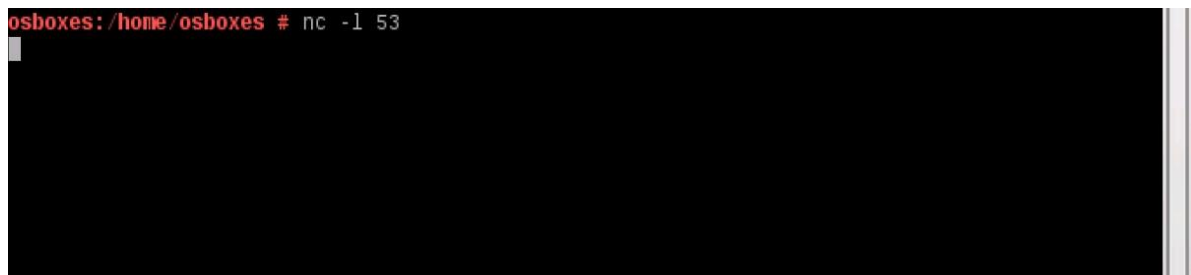
### 2.2 Terminal application.

### 2.3 Root user.



Command: **sudo su** was used to navigate the terminal as an administrator.

### 2.4 Port 53



In order to listen in on port 53, command: **nc -l 53** was used.

## 2.5 Back to the Kali virtual machine terminal

```
root@Kali2:~# nc 192.168.0.2 53
```

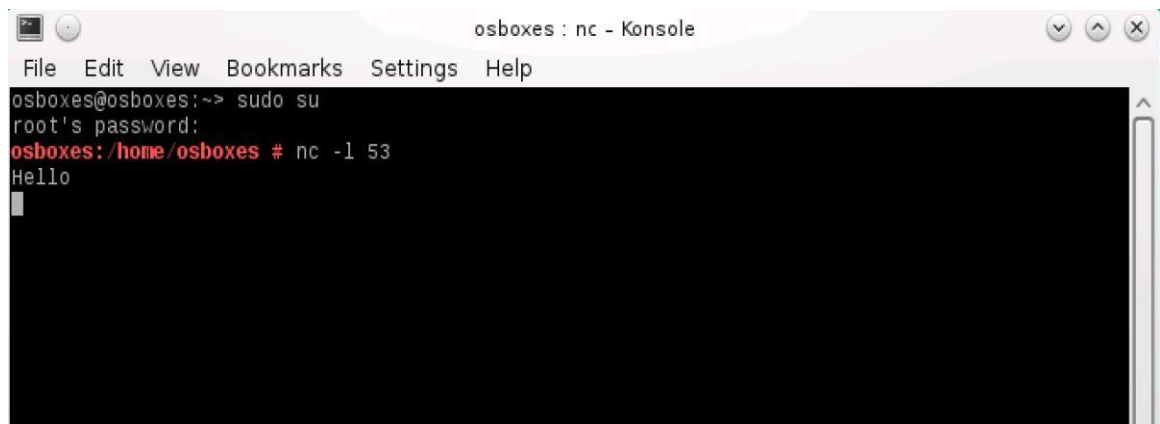
Command: **nc 192.168.0.2 53** was used to initiate a Netcat session to the IP address of the OpenSUSE virtual machine that is using port 53 to listen.

## 2.6 Confirmation

```
root@Kali2:~# nc 192.168.0.2 53
Hello
```

Typed the word **Hello** followed by pressing the **Enter** key. Command used: **Hello**

## 2.6 OpenSUSE virtual machine terminal

A screenshot of a terminal window titled "osboxes : nc - Konsole". The window has a menu bar with "File", "Edit", "View", "Bookmarks", "Settings", and "Help". The terminal content shows the user "osboxes" at the prompt "osboxes@osboxes:~>" running the command "sudo su". This prompts for "root's password:". The user then runs "nc -l 53" at the "osboxes:/home/osboxes #" prompt. The terminal receives the message "Hello" and shows a cursor on the next line.

```
osboxes@osboxes:~> sudo su
root's password:
osboxes:/home/osboxes # nc -l 53
Hello
```

The text message (**Hello**) sent by the Kali virtual machine has been received by the OpenSUSE virtual machine. Thereby indicating that a connection has been established through the firewall. I pressed **CTRL+C** to stop the Netcat application and connection.

