

Assignment Report

Kali Linux & Metasploitable 2

Prepared by:R.Deepak Kumar

Date: 2/3/2024

Executive Summary:

The purpose of this report is to document the setup of a hacker lab, including the installation of Linux, VirtualBox, and Metasploitable 2. The lab consists of an attacker machine (Linux) and a victim machine (Metasploitable 2). The report provides step-by-step instructions for each component of the setup. It is essential to note that this lab is intended for educational and testing purposes only, and ethical considerations should be taken into account while using it.

Linux Installation using VMware:

VMware Installation:

Download and install VMware Workstation Player from the VMware website.

Download Linux ISO:

Choose a Linux distribution (e.g., Ubuntu) and download the ISO image from the respective website.

Create a New Virtual Machine:

Open VMware, create a new virtual machine, and select the Linux ISO as the installer disc image.

Install Linux:

Follow on-screen instructions to install Linux on the virtual machine.

Linux Installation using VirtualBox:

VirtualBox Installation:

Download and install VirtualBox from the official website.

Download Linux ISO:

Choose a Linux distribution and download the ISO image from the respective website.

Create a New Virtual Machine:

Open VirtualBox, create a new virtual machine, allocate RAM, and create a virtual hard disk.

Configure Virtual Machine Settings:

Attach the Linux ISO to the virtual machine and adjust other settings as needed.

Install Linux:

Start the virtual machine and follow the Linux distribution's installer prompts.

Metasploitable 2 Installation using VMware:

Download Metasploitable 2:

Download the Metasploitable 2 VM from a trusted source in OVA format.

Install VMware:

Download and install VMware Workstation Player or VMware Workstation Pro.

Import Metasploitable 2 into VMware:

Open VMware, import the Metasploitable 2 OVA file, and configure settings.

Network Configuration:

Isolate Metasploitable 2 by configuring the network adapter to use "Host-only" or "NAT."

Start the Virtual Machine:

Start the Metasploitable 2 VM, note its IP address, and use penetration testing tools to explore vulnerabilities.