Name: Cristian Barreno

Incident Response exercises first group - Exercise 1 Incident response Steps

Task #1
List all the steps in a numbered list, and then separately explain each step in your own words.

1. Preparation: You are going to list all resources available for incident response. Including communication channels. It's important to train the team.
2.Detection: You are going to identify and assess the threat.
3.Analysis: you are going to check log files and intrusion detection systems.
4.Containment: Here you isolate the affected system.
5. Eradication: Here you are going to outline the methods for removing threats.
6.Recovery: Here you are going to restore affected systems to their pre- incident stage.
7.Leassons learned: you are going to document, talk to your team to make the organization stronger, and improve security posture.

Incident Response Phases
Task #2
List all the phases in a numbered list, and then separately explain phase step in your own words.

1.Preparation: What is the organization to respond to an incident? List resources, checklist, and train people involved.
2.Detection and analysis: What tools for detecting and analyzing are available? Look for indicators of compromise, and log files.
3.Containment, eradication, and recovery: The goal here is to isolate the affected systems, and mitigating service disruptions.
4.Post incident activity: The goal here is to learn from what went well, and what went bad, and how to improve the security posture.

Incident Response Policy
Task #3
Explain what the purpose of an incident policy is in your own words.

There has to be a document that lays down a structure framework for the incident response team to follow. This document should include the boundaries of the policy, roles and responsibilities of the incident response team, communications, legal compliance, response

strategy, criteria of what constitutes a security incident, Training requirement, a schedule about how often the policy needs to be reviewed, list of all tools and resources.

Incident Response Plan
Task #4
Explain what an IRP is, and what purpose does it play in your own words.

The goal of an Incident Response Plan is to prepare, act, and recover in case of a cyber attack.

Communication Plan
Task #5
Explain what an IRP is, and what purpose does it play in your own words.

IRP stands for Incident Response Plan. Is what organizations use to prevent, act, and recover from a cybersecurity incident.

Recon
Task #6
Explain what an enumeration is, and what purpose does it play in your own words.

Enumeration is data gathering about a network that a threat actor wants to target.

Exfiltration
Task #7
Explain what an tunneling is, and what purpose does it play in your own words.

Tunneling allows you to send private communications, across a public network. Tunneling technique allows you to hide malicious traffic with another format and send it through the network undetected.

Communication
Task #7
Explain what a pem file is, and what purpose does it play in your own words.

PEM stands forPrivacy enhanced email, is a text based file that is used to store digital certificates, and keys.

Incident Response – The Dominican Republic Incident

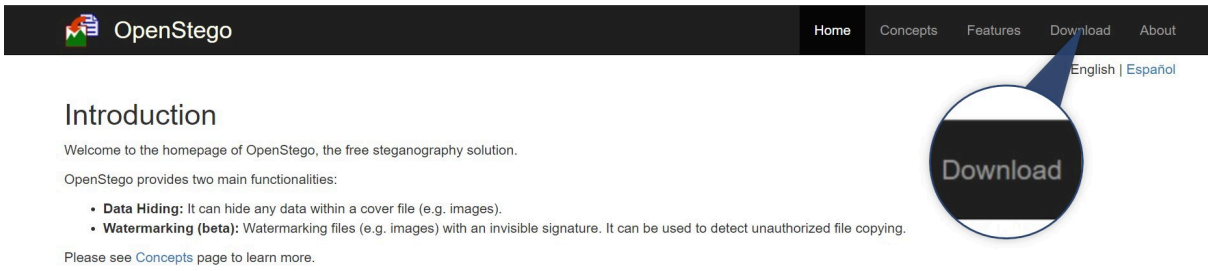
Task #1
Explain your takeaways on the incident response podcast.

The takeaways from the D.R Incident podcast are
-That no matter how small a country is it has to have the best cybersecurity incident response tool and resources.
- Omar reachout to cybersecurity professionals from Panama that were just targeted. For me that shows how important networking is, and making friendships.
-Is important to be up-to- date on worldwide cybersecurity events, know the names of different threat groups and always be informed.
-the last takeaway is to provide training to government workers, and teach them to report any emails or activity to cybersecurity professionals.

