**ITP 325 - Homework 06a – Nessus**

**Deadline:**

1 minute before the next class.

**Submission:**

1. Answer the questions at the end of this file, and name the document hw06a.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. Install Nessus within Kali by doing the following:
   1. Download the Nessus package from the following site:

<http://www.tenable.com/products/nessus/select-your-operating-system>

For Kali Linux, download the “Debian 6.0” \*.deb file. Just agree to the “Subscription Agreement”

* 1. Sign up for the Nessus feeds at the bottom of the download page with the link called “Nessus Home Registration Page”

<https://www.tenable.com/products/nessus-home>

**Note:** You can use whatever info you want. You will need to check your email to get the code to use to finish up the setup

* 1. Open up terminal and go to the directory that you downloaded the \*.deb to and run the following in the command line:

*# dpkg –i Nessus\*.deb*

1. Startup Nessus by running the following:

*# /etc/init.d/nessusd start*

1. Log into the Nessus interface by opening up a web browsers and going to the following site:

*https://localhost:8834*

**Note:** If you have an addon that blocks JavaScript (i.e. NoScript), it may make using the Nessus interface impossible.

**Note:** Remember to trust the certificate

1. Under “Initial Account Setup”, setup the login and password to whatever you want (root/toor is good too)
2. Under the “Plugin Feed Registration”, enter the “Activation Code” that you got in the email.
3. Setup a policy:
   1. Click “Polices” on the top menu
   2. Click on “New Policy” on the left
   3. Select “Basic Network Scan”
   4. Set the “Policy Name” to whatever you want, then press “Next”
   5. Set the “Scan Type” to be “Internal” then press “Next”
   6. Under “New Basic Network Scan Policy”, just press “Save”
4. Perform a vulnerability scan against the Windows 7 VM:
   1. Press “Scans” at the top of the page
   2. Click on the “New Scan” on the left side of the window
   3. Give it any name/description that you want. Under the “Targets” section, type in the IP address of the Windows 7 VM that you wish to test against.
   4. Click on the “Launch” button. Wait awhile and view the report.

**Question:**

1. Like we did in the lab, disable the Windows 7 Firewall, and then redo the vulnerability scan. Did your findings change?

**Note:** You can get a Windows 7 VM from the following

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

* 1. Yes

1. You do not have to use it yet, but name some alternatives to Nessus that is free to use. You will notice is Nessus is not completely free, and there are some limitations.
2. Life
3. Continuing with Lab 06, figure out what the USC networking is looking for when it comes to shutting down a port scan. Based on the reports that you are getting back, see if you can find a way to perform a port scan on the USC networking without being detected. Do no worries if you cannot figure out the answer, you just need to try.  
   a. Any suspicious activity, or some traffic that is trying to repeatedly ping
4. Some networks are setup in an interesting way. For the USC, if you are coming from outside (i.e. non-USC network) you are restricted to certain ports on certain machines. Using secure wireless (or maybe guest wireless would work), find a machine with port 3389 open and accepting connections. Leave the USC network (i.e. go to a public wifi at a coffee shop), and try to access the same machine again. Did it work? If not, how would you access that machine if you had no inside connection/help?
5. No