

Lab Exercise 1

Due: October 3, 2016

Points: 100

This laboratory exercise is straightforward. It is designed to get you comfortable with running virtual machines using a hypervisor called VirtualBox. We will use these in future labs. It also introduces you to a powerful network probing tool, *nmap*(1).

You are to work in teams for this laboratory. Form a team of 2–3 people, and work together to carry out the lab. When you turn in your results, be sure to list the team members.

We will use interactive grading for the labs. After the due date, we will schedule 10 minute periods where a team can meet with the instructor or TA. At that meeting, we'll examine your solution, talk to you about it and ask questions, and may ask that you demonstrate it to us. All members of the team will receive the same grade. So when you come to the meeting, make sure all team members understand how the lab was done, and can answer questions about the lab and the results.

Background

When attackers target a system, one of the first things they do is see what services the system makes available over the Internet. Once the attackers learn the services the system provides, they attempt to exploit vulnerabilities in the services to gain access to the system and the information on it.

The goal of this exercise is to carry out such an analysis (called a *port scan*) so you can see how attackers do it, and how you can hinder it.

What You Will Need

All the virtual machines and/or resources are available via the web at <http://nob.cs.ucdavis.edu/private/sec-ex1>. The user name is "secexer" and the password is "1ntel!" (without the quotes, of course).

You will also need a virtual machine, VirtualBox. You can download it from <https://www.virtualbox.org/wiki/Downloads>.

Setting Up

To install the virtual machines for this exercise, do the following:

1. Download the virtual machine **nmap1** (nmap1.ova). It's big, so be prepared for the download to take a while.
2. Import the machine on your VirtualBox via the menu **File > Import Appliance...** On a Mac, click Continue twice, then Import, select the VM you just downloaded, and then click Start.
3. Log in to the system. Username and password are both **ubuntu**.

Part I

Run *nmap*(1) with the local host, **nmap1**, as the target. List the services that are running.

Part II

Use the same procedure as before to download a second virtual machine, **nmap2** (nmap2.ova), and install it. The user name and the password are the same as for **nmap1**.

Now use *nmap*(1) to determine what servers are running on ports 1 through 1024 inclusive of system **nmap2**, and list them. Then log into **nmap2**, and run *nmap*(1) with the local host (that is, **nmap2**) as the target. Is the list the same?

Part III

Now log back into **nmap1**. Use *nmap*(1) to determine what operating system **nmap2** is running. Did *nmap*(1) get it right?