Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Through this experiment, we will create a LinkedIn phishing page using Social-Engineer Toolkit (setoolkit) which is a preinstalled functionality in Kali Linux. The phishing link can be sent to any user on the same Local Area Network as you and the data that they enter on the fraudulent page will be stored in a file on the attacker’s machine.

Social Engineering Toolkit or SET for short is the standard for social engineering testing among security professionals and even beginners must have a basic idea about using the tool. Basically, it implements a computer-based social engineering attack.

You can find out reference material in the links below:

https://www.tutorialspoint.com/kali\_linux/kali\_linux\_social\_engineering.htm

https://linuxhint.com/kali-linux-set/

https://medium.com/@nancyjohn\_95536/using-set-tool-kit-to-perform-website-cloning-in-kali-linux-67fa01c92af9

1. As root, open “setoolkit” from the command line. After reading and agreeing with the terms of service, you get to the main menu. Navigate through the menus to familiarize yourself. What path leads to the credential harvester?
2. Once there, choose the option “Site cloner” to craft a malicious web page. SET will ask you to provide an IP where the credentials captured will be stored. Enter the internal network IP address of your Kali Linux VM. Capture a screenshot.
3. We need to clone the login page of LinkedIn, hence enter the complete URL, including the protocol. Capture a screenshot.

NOTE: Make sure you select the URL leading to the login page where the credentials are introduced.

1. The setup for a phishing attack is complete, you have cloned LinkedIn and hosted it on Kali. Now, go to browser and type http://yourIP and you are able to open the fake LinkedIn page. Capture a screenshot.
2. Enter a random username and password and click on login. What happens next? Why users might not be suspicious?
3. In background, your settoolkit is catching up your credentials. Capture a screenshot of SET in the terminal showing the provided credentials.
4. Find out the permanent location where you can check them, that have been recorded in XML file. What is the directory? Capture a screenshot of the part of the file referring to “password”.
5. Go back to the main menu. Find the right options to send an E-mail to a single address. Then, send an email to your Herzing account from a Gmail account (create a new one if necessary). Capture a screenshot showing all options you chose before writing “END” to finish your message.
6. The message might or might not get to your Herzing account inbox, depending on Herzing’s and Google’s policies and your choices. Nevertheless, if successful, what kind of phishing attack were you trying? Justify your answer.
7. What would you need if you wanted to spoof the sender instead of using a Gmail account?