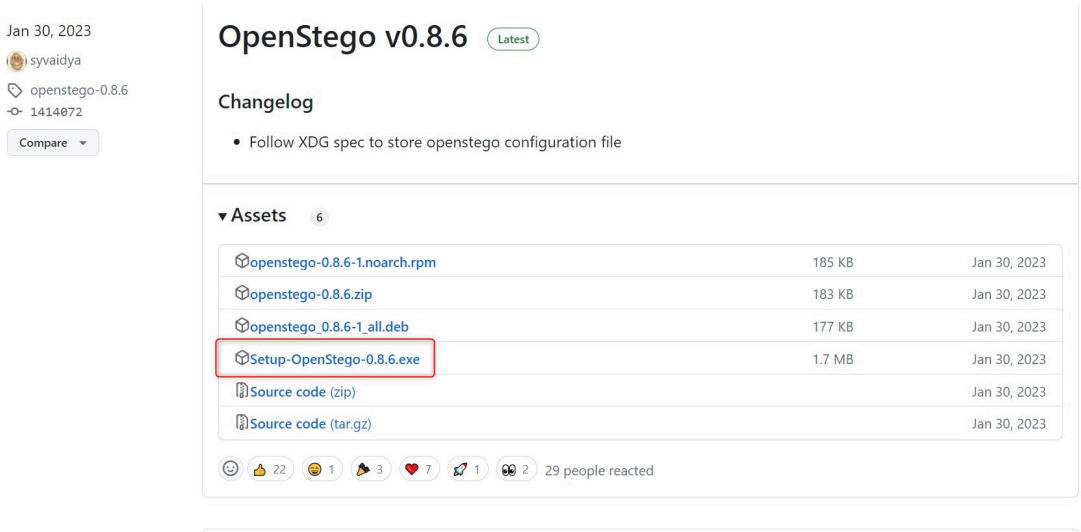
Incident Response exercises first group - Exercise 2 Steganography - Windows

