**ITP 325 - Homework 03b – Recon and CTF Practice**

**Deadline:**

1 minute before the next class.

**Submission:**

1. Answer the questions at the end of this file, and name the document hw03b.docx
2. Download the instructor’s GPG key from the following location:

<https://sites.google.com/a/usc.edu/chiso/files>

GPG encrypt both files with the instructor’s **and** your own GPG key.

1. Place the encrypted document into the repo and push to changes GitHub

**Procedure:**

1. Head to [Shodan’s website](https://www.shodan.io/) and create a free account with a dummy email addess

Go over the tutorials found on these pages:

<https://danielmiessler.com/study/shodan/>

<http://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-targets-using-shodan-the-worlds-most-dangerous-search-engine-0154576/>

Go answer question 1

1. Within Kali Linux, open up a terminal and run the following command:

*# dmitry –h*

After studying the command line parameters, try to execute a command that does the following:

* perform an IP and domain whois lookup on the usc.edu
* get the netcraft information regarding usc.edu
* find possible subdomains on usc.edu
* find possible email address on usc.edu
* save all the output of the command to usc.edu.txt

Go answer question 2

1. Check out the discover script from the following location:

<https://github.com/leebaird/discover>

Follow the instructions on setup and usage. Remember to get API keys for the following:

* Bing
* Builtwith
* Fullcontact
* GitHub
* Google
* Hashes
* Shodan

Run the following script against usc.edu then go answer question 3

1. Get together with your CTF team and do the following practices. Remember not to lookup the solution:

<https://jacobedelman.gitbooks.io/hsctf-3-practice-problems/content/>

**Question:**

1. Can you find anything interesting in the LA area with Shodan?
   1. No, not really
2. Found anything interesting with Dmitry
   1. No
3. Found anything interesting with the discover script?
   1. I found multiple pentesting attempts with this script.