Using Kali SET

This is the lab for client-side attack. We are approaching with a social engineering type. The purpose is to verify that users learnt and understood the security awareness program. If they click, see the website, and enter their ID/password, their workstation will be penetrated.

1. Pre-requisite:

a. Your Kali may need an Internet connection for additional files. Make sure yo ur VM has set the networking to **NAT**.

b. A Windows 7 workstation as a victim in the attack. This VM is set to NAT, so it can **ping** the Kali Linux.

2. Credentials:

a. Windows:

i. ***Username:*** **administrator**

ii. ***Pass:*** **vpn@123**

b. Kali:

i. ***Username:*** **root**

ii. ***Pass:*** **vpn@123**

3. Click on Application, Social Engineering, and select SET

4. When you see the menu:

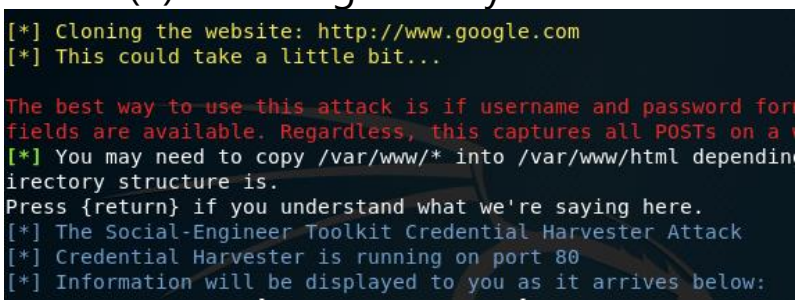
a. Select (1) *Social-Engineering Attacks*

b. Select Website Attack Vectors

c. Select Credential Harvester Attack Method

d. Select Web Templates

5. Verify the IP address of the web attack by making sure it's your Kali's IP address, and hit **Enter**
6. Select (2) for Google and you should see the below message:



7. Logon to your Windows 7, open Internet Explorer and enter: http://192.168.160.134 (or whatever your Kali's IP address is)
8. You should see the Google login page
9. Enter a username and password and click Sign In
10. Go back to your Kali Linux. Can you find the discovered username and password? **Copy text of the result, which will be included in the entries portion of the lab report.**
11. Follow the report template and create a report for this exercise