**ITP 325 - Homework 08 – Exploitation Part 2**

**Deadline:**

1 minute before the next class.

**Submission:**

1. Answer the questions at the end of this file, and name the document hw08.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. Make sure you completed the lab first then start up the Metasploitable2 and the Kali machine again.
2. Learn to brute force a login by using hydra. Run the following command in Kali against your Metasploitable2 machine:

*# cd /usr/share/wordlists*

*# ls –la*

*# cd /usr/share/metasploit-framework/data/wordlists/*

*# ls –la*

*# cd ~*

*# ln –s /usr/share/metasploit-framework/data/wordlists/unix\* .*

*# hydra –L unix\_users.txt –P unix\_passwords.txt ssh://<metasploitable2 vm>*

**Questions:**

1. In some cases, Metasploit does not get the latest and greatest exploits. At times, you will need to check out sites to find proof of concepts (PoC) and run them against your target.

Go to the following wesite:

<http://www.exploit-db.com>

Based on what you did in the lab, find the exploits again. Download them from the site and try to get it to work against the Metasploitable2 machine. How successful were you? What worked and what didn’t work.

* 1. Nothing worked. Life’s horrible and then you die.

If you are having trouble finding the exploits you used before, try to find new ones to use against the VM.

1. Sometimes there are timeouts for logins, so we need to setup hydra to continue the attack even if the account has been blocked for failed attempts. Look through the hydra manpage by typing :

*# man hydra*

See if you can find a flag that helps you deal with the login block problem. If you cannot find anything try using Google.

1. N/A