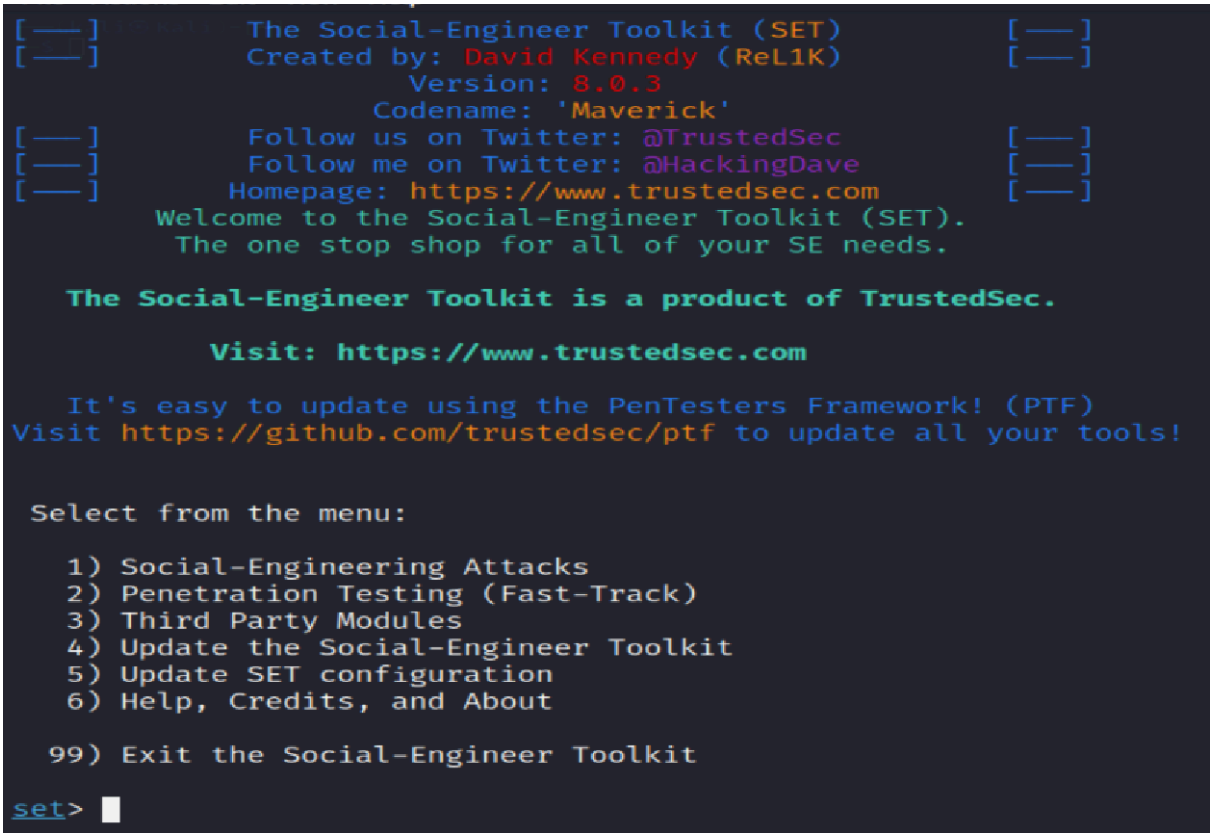
Exploring the Social Engineer Toolkit (SET)

Background / Scenario

In this activity, you will clone a website and obtain user credentials. This activity is performed under carefully controlled conditions within a virtual environment. SET tools should only be used for penetration testing in situations where you have written permission to perform social engineering exploits. In an actual penetration test, this procedure could be used to reveal problems with user security training and the need take measures to educate users about various types of phishing attacks.

