**Iyesha Thornton**

**ITP 325 – Lab 04 – Recon Part 2**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab04.docx
2. Download the instructor’s GPG key from the following location:

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

GPG encrypt the \*.docx with the instructor’s and your own GPG key.

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

**Procedure:**

**You will be doing the following in Kali Linux:**

1. Before you start the lab, make sure the change your MAC address and jump onto the Guest wireless.
2. Run the following command in the command line:

*# apt-get install metagoofil*

*# metagoofil –d www-scf.usc.edu -t docx -l 1000 -n 250 -o uscstudentfiles -f results.html*

**Note:** When you look inside the directory you may see something. There’s a strong chance that there is nothing print on the screen and/or nothing in the directory. That’s fine. Check out the question below.

1. Before we move on to the next step, make sure you got step 1 down. Let’s try another way to pull DNS information by running a brute force method:

*# fierce –dns usc.edu*

**Note:** You may want to do Question 4 before starting on this step. Also this step takes a long time. Also you may get kicked off the USC network.

**Questions:**

1. When you changed your MAC address from step 1, where you changing it within the VM or outside the VM? Does it matter? Do you need to do both?
2. Within the VM. Yes it matters, but no you don’t need to do both if you change it in the terminal.
3. From step 1, think about other ways you are going to get caught after you changed your MAC address. Discuss how you can cover those leaks so that in the future you are more stealthy  
   a. The guest wireless is an open network and someone can trace everything back to you.
4. Compare and contrast metagoofil with theHarvester. When would you use one or the other? Which tool do you think is more helpful to you?
5. Metgoofil is more helpful.

If you couldn’t get metagoofil to work, try to guess at what it does and what it will should you.

1. Fierce is very noisy. If you just run it directly you may get an angry email from ITS saying you started too many connections (why you forget to do step 1). Look through the help by typing the following command:

*# fierce –h*

Look through the options and find anything that would help make you stealthier. What is the more stealthier command from Step 3? Explain the options that you used, and why you think it helps.

1. If on step 2 on the assignment you couldn’t get metagoofil to work (or even if you could get it to work), what are the equivalent Google operators that you can use to give you the same search results for the following:

* Email address from a domain
* All MS Word docs (old version and new) from a domain
* All types of interesting documents form a domain (PDF, Excel, MS Word, etc)

Videos

Installation and Usage of Metagoofil on Kali 2.0

<https://youtu.be/drZw59eyrbk>