ETHICAL HACKING V2
LAB SERIES

Lab 15: Backdooring with Netcat

Document Version: 2020-08-24

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	2: Trojans and Other Attacks
EC-Council CEH v10 Domain Modules	7: Malware Threats 10: Denial-of-Service 11: Session Hijacking
CompTIA Pentest+ Objectives	3.5: Given a scenario, exploit local host vulnerabilities 3.7: Given a scenario, perform post-exploitation techniques 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	4: Vulnerability Scanning and Analysis 9: Web and Database Attacks 10: Attacking Local Host Vulnerabilities

Contents

Introduction

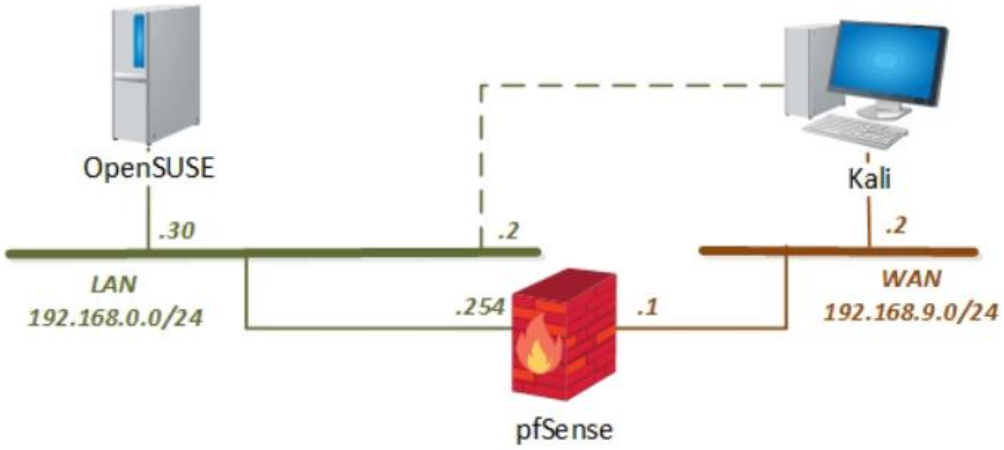
Netcat is installed in most Linux distributions. It can be used at a fundamental TCP/IP level to perform various functions. This lab explores some of the ways Netcat can be used.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Port Scanning with Netcat
2. Establishing Connections with Netcat
3. Transferring Files with Netcat

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OpenSUSE	192.168.0.30	osboxes	osboxes.org

1 Port Scanning with Netcat

1. Click on the **Kali** tab.
2. Click within the console window, and press **Enter** to display the login prompt.
3. Enter **root** as the *username*. Press **Tab**.
4. Enter **toor** as the *password*. Click **Log In**.
5. Open a new terminal by clicking on the **Terminal** icon located at the top of the page, if the terminal is not already opened.
6. In the new *Terminal* window, type the command below to scan for which outward-facing ports are open on the firewall. Press **Enter**.

```
nc -w 1 –zvn 192.168.9.1 1-100
```

```
root@kali:~# nc -w 1 -zvn 192.168.9.1 1-100
(UNKNOWN) [192.168.9.1] 100 (?) : Connection timed out
(UNKNOWN) [192.168.9.1] 99 (?) : Connection timed out
(UNKNOWN) [192.168.9.1] 98 (?) : Connection timed out
(UNKNOWN) [192.168.9.1] 97 (?) : Connection timed out
```

This command instructs Netcat to do the following:

-w: wait one second
-z: port scanning mode
-v: verbose
-n: don't use DNS lookups
1-100: port range to scan

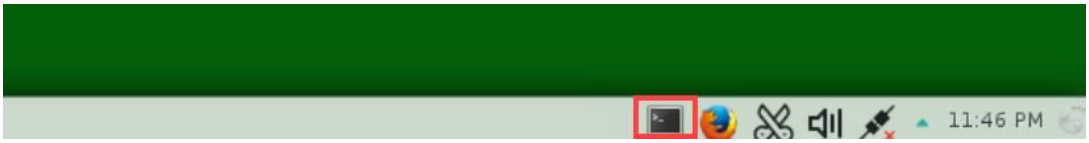
7. From the output, notice that ports 53 and 80 are open.

```
(UNKNOWN) [192.168.9.1] 81 (?) : Connection timed out
(UNKNOWN) [192.168.9.1] 80 (http) open
(UNKNOWN) [192.168.9.1] 79 (finger) : Connection timed out
```

```
(UNKNOWN) [192.168.9.1] 54 (?) : Connection timed out
(UNKNOWN) [192.168.9.1] 53 (domain) open
(UNKNOWN) [192.168.9.1] 52 (?) : Connection timed out
```


2 Establishing Connections with Netcat

1. Click on the **OpenSUSE** tab.
2. Enter **osboxes** as the *username* and **osboxes.org** as the *password*. Press **Enter**.
3. Open a new **Terminal** by clicking on the icon in the lower-right.



4. Change to the *root* user by typing the command below, followed by pressing **Enter**.

```
sudo su
```

5. When prompted for *root's password*, enter **osboxes.org**. Press **Enter**.
6. Type the *Netcat* command below to listen on port 53.

```
nc -l 53
```

7. Navigate back to the **Kali** PC viewer.
8. Using the terminal, enter the command below to initiate a *Netcat* session to the IP address of the *OpenSUSE* VM using port 53, which is set to listen.

```
nc 192.168.0.30 53
```

There is no confirmation.

