ITP 325 - Lab 10

Deadline

1 minute before the next scheduled lecture.

Objective

**You will be doing the following in Kali Linux:**

1. Startup both a Kali and Metapsloitable2 VM. Make sure that both the VMs can communicate with each other.
2. In Kali, startup a terminal and type in the following command:

# armitage

When the window pops up click on “Connect”. When asked about “Start Metasploit?” say “Yes”.

Note: If you get any messages saying you ran into trouble, just following the instructions and start again.

1. When armitage is started, select the following to do a ping sweep:

Hosts 🡪 Nmap Scan 🡪 Ping Scan

1. Do the following to get a port scan:

Hosts 🡪 Nmap Scan 🡪 Intense Scan

1. Do the following to find an attack against the machines on the network:

Attacks 🡪 Find Attacks

Questions

1. Why didn’t the class get introduced to Armitage earlier before the first wargames?

Armitage encompasses all that we have learned so far in this class. Specifically, we are learning the proper steps of ethical hacking and find different exploits independently. For Armitage, there is not a need to understand how everything works because you just need to do is press buttons and the application will do the rest of the work. This fundamentally defeats the purpose of learning the techniques of ethical hacking.

Submission

Answer the questions above. **Encrypt the file using the instructor's public key**, and name it **lab10.docx**. Upload the file to your **itp325 folder** on the web hosting.

Refer to Lab 01 if you need help in this.

Reference

<http://www.fastandeasyhacking.com/>