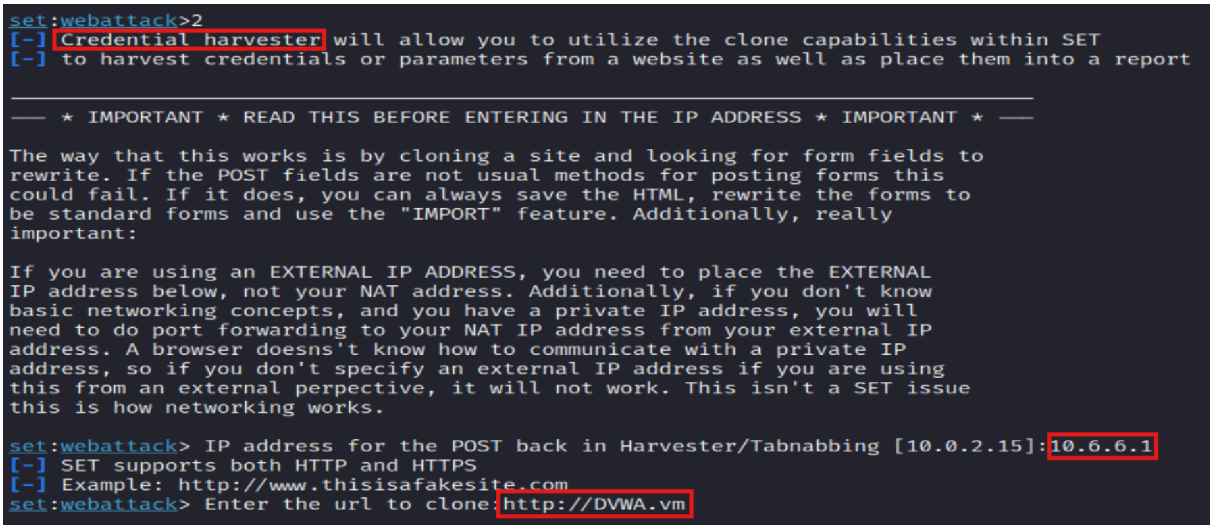
Part 1: Launching SET and Exploring the Toolkit

SET must be run as root. Use the **sudo -i** command to obtain persistent root access. At the prompt, enter the command **setoolkit** to load the SET menu system.

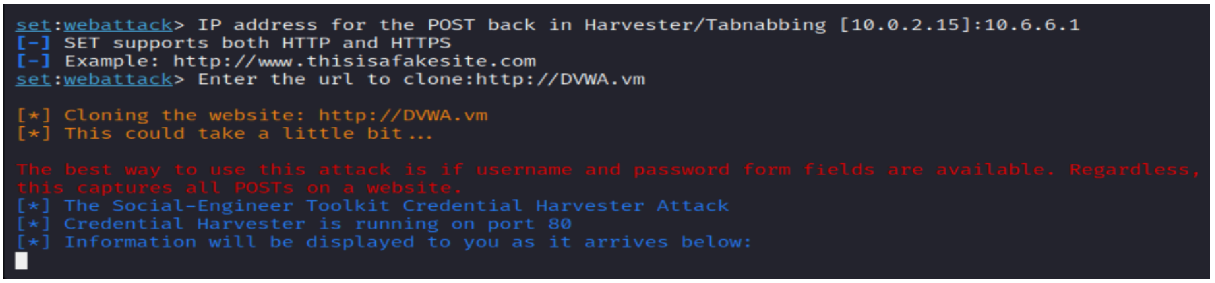


Part 2: Cloning a Website to Obtain User Credentials

In this part of the lab, you will create a perfect copy of the login page for a website. The fake login page will gather all credentials submitted to it and then redirect the user to the real website.



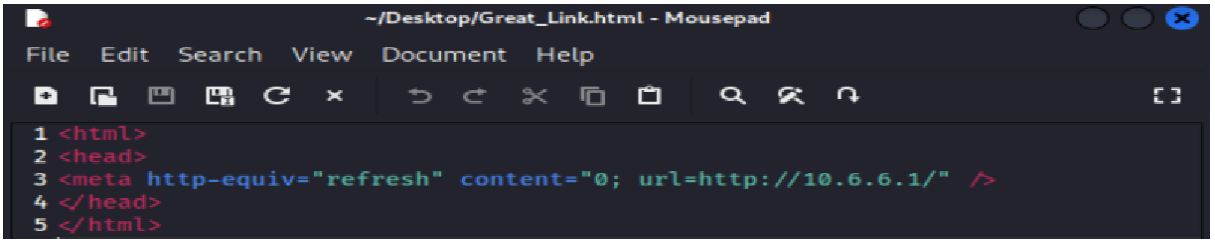
When the website is cloned, the following message appears on the terminal. No prompt will be returned to you. This is because a listener is now active on port 80 on the Kali computer and all port 80 traffic will be redirected to this screen. Do not close the terminal window.



Part 3: Capturing and Viewing User Credentials

In a “real-life” exploit, at this point, a phishing exploit containing a link or QR code that sends the user to the fake website is created and sent. In this lab, an html document is created to direct the user to the fake webpage. This

document simulates a distributed phishing URL. It could be distributed as a file attachment in phishing emails.



A good hacker would create a fake URL that would be very similar to the actual URL, so that unless the user inspects the URL very closely, it would go unnoticed.
Return to the terminal session that is running the SET application. Output from the login attempt should appear, similar to what is shown: