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, 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 1 – Getting Started with Openstack”

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

1. Login into OpenStack Horizon Dashboard
2. The steps for creating instances of Kali and Metasploitable are very similar to Lab 1. Follow those steps, using Kali and Metasploitable images instead of the Ubuntu image. Make sure when you assign both instances to the same network (the one you already created in Lab 1)

# 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, you will be

# Submission Instructions

This lab has no submission requirements.

# Further Learning/Links/Resources

1. https://