**Ethical Hacking Assignment 1**

**Open Source Intelligence (OSINT) or Reconnaissance**

**Objective:** Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources).

Using publicly available data conduct information gathering in the form of Email address, phone numbers, IPs, OS info, software versions, Geo locations, business or personal details, etc.

**Tools:** Google Dorks, Wayback machine, Whos.is, Netcraft, Host, NSLookup, dig, Maltego, IP2location, HTTrack, and Email Harvester. (there are many more tools, but these will be the focus of this lab)

**Reconnaissance Assignment:**

**Task -> Given a “Company Name” Now HACK!!**

1. **HTTRACK – Clone a Website for Offline Analysis**

First locate and copy a website locally using a Website Copier called HTTRACK, this enable you to conduct offline analysis and searches on the multitude of webpages comprising the website.

Download and Install HTTRACK at <http://www.httrack.com/>

Video: <https://www.youtube.com/watch?v=DNdNbYkr0X0>

Note: If you are trying to find information about a particular company for social engineering or trying to spoof a website or login, HTTrack is an excellent tool for both tasks. To create a clone website for [dnsspoof](http://null-byte.wonderhowto.com/how-to/hack-like-pro-spoof-dns-lan-redirect-traffic-your-fake-website-0151620/) or grab credentials for an [Evil Twin](http://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/), now you have the tool to do so! We will see this later.

Clone this website: URL -> <http://web.eng.fiu.edu/aperezpo>

Then, using your favorite web browser open enter

Navigate and explore the website looking for information that can be used in this phase, such as phone numbers, email addresses, business relationships, employee names, social media connections etc.

Makes a list of any of this information you find and submit it as part of this assignment.

Emails: [aperezpo@fiu.edu](mailto:aperezpo@fiu.edu) ; [apons@fiu.edu](mailto:apons@fiu.edu)

Address: Office Location: EC 3145 Office Hours: Tuesday and Thursday 10:00 AM to 12:00 PM

Tel#: 305-348-7253

Name: Dr. Alexander Perez-Pons

What value is associated with the key=value for the key Secret\_Cookie

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Exhaustive web search engine using Google Hacking or Dorks (Smart searches):**

<http://null-byte.wonderhowto.com/how-to/use-google-hack-googledorks-0163566/>

<http://www.digitaltrends.com/computing/directly-access-google-cached-pages/>

<http://www.google-dorking.com/>

1. Search only the FIU website looking for cybersecurity and record the number of hits, compare this number to just typing cybersecurity.

**site:fiu.edu cybersecurity**  3,130 results compared to **cybersecurity** 135,000,000 results

1. Search to find how many FIU webpages contain admin in the URL (hint: must combine multiple directives) Record how many hits found and explain why this would be valuable in conducting reconnaissance, what do we learn or find out? Try.

**inurl:admin** 74,600,000 results and then **site:fiu.edu inurl:admin** 110 results

**Why perform:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

c) To reduce your digital footprint search the cache webpages instead of the live webpages for cybersecurity, use the following link to find a cached version of the page:

<http://web.eng.fiu.edu/aperezpo> Has anything changed? Yes or No

h**ttp://webcache.googleusercontent.com/search?q=cache:** <http://web.eng.fiu.edu/aperezpo>

Google has recently changed the ability to search the cached webpage, in the past we could do:

**cache:fiu.edu cybersecurity**

to search all cached fiu.edu webpages for the term cybersecurity, now we must specify a specific webpage as in this exercise to get the cached version of a webpage. This was a great way to conduct passive reconnaissance, since the actual website is not searched, but instead the cached versions.

Use the Way Back Machine to look at past achieved website: <https://archive.org/web/>

What was the first year this web page appeared and when was it can by the Way Back Machine:

Year: 2015 Date: January 23, 2015

d) Use the following website to explain the latest <http://www.exploit-db.com> google hack, please record it and explain what it does.

