Trevor Kulczycki-McIntyre

Nathaniel Bitton

Karl Alvarado

Penetration Tests

Unix-Winter-2024

LIA-Project

# Part 1: Introduction

## What is Penetration Testing?

Penetration Testing is a cybersecurity technique where simulated attacks are conducted on a computer system, network or application to identify vulnerabilities and assess security.

## Purpose of this Project

The purpose of this project is not to discover new vulnerabilities, it is to exploit known ones in a step-by-step tutorial where we will document the challenges we faced, and how we overcame them.

# Part 2: Getting Started

## Downloading Kali Linux (Attacker)

Go to [osboxes.org](https://www.osboxes.org/) and download the most recent version of Kali Linux.

Kali Linux is a well-known Debian based OS widely used for simulating penetration tests and other cyber security assessments.

In this example we will use VirtualBox as our hypervisor however, VMWare is another viable option, just make sure you download the right image from osboxes.org.

## Create a Virtual Machine with Kali VDI file

Inside your hypervisor create a new virtual machine using the Kali Linux .VDI file that was downloaded in the previous step.

### On VirtualBox

New ->

Set the name for your VM, it doesn’t really matter

Type: Linux

Version: Debian 64-bit (since kali is a Debian based OS)

Expert Mode ->

Hard-Disk -> Use and Existing Hard Disk file

* Small folder icon will show you the current vdi files that were added (if any), since we just downloaded it, it should not appear here. Click on add

Add your .vdi file, select it and click choose in the bottom right.

After selecting your .vdi file, go to hardware (still in expert mode) and allocate a desired amount of RAM and CPUs to your VM. For mine, I chose around 5Gb of Ram and 1 CPU.

Press Finish

## Boot it Up!

Now that everything is configured, click on start and after logging in

Username: osboxes

Password: osboxes.org

You should be presented with the following screen A computer screen shot of a logo

Description automatically generated

Congrats! You’ve successfully installed Kali Linux!

## Downloading the Victim (Metasploitable 2)

The victim of our attacks is going to be Metasploitable 2. I’ve decided to use this VM since it is a well-known machine to perform penetration tests on, as it was designed to do so.

To download Metasploitable 2, go to <https://sourceforge.net/projects/metasploitable/files/latest/download> and download the .zip file.

A screenshot of a computer

Description automatically generatedAfter that, go into VirtualBox and create a VM with the VDI inside of the zip file, you do not need to allocate much RAM since there is no GUI. ~500 Mb will suffice however in my example I use 1000mb just to be safe.

### \*Network Configuration

On both virtual machines, make sure that in the Network settings, located in virtualbox, are set to bridged adapter, and promiscuous mode is set to allow all.

A screenshot of a computer

Description automatically generated

### Boot it up!

A screenshot of a computer

Description automatically generated

Congrats! You have successfully downloaded Metasploitable! Now lets get to the good stuff 😉

# Part 3: Start Hacking!

## Setup

This phase requires both virtual machines to be running on the host machine at the same time. Make sure that you carefully followed each previous step.

## Reconnaissance

The first step for any good hacker is always the recon phase. You need to scope out the environment to see what options are available.

In the Metasploitable VM run the command $ifconfig

This command is used to configure networks in Unix like systems, but for now we will just be using it to see the IP Address of the victim.

A screenshot of a computer

Description automatically generated

Here we see that the inet address of my Metasploitable VM is 192.168.2.26

This is what we’ll need to commence the hacking stage.

Now inside of Kali Linux open the terminal and run $sudo nmap -sV -O <ip address of victim>

Nmap is a tool used for scanning networks, -sV will show the version, and -O will show the operating system

A computer screen shot of a computer program

Description automatically generated

This will give you a sum of the vulnerabilities inside of the Metasploitable VM.

Alternatively, you can download Nessus, a vulnerability scanner available for download at <https://www.tenable.com/downloads/nessus?loginAttempted=true> on Kali Linux.

Make sure to download the version for Linux-Debian-amd64

After downloading, run the following command to install A screenshot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

Make sure you run the command in the same directory that you’ve downloaded the file, default is the downloads directory.

Now after a successful installation, start the service with:



And enable the service with



Now that the service is running, open the web browser and navigate to <https://localhost:8834>, it will give a security error, just press accept and continue.

A screenshot of a computer

Description automatically generated

Choose Online registration 🡪 Register for Nessus essentials, use your student email as it works as a business email, else you will have to pay for a business email.

After filling out the fields you will see your activation code appear on the screen, copy it. Create an account

A screenshot of a computer

Description automatically generated

Congrats, you have successfully installed and configured Nessus.

It will take some time to compile plugins so be patient before attempting to start a scan

After the plugins are done compiling, create a new folder and start a scan on the victim IP address.

A screenshot of a computer

Description automatically generated

Nessus works great because it scans the victims IP Address for vulnerabilities, similar to nmap however it shows you the level of vulnerability using a rating system, and even shows you how you can exploit the vulnerability. As you can see this vulnerability has a severity of critical and can be exploited by logging into the VNC server using the password ‘password’

## Setup the Hack

Now that we’ve found the vulnerability, and decided our attack, we shall commence the hacking phase.

Install a VNC viewer so that we can access the Metasploitable 2 VNC server.

Run the following commands:

$sudo apt update, to refresh package list.

$sudo apt install tigervnc-viewer.

A computer screen shot of a computer program

Description automatically generated

Now use the viewer to remotely access the system.

## Start the Hack!

As we saw in the recon step, the victims VNC server is running on port 5900, so we will use our VNCViewer to access the shell from that port.

Run the command:

$xtigervncviewer <IP Address>:<Port>

A screenshot of a computer

Description automatically generated

And enter the password that was discovered by Nessus.

(Had to change the terminal colors to match the occasion.)

A screenshot of a computer

Description automatically generated

And were in!!!

Now write to a file to confirm that weve successfully breached Metasploitable and show our presence.

A screenshot of a computer

Description automatically generated

Read the file in Metaploitable 2

A screenshot of a computer

Description automatically generated

And now we have proof that we have successfully hacked into Metasploitable 2!