9. Type the word **Hello** followed by pressing the **Enter** key.

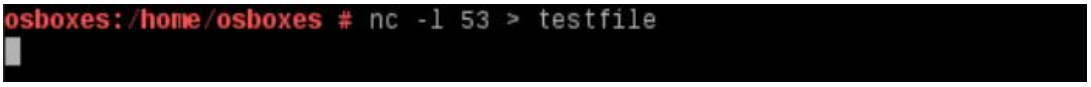
10. Navigate back to the **OpenSUSE** tab.

11. Focus on the **Terminal** with *Netcat* running and notice that the *Hello* text is visible. It can be confirmed that a connection has been established through the firewall. Press **CTRL+C** to stop the *Netcat* application and to close the connection.

3 Transferring Files with Netcat

1. While on the *OpenSUSE* VM, type the command below into the *Terminal*.

```
nc –l 53 > testfile
```

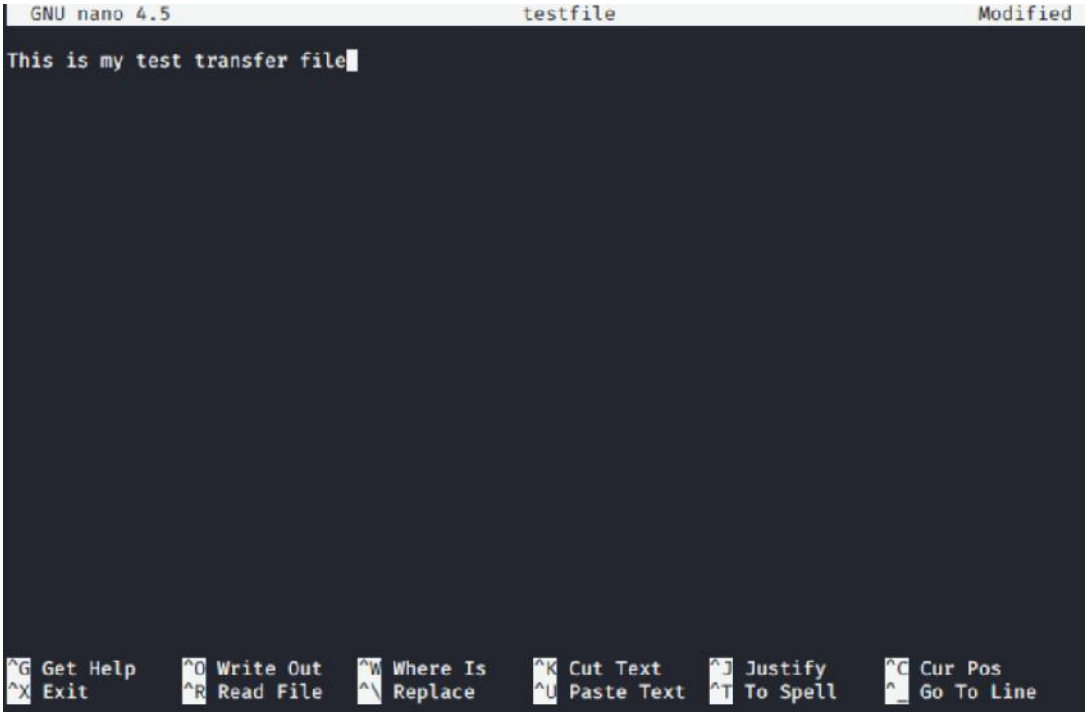


The cursor will wait for a connection.

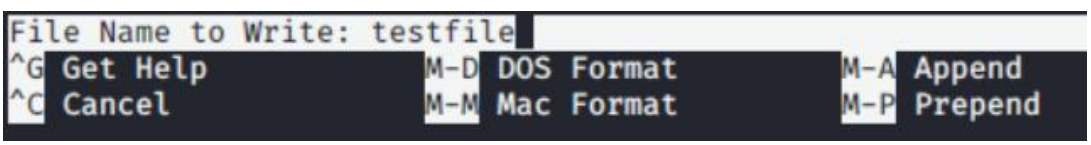
2. Click on the **Kali** tab.
3. Enter the command below using the *Terminal*.

```
nano testfile
```

4. When the *Nano* editor opens, type **`This is my test transfer file`**.



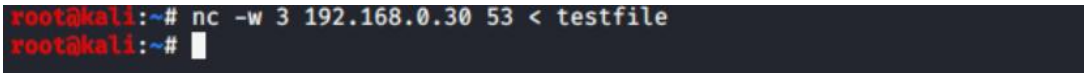
5. Press **CTRL+O** to write out the file.
6. Notice the prompt at the bottom. When prompted for *File Name to Write*, press the **Enter** key.



7. Pres **CTRL+X** to exit the editor.

8. Type the command below, followed by pressing the **Enter** key to send the *testfile* to the *OpenSUSE* VM.

```
nc –w 3 192.168.0.30 53 < testfile
```

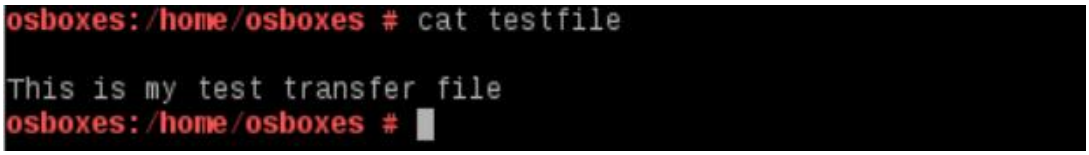


9. Switch to the **OpenSUSE** VM. Wait for the prompt to reappear.
10. Using the *Terminal*, enter the command below to list the current files in the directory.

```
ls
```

11. Notice the *testfile* is listed. Enter the command below to verify the contents of the file.

```
cat testfile
```



12. You may now end your reservation.