Task #1

To download openstego i went to: https://www.openstego.com/

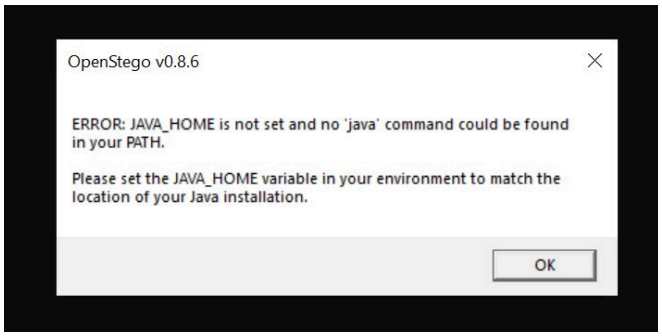


Next, i clicked on the downloads tab, and clicked on Setup-Openstego-0.8.9.exe

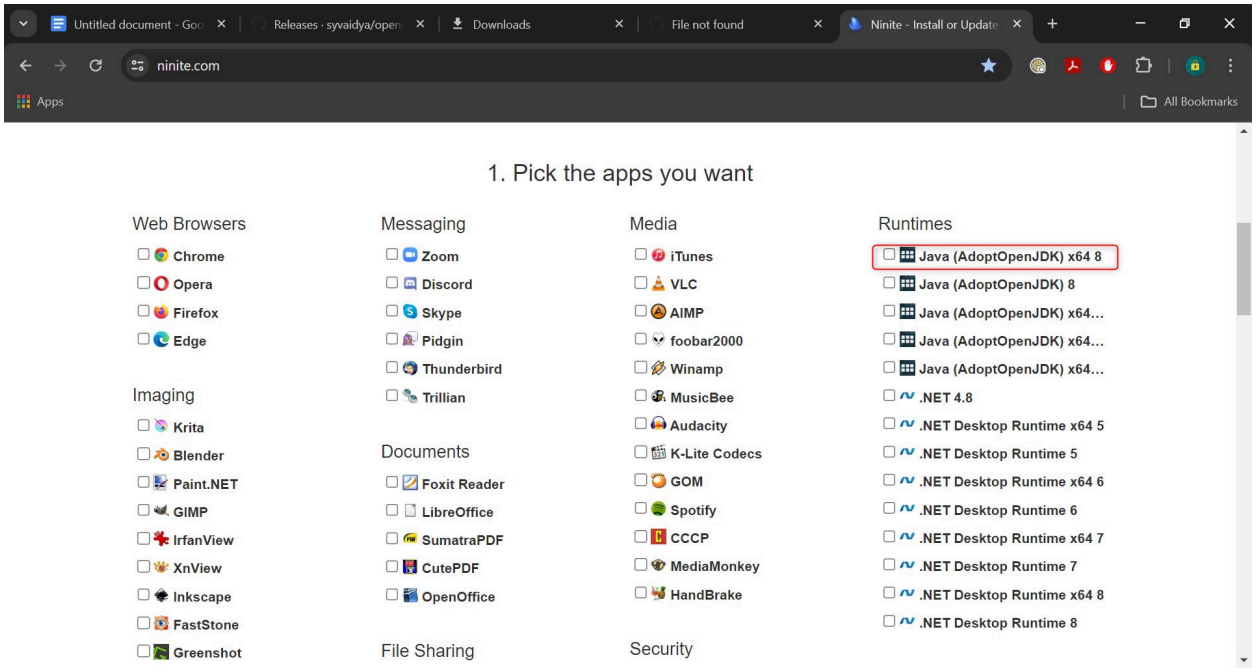


Task #2 - Dependencies

I got a dependency error, and I had to read it carefully to troubleshoot it. The error message is telling me that it is missing Java, and I need to install it so the application can run correctly.



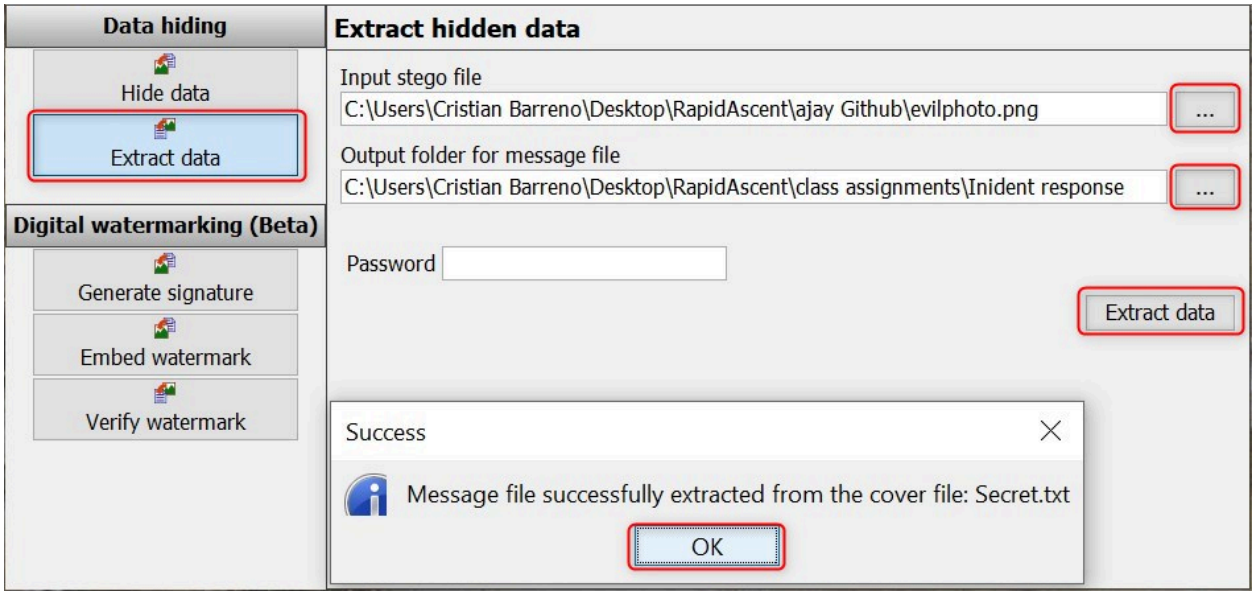
To install Java i went to ninite.com, and clicked on Java x64



Task #3 - Data Extraction

I re-run opentego, and now it worked perfectly fine.

Next, I clicked on Extract data, then I selected the input stego file, followed by the output folder for the message file, and finally clicked on extract data.

