**Iyesha Thornton**

**ITP 325 – Lab 08 – Metasploit**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab08.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. Obtain the Metasploitable 2 VM from the following location:

<http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

1. Start both the Kali and Metasploitable2

**Note:** If you are importing Metasploitable2 into VirtualBox, you need to create a new VM. Instead of creating a new virtual disk, you use the \*.vmdk file that was package in the Metasploitable2 zip file that you downloaded.

1. Perform everything that you learned up to this point against the VM. Try to get in and become an administrator.
2. Do NOT look up the answers on getting into the Metasploitable 2. In addition, do not look at the VM as it starts up. If you wish to get better at pentesting it is important that you develop the skillset to get in without cheating.

**Questions:**

1. Submit your port scan.
2. Submit your vulnerability scan.
3. See if you can find 5 ways to get root/administrator access into Metasploitable. List the ways you got in (include the ports and services). Describe how you figured it out.
4. Life
5. Place a picture of a cat into the root home folder without using a USB or VirtualBox/VMware shared folders. Describe in detail how you were able to do this.
6. Mystery of life
7. Although we have not covered it yet, think about the ways Metasploit2 machine can detect you getting in. In addition, think about question 4 and how would you get discovered (besides the cat picture) by the operating system. Describe them here, and do not worry about the details.
8. Port scan, ping,