**CYBR 644 Assignment-3**

1. OSINT Collection

1. Open a browser and go to: http://www.netcraft.com
2. In the “what’s that site running box”, type, www.umbc.edu
3. Note the IP Address, Operating System, and version of the Web server Software

Ans: A screenshot of a computer

Description automatically generated

**IP Address**: 23.185.0.4

**Operating System**: Linux

**Web Server Software**: Patheon Varnish

1. Get DNS Records for UMBC by browsing <http://www.robtex.com/dns/www.umbc.edu>

Ans: A screenshot of a computer

Description automatically generated

1. Get the whois information by checking: http://www.whois.net/whois/umbc.edu or using <http://centralops.net/co>

Ans: A computer screen shot of a computer

Description automatically generated

1. Google “UMBC network jobs” and look for details concerning technologies used within the college

Ans: A screenshot of a computer

Description automatically generated

**Technologies Highlighted**: Linux, Python, SQL and Tableau

1. Try using https://viewdns.info to gather the same information within their "One Stop Shopping" website

Ans: A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2. Information Collection by visiting a site

1. Open wireshark and start a capture on the Interface connected to the Internet.
2. Go to the website bom.gov.au with the browser of your choice.
3. Stop the Wireshark Capture and type the following filter in the filter pane and click apply:

http and frame contains bom.gov.au

1. Right click on the first frame and select follow TCP stream. View the server’s response.

Ans: A screenshot of a computer

Description automatically generated

1. Repeat these steps by visiting lairnet.academy and compare the server's response with bom.gov.au's.

Ans: A screenshot of a computer

Description automatically generated

Some of the differences between bom.gov.au and lairnet.academy are:

* HTTP responses are different. Bom.gov.au gives http response 302 status code that indicates that a resource has been temporarily moved to a new URL, whereas lairnet.academy gives http response 200.
* The html response of lairnet.academy is encoded.

3. Information Collection via Search Engine

1. Perform a Google Hacking Search for all PowerPoint Documents (.pptx extension)

Ans: A screenshot of a computer

Description automatically generated

1. Narrow that search to a specific domain or site

Ans: A screenshot of a computer

Description automatically generated

1. Perform a Shodan search for Apache webservers

Ans: A screenshot of a computer

Description automatically generated

1. Find any with an HTTP 200 OK response

Ans: A screenshot of a computer

Description automatically generated

1. Perform a Bing IP search on a small business website such as shops in old Ellicott City, mainstreet Catonsville, a local coffee shop (not Starbucks), etc.

Ans: A screenshot of a computer

Description automatically generated

4. Automated Tools for Information Gathering

1. Using The Harvester, search for all email addresses from the umbc.edu domain from google and linkedin

ANS: A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. Using Recon-ng, search for all points of contact for a large company (defense contractors work well), by loading the /recon/domains-contacts/whois\_pocs and setting the source to the domain name of your target.

Ans: A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. Using Spiderfoot, perform a search against a domain related to your target.

Ans: A screen shot of a computer

Description automatically generatedA screenshot of a computer screen

Description automatically generated

Spiderfoot is finding all sorts of information like linkedin, emails and domains. It is way more powerful that recon-ng or theHarvester.

5. Dox the instructor

Collect as much information as you can on me. Check websites such as viewdns.info, pipl.com, google.com profileengine.com, and various social media web sites to figure out everything you can about me. I happen to have a fairly unique name, so finding information on me isn’t that difficult. You DO NOT need to pay for any online "report" for this assignment.

Some of the information is incorrect online as you will see. It will help if you can figure out what alias I use online for most of my accounts in finding more information. Remember to "go beyond" the first page or two of a google search.

Answer the following questions:

1. Who do I work for and who have I worked for?

Ans: A screenshot of a computer

Description automatically generated

1. When did I get married?
2. Where do I/have I lived?

Ans: Ellicott City, Maryland.

1. Who are my relatives?

Ans: Christophe Hennick

George Hennick

Mary Hennick

Molly Hennick

Rebecca Hennick

Susan Hennick

1. What schools have I attended?

Ans: A screenshot of a computer

Description automatically generated

1. What are some of the people I know (three or four is enough)?
2. What are some of my interests (two or three is enough)?
3. Do I have children? Names?
4. Did/do I own a domain name?

Ans: Lairnet.academy