### Lab 12 – Blackeye Tool

### Due as per D2L dropbox

Blackeye Tool Scoring Rubric

|  |  |
| --- | --- |
| 100 | Successfully completes the hard version and provides all of the required video or screenshots documentation (or provides in-lab demo in front of instructor). |
| 80 | Successfully completes the easy version and provides all of the required video or screenshots documentation (or provides in-lab demo in front of instructor). |
| 0 | Nothing turned in or document is not readable or does not accomplish the lab activities. |

Goal

Use the Blackeye tool to do phishing attacks on Target. 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 screenshots).

**Background and Tools**

* Use this following reference for how to use Blackeye and Social Engineering Toolkit:
* [Blackeye Install](https://github.com/The-Burning/blackeye-im)
* [How to install Blackeye in Kali Linux](https://www.youtube.com/watch?v=J0dEra-f58k)
* [Social Engineering Toolkit - Kali Linux - Simple Tutorial](http://moinkhans.blogspot.com/2013/05/social-engineering-toolkit-kali-linux.html)
* [Social Engineering Attack Demo Video](https://www.youtube.com/watch?v=F8tUPeMl_DU)

**Challenge:**

\*\*EASY VERSION\*\*

* You can select any attack sites you want (Facebook, Google, Instagram, ….) and use yourStartId@mnsu.edu for username and CIS450 for password.
* Take a screenshot to show the evidence you can get credential.

\*\*HARD VERSION\*\*

* **Use the Social Engineering Toolkit to send victim one email that contains the link you get in Blackeye**
* **Select “Mass Mailer Attack” and remember to isolate your VMs by either disconnecting from the Internet (or WAN) or by switch “Host-only”**
* **Collect visual evidence to demonstrate that you have accomplished this activity**
* **Notice: use only your own email addresses.**

**Background & Resources**

* **Scanning chapter in CHR**
* **Document for Blackeye and SET (see the tool itself)**

**Tram Nguyen**

**CIS 450**

**Lab 12**

**\*\*\* EASY VERSION \*\*\***

* **Set up Blackeye**

**A screenshot of a computer

Description automatically generated with medium confidence**

* **Run Blackeye with cmd *./blackeye.sh .***
* **It lists a lot of options so for example, I choose number 1 (Instagram).**
* **This tool starts php server, ngrok server and then show a link that can be sent to victim.**

**Text

Description automatically generated with medium confidence**

* **When clicking that link, the browser shows the Instagram login page.**
* **After I type my account and password, blackeye gets this credential immediately in the terminal.**

**Graphical user interface

Description automatically generated**

**\*\*\* HARD VERSION \*\*\***

* **Social Engineering Kit**
* **1. Social-Engineering Attacks > 5. Mass Mailer Attack > 1. E-mail Attack Single Email Address**

**Text

Description automatically generated**

* **Enter the victim or target’s email address.**
* **I will use my own email address to send the email so selecting number 1**

**Text

Description automatically generated**

* **Fill out all information needed (my 2nd email, password, email subject….)**
* **In body of message field, paste the link Blackeye tool creates**

**Text

Description automatically generated with medium confidence**

* **The victim will get new mail immediately, and click that link**

**Graphical user interface, text, application

Description automatically generated**

* **Same as easy version, the browser also goes to the Instagram login page.**
* **Do the same in easy version.**

**Graphical user interface

Description automatically generated**