Project

Penetration Testing
Team of 2 (max)
(50 points)

0. Learning Objectives

- Practice using **nmap** to scan/map a network
- Practice vulnerability scanning of hosts using **Nessus**
- Practice exploitation of a target host based on a known vulnerability using **metasploit**
- Practice writing a simple penetration testing report
- Optional: Teamwork!

1. Project Introduction

The focus of this project is to exploit a target host based upon a known vulnerability and write a simple penetration testing report. To complete this project you must use the Kali machine on the Pitt Cyber Range.

In this project, you will identify a specific machine on a network, scan it for vulnerabilities, research exploitation, exploit a vulnerability, and write a report showing your work.

Note: You can work on this project alone or with (ONLY) one other student in the same course.

2. Problem Statement

From the Kali machine, scan the 11.11.0.1/24 network to **find the vulnerable Windows XP machine**. Enumerate it to know what ports are open and what services are running on these ports.

You have the Nessus vulnerability scanner installed on your Kali machine. To learn how to start it, watch this YouTube video. Then, use Nessus to scan the Windows XP machine. Research the vulnerabilities to learn about them. **Exploit the Windows XP machine using metasploit.**

> *Note: Don't try to exploit **any other machines** on the network. You are only authorized to exploit the vulnerable WINDOWS XP machine. There's only ONE Windows XP machine on the network.*

Find the files on the desktop of the Administrator account (don't delete or alter anything on the target machine). Read the `README.txt` file (`cat README.txt`). Download all other files to your Kali machine. And take a screenshot of the desktop. What number is in the Notepad?

Good luck!

Here's a screenshot of what's on the Administrator's Desktop folder:

```
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  190    fil   2020-02-09 18:16:58 -0500  README.txt
100666/rw-rw-rw-  9      fil   2019-02-08 02:44:06 -0500  flag.txt
100666/rw-rw-rw-  13779  fil   2020-02-09 18:17:06 -0500  fruit.jpg
```

Once you are inside the Desktop folder (as shown above), you can view the content of the `README.txt` file by typing: "`cat README.txt`".

You can download the `fruit.jpg` file by running the following command:
`download fruit.jpg`

In addition, you can take a screenshot of the exploited machine by running the following command:
`screenshot`

3. Notes

Q) What is Metasploit?

Metasploit is a penetration testing framework that comes installed in Kali Linux. Metasploit commands are run from the command line.

First, you need to start the postgresql database service. This database is used by Metasploit to store information gathered via penetration testing activities.

```
service postgresql start
```

Second, you will have to initialize the msf database using the msfdb init command as follows. You will need to use the sudo command to run with root level privileges.

```
sudo msfdb init
```

Finally, you can start the Metasploit Framework Console by using the msfconsole command as follows:

```
msfconsole
```

Q) When does the Windows XP machine revert back to its original state?

The Windows XP machine is configured to automatically revert back to its original state at the following times:
4 AM ET
8 AM ET
12 PM ET
4 PM ET
8 PM ET
11 PM ET