**Iyesha Thornton**

**ITP 325 – Lab 06 – Nmap**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab06.docx
2. Download the instructor’s GPG key from the following location:

<https://sites.google.com/a/usc.edu/chiso/files>

GPG encrypt the \*.docx with the instructor’s and your own GPG key.

1. Place the encrypted document into the repo and push to changes GitHub

**Procedure:**

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

1. Before you can get started, you’re going to need to create or download a Windows 7 VM.

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

1. Start up both the Kali and Windows VM.
2. Within Kali, run a ping sweep with nmap by issuing the following command:

*# nmap –sP <target window’s vm ip>*

**Note:** If you are having trouble getting in touch with the machine, make sure they are both the same virtual network (i.e. bridged or NAT Network)

**Note:** If you are sure everything is right and the IPs or both VMs look good, then think move onto the questions below. You’re probably not doing anything wrong.

1. Identify the Windows VM, and run a port scan against it.

*# nmap <target window’s vm ip>*

**Questions:**

1. You may have notice that a default Windows 7 VM may not have given you the best results when it comes to a port scan. Remember whom Windows 7 is targeted towards. Disable “Windows Firewall”, and rerun the port scan again. Did you notice a different in the results? If there were differences in the results, explain why the firewall was so restrictive.
2. The firewall does not allow a connection to the target so the ping will not work. The firewall protects the target from certain kinds of traffic.
3. Going back to question 1, why are those ports open? What are they used for. You can use a table to list out the ports and a short explanation of their purpose.
4. They are used for life
5. Run a version detection scan against the Windows 7 machine. Were the results accurate? Now try an OS detection by running the following:

# nmap –O <target window’s vm ip>

Based on the results of the OS detection, did you find the scan accurate?

1. No, nothing is accurate.
2. Run a UDP scan against the Windows 7 VM. Did you find anything interesting? If you found some ports, explain their purpose. Limit the ports you want to talk about to no more then 5.
3. No
4. In the lecture, it was mentioned that you could perform a decoy scan using nmap. Explain why it would be useless when executing it within the USC network.
5. It would be useless because the USC network has an enormous flow of traffic and so they work very hard to control and manage that traffic to ensure protection of their users.