TASK 1 – Intro

In task one we need to read the introduction to the room and the room lets us know

“All answers can be obtained via passive OSINT techniques, DO NOT attempt any active techniques such as reaching out to account owners, password resets, etc to solve these challenges.”

For this task if you read all the way through the information tells you the following

“Ready to get started? Type in "Let's Go!" in the answer box below to continue.”

Answer = Let’s Go!

Task 2 – TIP OFF

In the information deplayed you need to read the following

“The OSINT Dojo recently found themselves the victim of a cyber attack. It seems that there is no major damage, and there does not appear to be any other significant indicators of compromise on any of our systems. However during forensic analysis our admins found an image left behind by the cybercriminals. Perhaps it contains some clues that could allow us to determine who the attackers were? “

Calendar

Description automatically generatedThis give us a link to a picture

<https://raw.githubusercontent.com/OsintDojo/public/3f178408909bc1aae7ea2f51126984a8813b0901/sakurapwnedletter.svg>

the link above also tell us it’s a svg file which is a scalable vector graphics meaning that some times this can contain metadata embedded in the file when the image is generated.

So I clicked on inspect and found a file path highlighted below

Text

Description automatically generated

Answer to task 2 is = SakuraSnowAngelAiko

Task 3

I went on used google to search” SakuraSnowAngelAiko”

And found the following

<https://github.com/sakurasnowangelaiko> and what stood out was one of the repositories called PGP ( pretty good privacy)

Graphical user interface, text

Description automatically generatedwe can see here that this is encoded in base 64 so to decode this head over to cyber chef making sure not to copy the being of and end of pgp we will then get this output

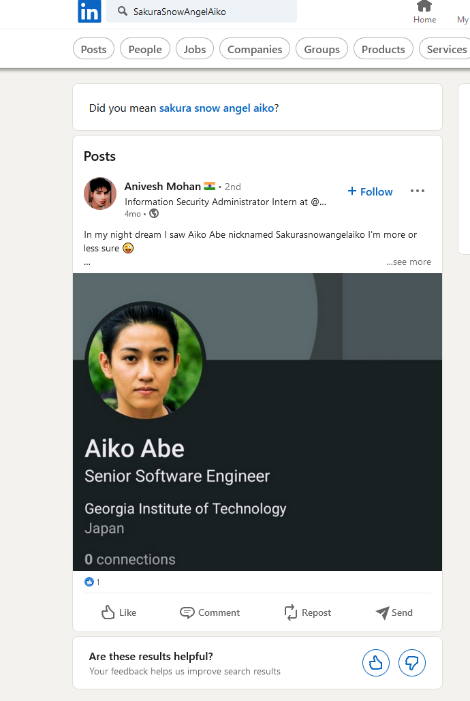
Graphical user interface, text

Description automatically generated

Making task 3 answer = [SakuraSnowAngel83@protonmail.com](mailto:SakuraSnowAngel83@protonmail.com)

Task 3 .2 - I searched social media platforms using the user name given on task 2 and went to LinkedIn in first and was given the answer

Task 3.2 = aiko abe



Task 4

This is where I went through thr known cryto respoities and took some time until I went through ETH is also called **Ethereum which is the answer to**

**Task 4.1 Ethereum**

A screenshot of a computer

Description automatically generated with medium confidencei then looked down on the history and found this ( highliegted in yellow)

A screenshot of a computer

Description automatically generated

4.2 answer = 0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef

Know we know his wallet I went to the website after much digging <https://etherchain.org/>

We can see the users’ transactions

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, table

Description automatically generated



So we can see that the mining pool is

4.3 answer – Ethermine as show from above

4.4 answer – Thether as we can see the other attacker has exchanged

Task 5

Just as we thought, the cybercriminal is fully aware that we are gathering information about them after their attack. They were even so brazen as to message the OSINT Dojo on Twitter and taunt us for our efforts. The Twitter account which they used appears to use a different username than what we were previously tracking, maybe there is some additional information we can locate to get an idea of where they are heading to next?

We've taken a screenshot of the message sent to us by the attacker, you can view it in your browser [here](https://raw.githubusercontent.com/OsintDojo/public/main/taunt.png).

Quick google give us

Graphical user interface, text, application

Description automatically generated

5.1 - @SakuraLoveraiko

Then I found

Graphical user interface, text, application

Description automatically generated

Then using the screen shot from the hint section we can see the following information

A screenshot of a computer

Description automatically generated with medium confidence

Answer 5.2 = http://deepv2w7p33xa4pwxzwi2ps4j62gfxpyp44ezjbmpttxz3owlsp4ljid.onion/show.php?md5=b2b37b3c106eb3f86e2340a3050968e2

Finally, the last flag for this section. Try to search for “find wifi ssid and bssid online” on Google, and you will get this website <https://wigle.net>

Create an account, and you will be able to search by advanced queries. Look for the SSID, and you got the bssid :

Graphical user interface, text, application

Description automatically generated

Answer 5.3 = 84:af:ec:34:fc:f8

Task 6 homehoube

**Background**  
Based on their tweets, it appears our cybercriminal is indeed heading home as they claimed. Their Twitter account seems to have plenty of photos which should allow us to piece together their route back home. If we follow the trail of breadcrumbs they left behind, we should be able to track their movements from one location to the next back all the way to their final destination. Once we can identify their final stops, we can identify which law enforcement organization we should forward our findings to.  
  
  
 **Instructions**  
  
In OSINT, there is oftentimes no "smoking gun" that points to a clear and definitive answer. Instead, an OSINT analyst must learn to synthesize multiple pieces of intelligence in order to make a conclusion of what is likely, unlikely, or possible. By leveraging all available data, an analyst can make more informed decisions and perhaps even minimize the size of data gaps. In order to answer the following questions, use the information collected from the attacker's Twitter account, as well as information obtained from previous parts of the investigation to track the attacker back to the place they call home.