**Lab 11 - SET, Social Engineering Toolkit**

Objectives

* Become familiar with Social Engineering based attacks.
* Become familiar with the Social Engineering Toolkit as a tool to perform such attacks.
* Become familiar with the ease of cloning a website to be used in a credential harvesting campaign.

Pre-Lab

For this lab, you'll need your Kali VM and internet connectivity.

1. Autopwn Attack

* To open SET, in Kali go to Applications -> Kali Linux -> Exploitation Tools -> Social Engineering tools -> SET
* Agree to the User Agreement
* Select Social Engineer Attacks
* Select Website attack vectors
* Select the Metasploit Browser Attack
* Select the Web Templates option
* Say No if asked about using NAT
* Enter your IP address of your Kali VM
* Select a template
* Select the Metasploit Browser Autopwn option
* Select Reverse\_TCP Meterpreter

A computer screen shot of a computer code

Description automatically generated

* When complete, go to the URL that is shown in your victim Windows VM, or from within Kali. (Note - if using Kali, ensure your proxy settings are no longer set to reference Burp from lab 9)

A screenshot of a computer

Description automatically generated

We get a remote shell, once the user opens our URL.

Note: This attack may have limited to zero affect on the victim browsing it due to the nature of it "automatically" picking random attacks to throw at the browser visiting the site.

2. Website Cloning Attack

* Assuming SET is already open, Select Social Engineer Attacks
* Select Website attack vectors
* Select the either Credential Harvester Attack
* Select the Site Cloner option
* For the website, enter a website with a username and password logon (banks, email sites,etc)
* Many webmail sites now only expose a username field and then a password field to thwart attacks like this. Sites like my.umbc.edu however expose both a username and password field on the same page as part of the "Log in with UMBC" option. Be sure to clone the correct address that presents the login fields.
* From the victim browser, go to the site: http:// where you should see a copy of the website you cloned running on the Kali IP.
* Enter in a fake username and password
* Your credentials should be shown in the SET terminal after you click submit

A screenshot of a computer

Description automatically generated

We created a fake facebook website and harvested credentials from the victim PC as shown in the screenshot.