**Iyesha Thornton**

**ITP 325 – Lab 05 – Social Engineering Toolkit**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab05.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. Startup SET by running the following command in the terminal:

# setoolkit

1. Try out a website cloning by doing the following:

* Select “Social-Engineering Attacks” (option 1)
* Select “Website Attack Vectors” (option 2)
* Select “Web Jacking Attack Method” (option 5)
* Select “Site Cloner” (option 2)
* Enter a public IP address of the machine you are running on

**Note:** for now, you can put in 10.0.2.15 (or whatever your IP address was assigned to your Kali distribution)

* Enter the following URL: https://www.linkedin.com
* When asked “… do you want SET to start the process?” type ‘y’

Open a web browser within Kali and use the IP address that you typed in to setup the attack. Watch it happen

1. Try out a spear-phising attack by doing the following (assuming you’re starting from the main menu):

* Select “Social-Engineering Attacks” (option 1)
* Select “Spear-Phishing Attack Vectors” (option 1)
* Select “Create a FileFormat Payload” (option 2)
* Select “Adobe PDF Embedded EXE Social Engineering” (option 12)
* Select “Use built-in BLANK PDF for attack” (option 2)
* Select “Windows Meterpreter Reverse\_TCP” (option 2)
* Enter a public IP address of the machine you plan to listen for the callback
* Use the default port
* Select “Keep the filename, I don’t care.” (option 1)

Continue with Question 2.

Questions

1. Try to figure out the best way to clone the USC authentication system using SET. What problems did you run into when trying to execute the clone? What do you think you need to do to fix it, if any?
2. Everything
3. Now to run the attack. Setup a fake Gmail account to use with SET. Finish up step 2 in the procedure. See if you can send the email to the professor (yes spam ‘em). What problem did you run into? Try to figure out a way around it.
4. I couldn’t send the email.

Keep in mind that you don’t have to succeed in completing this question. It’s more important that you learn the limitations of the system. In addition, don’t worry about the callback just yet. We’ll cover that later on.

1. Explore the other various attacks that are available in SET. Which one do you think will be very helpful for you when performing a social engineering attack against the student body on campus? Explain.
   1. Any email that is spam/virus that is spreads on its own once opened, but the person does not suspect it.