### Lab 9 - Social Engineering Toolkit

### Due as per D2L dropbox

Social Engineering Toolkit Scoring Rubric

|  |  |
| --- | --- |
| 100 | Successfully completes the assignment and provides all of the required video documentation (or provides in-lab demo in front of instructor). |
| 50 | Successfully completes the assignment but only documents via screenshots. |
| 0 | Nothing turned in or document is not readable or does not accomplish the lab activities. |

Goal

To use the Social Engineering Toolkit to compromise a target host. The student must demonstrate an attack against a browser.

Deliverables

Upload an MS Word DOCX, RTF, or PDF file to D2L with name, course #, assignment and appropriate documentation (e.g. link to online video of your actions or embedded screen-shots).

Building Details for Social Engineering Toolkit

The Social Engineering Toolkit is included in Kali/Backtrack distributions. See the following references for how to use it.

1. [Creating Fake Sites to Harvest Passwords](http://moinkhans.blogspot.com/2013/05/social-engineering-toolkit-kali-linux.html)
2. [Social Engineering Toolkit Tutorial (12 min video) Updated on 20211005](https://www.youtube.com/watch?v=F8tUPeMl_DU)

Attack Details for Social Engineering Toolkit

Either select a particular attack (e.g. “Web Site Java Applet”) or instruct the tool to use an autop0wn feature (i.e. try a bunch of attack vectors on its own). Select the particulars of the attack and the payload (e.g. Meterpreter). Using a Windows VM, or other platform running an outdated browser, visit the URL of the SET tool. Collect visual evidence to demonstrate that you have accomplished this activity (e.g. short video or series of screenshots; note: check the grading rubric).

Restrictions[[1]](#footnote-1)

* Students should take care when entering a target machine's IP addresses (or CDIR addresses) to ensure that only the correct address(es) are scanned/targeted. It is recommended that for the duration of the attack phase of this lab (i.e. not when building the VMs or updating the BackTrack distribution), you isolate your VMs by either disconnecting from the Internet (or WAN) or by switch your VirtualBox network to “Host-only” (but if you do the latter, remember to refresh the IP addresses of the VMs).
* Under no circumstances are students to actively compromise or subvert control of any hosts for which they are not the rightful owner or for which they do not have written permission to do so.

Background & Resources

* Scanning chapter in CHR.
* Documentation for the Social Engineering Toolkit (see the tool itself, and online). The tool is included in the Kali/Backtrack distribution.

1. “Warning sign” image from <http://en.wikipedia.org/wiki/Exclamation_mark> [↑](#footnote-ref-1)