**ITP 325 - Homework 06b – OpenVAS**

**Deadline:**

1 minute before the next class.

**Submission:**

1. Answer the questions at the end of this file, and name the document hw06b.docx
2. Download the instructor’s GPG key from the following location:

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

GPG encrypt both files with the instructor’s **and** your own GPG key.

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

**Procedure:**

1. Start up the Kali and Windows 7 VM that you did in the lab. Make sure you have the firewall turned on for Windows 7.
2. Run the following commands to get OpenVAS working:

*# apt-get update; apt-get install openvas*

*# openvas-setup*

**Note 1:** Remember the password that was dumped onto the screen. It is what you will be using to get into the scanner

**Note 2:** If you forget your password later on, run the following command:

# openvasmd --user=root --new-password=toor

**Note 3:** If you are smart and read ahead, you can skip all those steps above in Kali by going to Appliacations 🡪 Kali Linux 🡪 System Services 🡪 OpenVas 🡪 openvas initial setup

1. Start OpenVAS by running the following:

*# openvas-start*

1. Let’s use OpenVAS by opening a browser and heading to the following location:

<https://localhost:9392>

the user should be **admin** and the password is what was printed on the screen

**Note:** If it doesn’t work, try running gsad again.

**Questions:**

1. Rerun all the questions from Homework 6a. Compare the results from OpenVAS with Nessus. What were the difference between the two scanners (not from the UI standpoint)?  
   a. They were different
2. What are the pro’s/con’s of each vulnerability scanner?
   1. They were different.