First Dork: intitle:"oracle bi publisher enterprise login"

Purpose: Find Sites running Oracle Business Intelligence

1. **The Email Harvester -> Discovery Emails Associated with a Domain (performing Open Source Intelligence Gathering)**

[**https://www.youtube.com/watch?v=7XRRvrZsJ7o**](https://www.youtube.com/watch?v=7XRRvrZsJ7o)

<https://www.youtube.com/watch?v=0-OyZGbpSJk>

**Using Kali**, run the harvester tool on the website: fiu.edu, Show the results?

theharvester –d fiu.edu –l 10 –b google

email\_1: academic@thewolf.fiu.edu

email\_2: boxoffice@thewolf.fiu.edu

email\_3: smorr057@fiu.edu

Now use bing as the search engine and list the first three emails, are they the same or different,

email\_1: noreply@login.fiu.edu

email\_2: danjohns@fiu.edu

email\_3: name@fiu.edu

Explain: They are different due to different search engines.

1. **Using WHOIS, NETCRAFT, HOST, NSLOOKUP, DIG**

Use two companies, one large and one not so large, like sears.com and gilbertsbakery.com with these two company domains use the tools identified on Linux (Kali) or Windows to get as much information as possible. Submit a report with the information you have learned and are there any differences between the two company reports. Be aware that doing this is legal, since these are public databases that maintain all of this information; we are not accessing any information on these specific domains. Show the results for each company and the results obtained after running these tools. Describe what you have learned?

You can use the GUI or CLI tools or one of these websites or you can use any means you like

<http://www.whois.net>

<http://searchdns.netcraft.com>

<http://www.dnsstuff.com/tools>

<http://network-tools.com/nslook/>

<http://dig-nslookup.nmonitoring.com/dns-dig-nslookup.html>

A netblock is a range of IP addresses. ISP's must be assigned addresses in blocks, and the larger the block that can be assigned to someone the better because that makes for less entries in the Internet routing tables for information on how to get to those addresses.

**Sears**

**IPs: 23.40.215.124; 23.195.126.84; 104.82.183.218; 95.101.128.153; 92.123.140.40; 104.98.2.184; 88.221.134.216; 92.123.140.17**

**NS: whois.corporatedomains.com**

**Admin: rm-hostmaster@ems.att.com**

**Date Reg:**

**Number of subdomain:**

**List the earliest subdomain:**

**What is the hosting company: Akamai Technologies**

**Netblock Owner: Akamai International, BV**

**IPs associated with A records: 23.38.109.235**

**MX: Priority: 10**

**Exchange: sears-**

**com.mail.protection.outlook.com**

**Gilbertsbakery**

**IPs:** *184.168.62.1;* 184.168.62.1; 72.167.183.16

**NS:** NS3.SECURESERVER.NET; NS4.SECURESERVER.NET

**Admin:** *dns@jomax.net*

**Date Reg:**

**Number of subdomain:**

**List the earliest subdomain:**

**What is the hosting company: GoDaddy**

**Netblock Owner:**  *GoDaddy.com, LLC*

**IPs associated with A records: 184.168.62.1**

**MX: Priority: 5**

**Exchange: ALT1.ASPMX.L.GOOGLE.com**

**Priority: 5**

**Exchange: ALT2.ASPMX.L.GOOGLE.com**

**Priority: 10**

**Exchange: ALT3.ASPMX.L.GOOGLE.com**

**Priority: 10**

**Exchange: ALT4.ASPMX.L.GOOGLE.com**

**Priority: 1**

**Exchange: ASPMX.L.GOOGLE.com**

**What can you discuss in comparing the results for these two companies?**

**­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**What DNS was used by the tool to obtain information (zone transfer) for your results?**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**5) Maltego –An Intelligent Information Gathering Tool**

a) Go to <https://www.paterva.com/web7/downloads.php>

and download and install the community version for your platform. You need to register with your email and password to use it for a limited amount of time. This is a tools used by law enforcement to discovery relationships among various entities. The way it works is that it accesses various available data repositories, Whois, DNS, social media, etc. to discovery associations. For example, we could determine what DNSs are associated with a website or what domains are associated with a specific IP address, which friends do these people have in common, remember just about everything is linked or known through your email on the Internet.

Please see videos below to see how to perform many of the activities with this tool.

<https://null-byte.wonderhowto.com/how-to/video-use-maltego-research-mine-data-like-analyst-0180985/>

<https://www.youtube.com/watch?v=46st98FUf8s>

<https://www.youtube.com/watch?v=c7vZskOkINw>

Tutorial: <https://www.youtube.com/watch?v=09PfRJ4-5_0>

Please perform the above video’s tasks on a selected person and list what you have learned about the person and the relationship discovered.

**­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**