A picture containing graphical user interface

Description automatically generated

**CYBV 480: Cyber Warfare**

Reconnaissance Exercise

**Part 1 – People Exercise**

Look yourself up using the following web-based services:

US Search (ussearch.com/search-select/)

Spokeo (spokeo.com)

Graphical user interface, website

Description automatically generated

Chart

Description automatically generated with medium confidence

Questions:

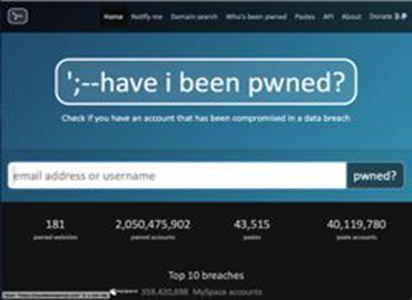
1. How did the information differ from one site to another?
2. How could the information be used to target you?

**Part 2 – Credentials Exercise**

Look your email up using the following web-based services:

Have I been Pwned (haveibeenpwned.com)

Data Breach Check (https://whatismyipaddress.com/breach-check)



Graphical user interface, text, application

Description automatically generated

Questions:

1. How did the information differ from one site to another?
2. How could the information be used to target you?

**Part 3 – Social Media Exercise**

This part of the exercise will provide you with some experience in navigating social media to obtain information. For Social Park and ChirpyHub you will identify information about an individual and company. Annotate any information that may be valuable from the perspective of an attacker or penetration tester.

Social Park

1. Open a browser within CyberApolis and navigate to Social Park
2. Create an account
3. Search for CyberApolis Power Company
4. Examine the following aspects of the Power Company:
   1. Posts
   2. Photos
   3. Contacts
   4. Through the contacts, navigate to Annie Brown’s page

ChirpyHub

1. Open a browser and navigate to ChirpyHub
2. Create an account
3. Search for the CyberApolis Power Company
4. Examine the following aspects of the Power Company:
   1. Quips
   2. Following
   3. Followers
   4. Through the followers, navigate to Annie Brown’s page

**Part 4 – Metadata Exercise**

Metadata Hunt

1. Open a browser and navigate to the Artificial Creations website
2. Download the logo in the upper left corner of the website
3. To use exiftool, you will need to ensure that you use the correct / full path when you save the file.
   1. Save to the desktop and make sure you are in the desktop in the CLI
   2. Type in the full path when running the command
4. Open a terminal window
5. Type the following command:
   1. C:\Users\Administrator> exiftool [file path]
   2. Example if logo is on the desktop: C:\Users\Administrator\Desktop>exiftool logo.png
   3. View the logo.png metadata
6. If you have time, download a document from the web and extract the file’s metadata

Questions:

1. What metadata is visible?
2. Of the data available, what would be the most valuable to an attacker or penetration testing?
3. Research how you would be able to modify the metadata. Describe the process.
4. Research whether metadata can be erased. If so describe the process.

**Part 5 – Recon-ng**

This exercise will introduce you to the recon-ng tool.

Steps:

1. Log into CyberApolis
2. Double click on the Kali Linux Shortcut on your desktop
3. When the command prompt comes up type the following:
   1. recon-ng
   2. You should see the recon-ng command prompt

Text, letter

Description automatically generated

1. There may not be any modules loaded. If you see zero modules loaded then type the following
   1. marketplace install all
2. Next, we will use a module that doesn’t require an API key, specifically one for gathering domain names. We will do one in within cyberapolis and one for University of Arizona.
   1. Type the following (tab autocomplete is your friend):
      1. modules load hackertarget
      2. options set SOURCE capower.com
      3. run
      4. options set SOURCE arizona.edu
      5. run
3. There are many modules that you can explore. If you do anything besides what is listed in the exercise only use those modules against domains within CyberApolis.