A picture containing graphical user interface

Description automatically generated

**CYBV 480: Cyber Warfare**

Information Gathering Exercise

This exercise is designed to be an introduction to Maltego. The cyber program has additional courses that go in depth for open source intelligence (OSINT) and cyber threat intelligence that will go into more detail for this excellent tool. Once you feel comfortable with the tool, conduct additional research using the URL for SANS (www.sans.org). Review the output

**Part 1**

Steps:

1. From your Windows Desktop open up Maltego
2. Once Maltego opens, click on Maltego CE (Free)
3. Accept the license agreement and click next
4. If you have not already done so, you will need to create an account.
5. Once you are logged in, you should see the transform hub. A transform is a small piece of code that fetches related information for a given input, and formats the results to be returned as entities to Maltego. Transforms should be extensible and return the smallest piece of information possible.

A screen shot of a computer

Description automatically generated

**Part 2**

1. Within Maltego there are a variety of machines. To see the options follow these steps:
   1. Click on machines
   2. Run Machine
   3. Review list of machines
2. Some of the more common ones are:
   1. Company stalker – this machine will try to get all email addresses at a domain then see which resolves on social networks. It also gets documents and extracts metadata. The input is domain.
   2. Footprint 1 – Performs a fast, basic footprint of a domain
   3. Footprint 2 – Performs a mild footprint of a domain
   4. Footprint 3 – Performs an intense footprint on a domain. It takes a while and it eats resources. Use with care.
   5. Person – Email Address – tries to obtain someone’s email address and sees where it is used on the internet. Input is an email address.

A screenshot of a computer

Description automatically generated

**Part 3**

1. Click on the company stalker machine and click next
2. In the domain name enter
   1. Sans.org
3. Click finish
4. If you see a warning banner just hit close. This is notifying you that the community edition has some limitations.
5. Click on the proceed with selected (Blue Arrow)

A screenshot of a computer

Description automatically generated

1. This brings up the email addresses associated with sans.org
2. It also brings up additional information on a couple of people.
3. Let’s look into one of them. If you click on allthatissold, it will bring up additional information in the detail view.
4. Click on the view (red arrow). This will bring up the myspace page for this individual.

A screenshot of a computer

Description automatically generated