Lab – Creating a Sandboxed Penetration Testing Environment

# Lab Purpose

This lab will assist you in creating two virtual machines – Kali Linux and Metasploitable 2. They will be put on the same virtual closed network to allow for sandboxed penetration testing practice.

# Learning Outcomes

1. Configure two virtual machines on the same virtual network
2. Understand the significance of a sandboxed network environment

## Relevant NICE Cybersecurity Framework Version NIST 800-181, TASKS and KSAs (<https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>)

|  |  |
| --- | --- |
| **TASK(S)** | T0028 |
| **Knowledge ID** | K0001, K0005, K0109, K0177, K0224, K0342, K0362 |
| **Skill ID** | S0204, S0258, S0264, S0294 |
| **Ability ID** | A0086, A0092 |

Environment

1. You should have already received instructions on logging into the lab environment from your instructor
2. Any computer with Internet access should work. Latest versions of Chrome and Firefox browsers are preferable.

## Background Knowledge

1. You should have completed “Lab – Getting Started with OpenStack”

# Lab Task 1: Create Kali Linux and Metasploitable Virtual Machines

1. Login into OpenStack Horizon Dashboard
2. You will create two virtual machine instances – Kali Linux and Metasploitable. The steps for creating instances of Kali and Metasploitable are very similar to “Lab – Getting Started with Openstack”. Follow those steps, using Kali and Metasploitable images instead of the Ubuntu image.
3. Make sure you assign both instances to the same network for now. You may later choose to deploy the attack machine (Kali) and the target machine (Metasploitable) in separate networks to make it a bit more challenging

# Lab Task 2: Launch the Instances and Confirm a Proper Network Configuration

## Login to the instances

1. Launch and login to both machines. The default login for Kali Linux is:

User: root

Password: toor

For Metasploitable it is:

User: msfadmin

Password: msfadmin

However, it is possible the sysadmin may have changed these defaults.

## Confirm network settings

1. In the Kali instance, open a terminal window and use the command line to determine the Kali virtual machine ip address:

root@kali: # ifconfig <enter>

In the output, you should see a line similar to this:

inet 192.168.174.137 netmask 255.255.255.0 broadcast 192.168.174.255

In this case, the IP address for the Kali virtual machine is 192.168.174.137 (the number will most likely be different for you own machine). Use the same command in Metasploitable to determine it’s IP address as well. These two IP address have been arbitrarily assigned by the Dynamic Host Configuration Protocol (DHCP) Server that you created during the process of creating a virtual network. Make a note of the Metasploitable IP address. You will be using it during penetration testing of the intentionally vulnerable Metasploitable virtual machine.

1. You are now ready to begin developing your penetration skills in a sandboxed environment.
2. You may start by conducting basic enumeration and fingerprinting. A nice introduction is available here: <https://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-enumeration/>

# Submission Instructions

This lab has no submission requirements.

# Further Learning/Links/Resources

1. <https://www.kali.org/kali-linux-documentation/>
2. <https://www.offensive-security.com/metasploit-unleashed/>
3. <https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide>
4. <https://www.hackingtutorials.org/metasploit-tutorials/>
5. “Awesome Pentesting Resources” <https://github.com/enaqx/awesome-pentest>