**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.  
   a. I found out the name of the Registrant, the administrative contact (which is Brian Yamaguchi), the technical contact, the name servers, when the domain was activated, when the domain expires, and when the domain was last updated.:

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.
2. I found out the name of the Registrant, the administrative contact (which is Brian Yamaguchi), the technical contact, the name servers, when the domain was activated, when the domain expires, and when the domain was last updated.

1. 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.
2. I learned the domain’s ip address . I could use this information to try to do a port scan attack or learn more information about the network. The results are not different for another school.

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?   
a. I got the name of the servers: usc.edu name server ns1.usc.edu.

usc.edu name server ns2.usc.edu.

usc.edu name server ns3.usc.edu.

usc.edu name server nserver.apple.com.

usc.edu name server uucp-gw-1.pa.dec.com.

1. Did doing a zone transfer work against usc.edu? If it did work, did you have any servers that are interesting?
   1. No, it did not work.
2. 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.  
   a. Yes I discovered many different emails of people that either are employed by or attend USC from campus organizations to the office of the provost.