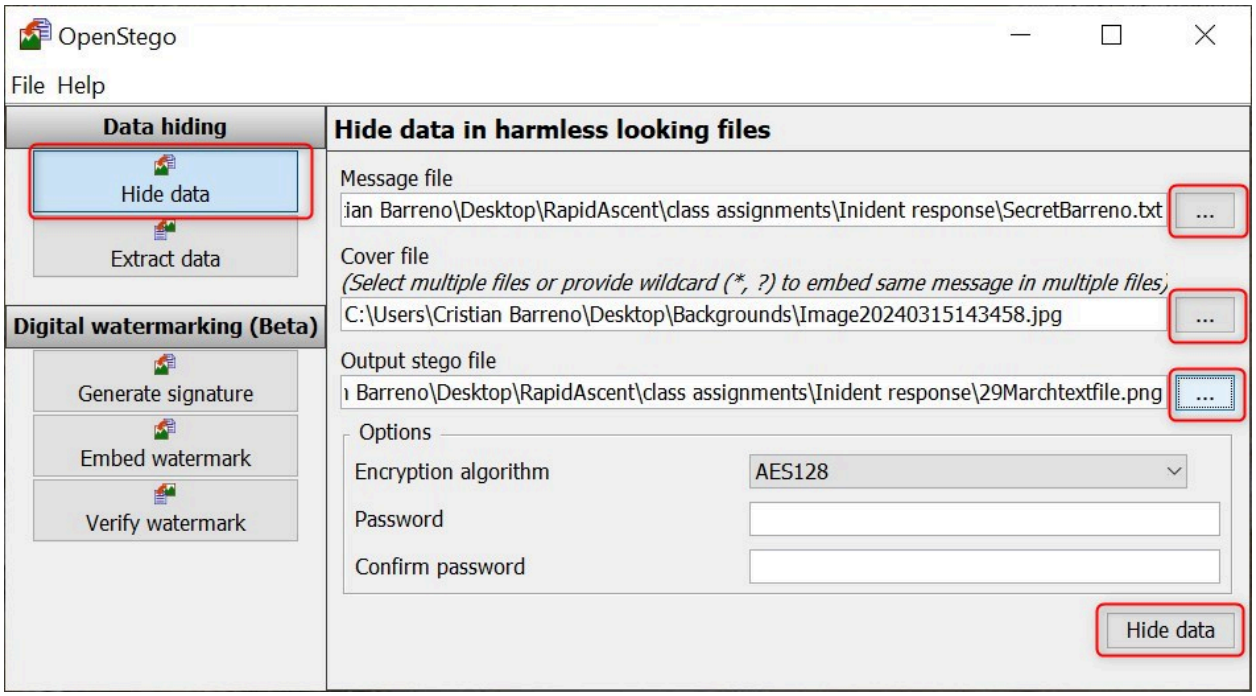


The output generated in a new file. I opened the file, and this is the secret message:

Openstego is capable of extracting secret messages that have been hidden in files by using steganography. We selected the location of the file with the hidden message, and then the location that we want the output message to go.

Task#4 - Implement Steganography

To implement steganography I clicked on Hide data, then I created a .txt file with a hidden message, then I selected a funny picture from my folder, followed by the output stego file location.



Exercise 3 - Steghide

Task #1 – Installation

I used dpkg which stands for debian package manager, then I connected the output of the first command with pipe “|”, directly into the output of grep Steghide. The grep command is used to search files of a specific pattern or word.

Task #2 – Download and extract the secret

I extracted the image and saved it in my folder.

In the image below I typed steghide - -help to learn more about steghide, and learn how to extract a secret message from an image.

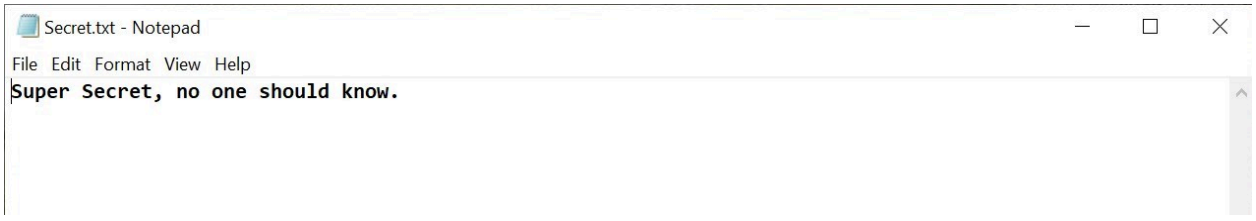
```
lynx@lynx: ~
options for the info command:
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to get info about embedded data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg
lynx@lynx:~$
```

I entered: Steghide extract -sf Funny-Cat-Hidden.jpg. Finally , I typed the password that I was given by the originator,and it gave me the output in a file.

```
lynx@lynx: ~
lynx@lynx:~$ steghide extract -sf Funny-Cat-Hidden.jpg
Enter passphrase:
the file "secret.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.txt".
lynx@lynx:~$
```

Below is the screenshot of the Hidden message in a .txt file.



Task #3 – Embed a secret into an image

This task was fun to do, and I look forward to a classmate reading my secret message. What i did in this task was first, download a funny .jpg file, then i created a secret message on Notepad.
After I downloaded both files in my download folder, I secure copy (scp) both items in the command prompt.
In my Linux CLI i entered steghide embed -cf funnyraccoon.jpg -ef gtaBarreno.txt.
And the last step was to create a password.