Getting Ready and Bad Habit

Objectives

In today's hands-on labs, you will perform the following:

Part #1 – Double Check Lab Environment

Part #2 – Login to ThreatActor's VM using SSH

Overview

This is our first lab of our series of the Offensive Security & Reverse Engineering course. We will start by making sure we have all our VMs configured properly and then we will be testing our connectivity to our Threat Actor's box using SSH.

Requirements:

1. For this lab, you will need a working Windows 10 system and a Kali Linux system.
2. Access our lab here <REMOVED>
3. Download **putty.exe** file found for this lab (password=infected). Please remember this password as it will be used for all our labs.

Part #1 – Double Check Lab Environment

In this part of the lab, you are required to make sure all of your systems (VMs) are configured with the correct IP addresses.

Deliverable #1: Submit a screenshot of your VMs showing the correct IP address for each VM.

Part #2 – Login to ThreatActor's VM using SSH

In this part of the lab, we will make sure you are able to connect to your Kali Linux system, which will be used as your Threat Actor's VM. Extract putty.exe from the given 7zip file using the password given and then double click on it.

Deliverable #2: Use putty.exe to connect to the IP Address of your Threat Actor VM. Now, reflect in your own words, what lesson did you learn and what should you do next time?

Part #3 – Please reflect on what you learned from this lab