### 3. Transferring Files with Netcat

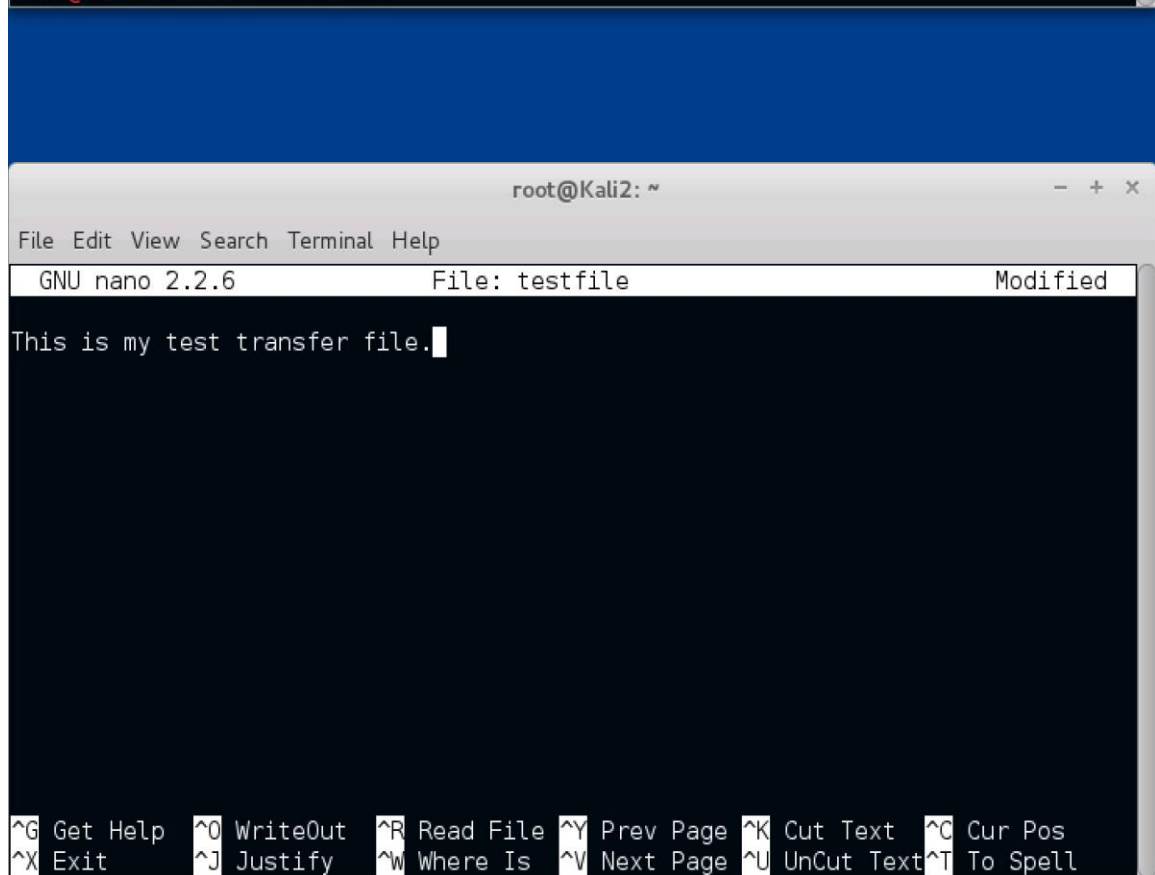
#### 3.1 OpenSUSE virtual machine terminal

```
osboxes:/home/osboxes # nc -l 53 > testfile
```

