**Samuel Park**

**ITP 325 – Lab 03 – Recon Part 1**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab03.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. Use Netcraft against www.usc.edu
2. Use whois against www.usc.edu

*# whois usc.edu*

1. Run nslookup against www.usc.edu

*# nslookup www.usc.edu*

1. Use the host command against www.usc.edu

*# host -t ns usc.edu*

1. Try to do a zone transfer against www.usc.edu, then do a zone transfer against zoneedit.com  
     
   *# host –l usc.edu ns1.usc.edu*

*# host –l zoneedit.com ns2.zoneedit.com*

1. Run theHarvester in Kali and see all the emails that you can find for usc.edu  
     
   *# theharvester -d usc.edu -l 500 -b all*

**Questions:**

1. What did you find out against usc.edu? How would this information that you found in Netcraft useful in getting into the USC network. Try a different school (i.e. Marshall) and see if the results are different.

Found IP addresses, domain names, different email addresses and time of activation and deactivation of domain names. This is helpful for recon to know what ip addresses you can target and domain names associated with USC or other websites.

1. What kind of information did you get out of the whois command? How would this information be helpful in an attack? Try a different school (i.e. Marshall) and see if the results are different.  
   Similar to netcraft, it shows name servers, technical contacts, domain name records.
2. What kind of information did you get out of the nslookup command? How would this information be helpful in an attack? Try a different school (i.e. Marshall) and see if the results are different.  
   Found Server and Address of usc.edu.
3. What kind of information did you get out of the host command? Did anything happen? If you got some information, how would this information be helpful in an attack?   
   It gave information of different server names associated with [www.usc.edu](http://www.usc.edu).
4. Did doing a zone transfer work against usc.edu? If it did work, did you have any servers that are interesting?   
   No, I didn’t get the zone transfer to work.
5. Did you discover anything interesting from running theHarvester against USC? Try to use a search engine (Google/Bing/etc) see if you can find the pages that the emails were pulled from.  
   It was similar information to the other tools used in this assignment. More server names and IP addresses and domain names.