ETHICAL HACKING
LAB SERIES

Lab 9: Backdooring with Netcat

Material in this Lab Aligns to the Following Certification Domains/Objectives	
Certified Ethical Hacking (CEH) Domains	SANS GPEN Objectives
5: System Hacking	9: Moving Files with Exploits

Document Version: 2018-11-05

Contents

Introduction

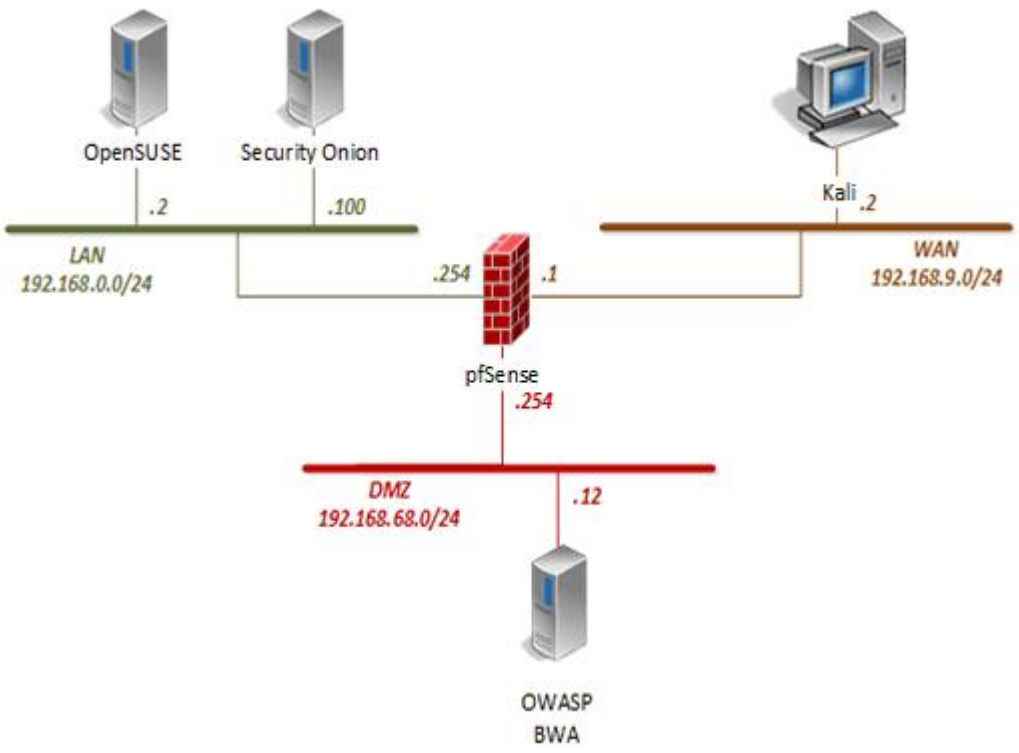
Netcat is installed in most Linux distributions. It can be used at a fundamental TCP/IP level to perform various functions. This lab explores some of the ways Netcat can be used.

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	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Port Scanning with Netcat

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter **`root`** as the *username*. Click **Next**.
4. Enter **`toor`** as the *password*. Click **Sign In**.
5. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.

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
```

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

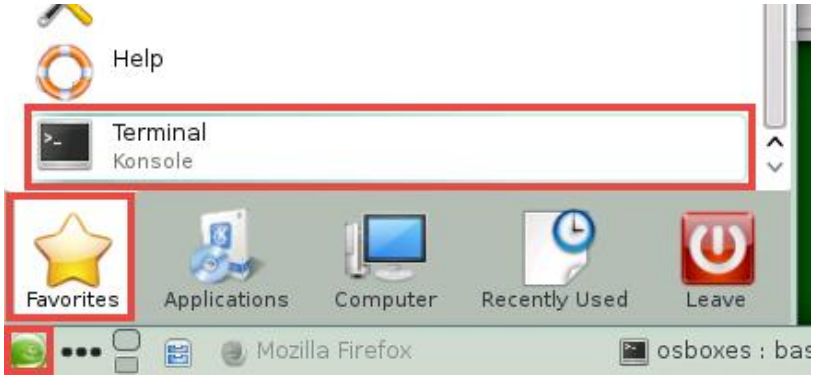
7. From the output, notice that ports 53 and 80 are open.

```
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 79 (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
```


2 Establishing Connections with Netcat

1. Navigate to the topology page and click on the **OpenSUSE** icon.
2. Enter **osboxes** as the *username* and **osboxes.org** as the *password*. Press **Enter**.
3. Open a new **Terminal** from the *Application Launcher* while on the *OpenSUSE* VM.

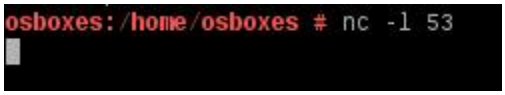


4. Change to the *root* user by typing the command below followed by pressing **Enter**.