Command used: nc -l 53 > testfile

#### 3.2 Back to the Kali virtual machine terminal

```
root@Kali2:~# nano testfile
```



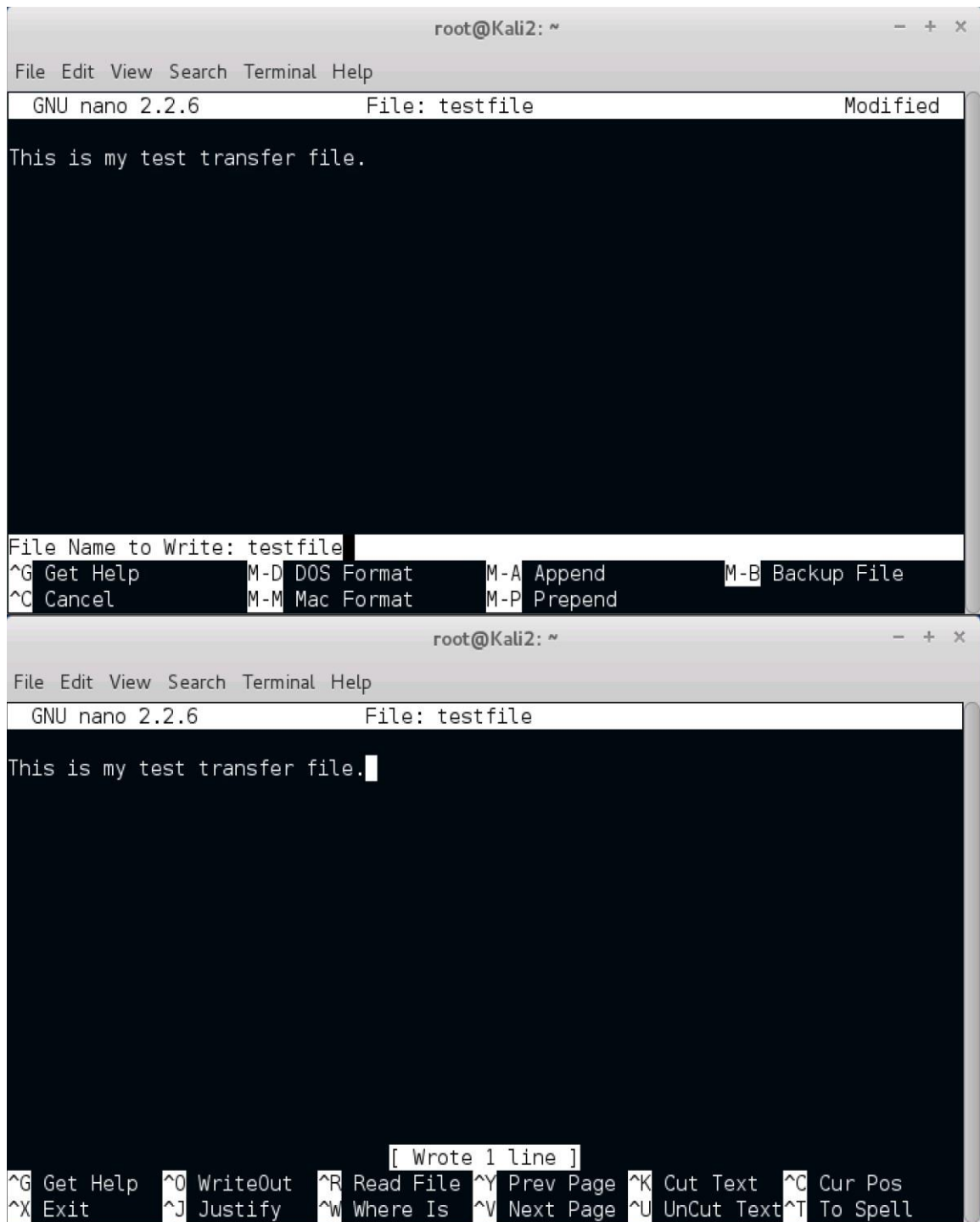
The screenshot shows the Nano text editor interface. At the top, the title bar reads 'root@Kali2: ~'. Below it is a menu bar with 'File Edit View Search Terminal Help'. The status bar shows 'GNU nano 2.2.6 File: testfile Modified'. The main editing area contains the text 'This is my test transfer file.' followed by a cursor. At the bottom, a help bar lists keyboard shortcuts: ^G Get Help, ^O WriteOut, ^R Read File, ^Y Prev Page, ^K Cut Text, ^C Cur Pos, ^X Exit, ^J Justify, ^W Where Is, ^V Next Page, ^U UnCut Text, and ^T To Spell.

Command used: nano testfile, this command opens the Nano editor.

### 3.3 File write out

### 3.4 File name to write

### 3.5 Exiting out of editor



The image shows two screenshots of the nano text editor interface. The top screenshot shows the editor with the text "This is my test transfer file." and a prompt "File Name to Write: testfile" at the bottom. The bottom screenshot shows the editor with the same text and a status bar at the bottom indicating "[ Wrote 1 line ]".

```
root@Kali2: ~  
File Edit View Search Terminal Help  
GNU nano 2.2.6 File: testfile Modified  
This is my test transfer file.  
File Name to Write: testfile  
^G Get Help ^M-D DOS Format ^M-A Append ^M-B Backup File  
^C Cancel ^M-M Mac Format ^M-P Prepend  
root@Kali2: ~  
File Edit View Search Terminal Help  
GNU nano 2.2.6 File: testfile  
This is my test transfer file.  
[ Wrote 1 line ]  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Pressed **CTRL+O** to write out the file.  
Noticed that the prompt at the bottom prompted for what **File Name to Write** and pressed the **Enter** key. Lastly, pressed **CTRL+X** to exit the editor.

### 3.6 testfile to OpenSUSE virtual machine

```
root@Kali2:~# nc -w 3 192.168.0.2 53 < testfile
root@Kali2:~#
```

Command used: nc -w 3 192.168.0.2 53 < testfile

### 3.7 Back to the OpenSUSE virtual machine terminal

#### 3.8 Current files

```
osboxes:/home/osboxes # ls
.ICEauthority  .emacs          .macromedia      .xim.template    Pictures
.Xauthority    .esd_auth       .mozilla         .xinitrc.template Public
.adobe         .fonts          .oracle_jre_usage .xsession-errors Templates
.bash_history  .gnupg          .pki             .xsession-errors-:0 Videos
.bashrc        .gstreamer-0.10 .profile         .y2log           bin
.cache         .gtkrc-2.0      .qt             .y2usersettings public_html
.config        .inputrc        .skel            Desktop          testfile
.dbus          .kde            .thumbnails     Documents
.directory    .kde4           .viminfo        Downloads
.dmrc         .local          .vnc            Music
```

To list the current files in the directory, **ls** command was used. The **testfile** is listed.

#### 3.9 testfile

```
osboxes:/home/osboxes # cat testfile
This is my test transfer file.
osboxes:/home/osboxes #
```

Command: **cat testfile** was used to verify the contents of the file; **testfile**.