```
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
```

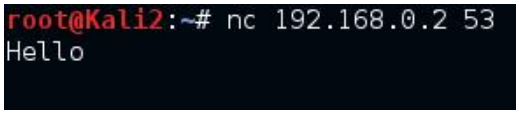


7. Navigate back to the **Kali** PC viewer.
8. Using the terminal, enter the command below to initiate a *Netcat* session to the IP address of the *OpenSUSE* VM using port 53 which is set to listen.

```
nc 192.168.0.2 53
```

The cursor will blink, indicating that it is waiting for an incoming connection. There is no confirmation.

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



10. Navigate back to the **OpenSUSE** PC viewer.

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**.

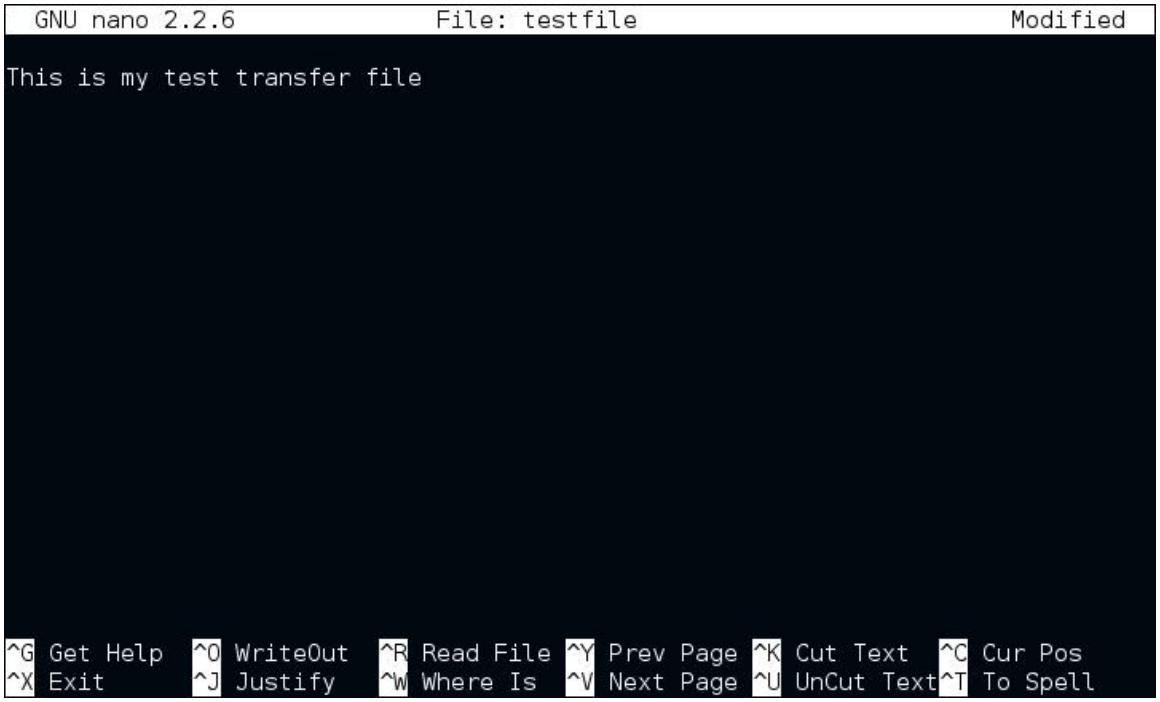
```
nc –l 53 > testfile
```

The cursor will wait for a connection.

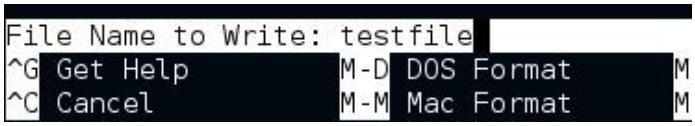
2. Change focus to the **Kali** VM.
3. Enter the command below using the **Terminal**.

```
nano testfile
```

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



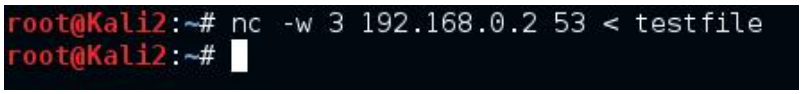
5. Press **CTRL+O** to write out the file.
6. Notice the prompt at the bottom. When prompted for *File Name to Write*, press the **Enter** key.



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 3 192.168.0.2 53 < testfile
```



9. Switch to the **OpenSUSE** VM.
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. Close the **OpenSUSE** and **Kali** PC viewers.

