Beginner OSINT Training for CTFs

ECU RedRoom training

26th and 28th September 2024.

Training by - Lindsay Coudert SM Tafe.

What will we be covering today?

- OSINT in general
- Some demos and walkthroughs
- Try some yourself

What is OSINT

OSINT =

Open Source Intelligence

Sources can include:

- Social Media
- Public records
- News articles
- And more

Flag format example:

Redroom{Bathurst_Showgrounds}

Don't be afraid to ask questions throughout the presentation as well. You are here to learn.

What is OSINT

It is the gathering of information which is available to the public.

It is NOT hacking or accessing restricted data.

Use in CTFs

It is widely used in CTFs and anyone can do OSINT as long as they have internet access and an analytical mind.

TO NOTE:

Ethical considerations are important when performing an OSINT investigation. Stick to what you need for a challenge and nothing more.

Common OSINT Methods for CTFs

OSINT is widely used in CTFs. Beginner challenges often include things such as using social media profiling, finding the location that an image was taken, reverse image lookups.

Social Media

Social media is a valuable resource for OSINT. Profiles can reveal names, locations, interests, and more. This information can be used to solve challenges. For example, an OSINT challenge can include the someone's github username.

Reverse Image lookups

Another very popular CTF challenge is reverse image lookups, this is usually used when the flag is looking for a specific location whether it's the name or the coordinates of said location.

Common CTF challenge examples

Find the location of a given image:

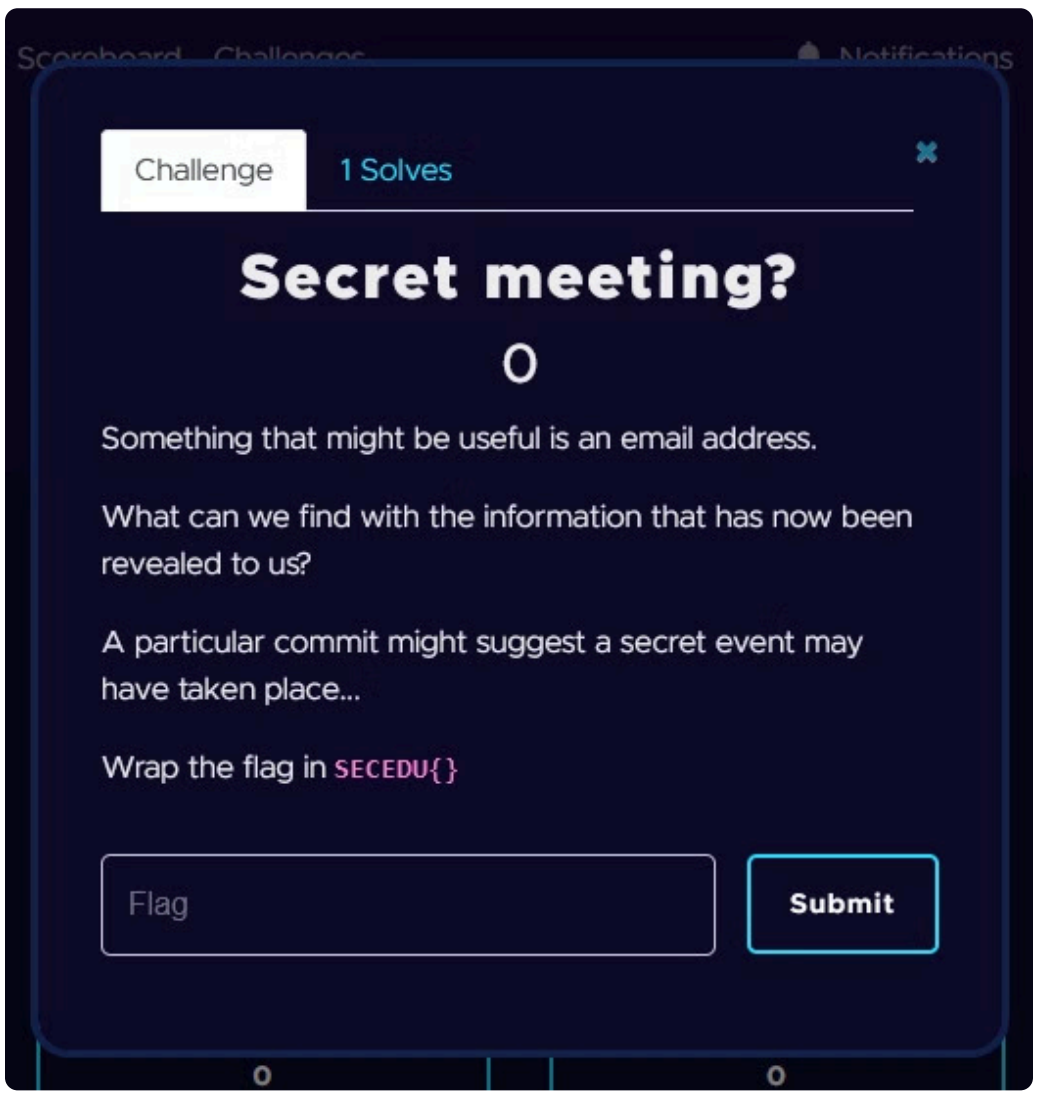
One of the common CTF challenges are finding locations of a given image:

Email analysis and analysis of a person:

From the SECEDU Australian Cybersecurity Games one challenge included the use of email analysis and opened up 3 more. For the main challenge we used a tool called Epieos: https://epieos.com/

The other three challenges that opened up from this one was, what is the name of Cipher's beloved cat? And what is Cipher's favourite colour - for this we used the wayback machine. The third challenge asked for the birthday of the email's owner. The fourth challenge was finding a set of co-ordinates.

https://web.archive.org/

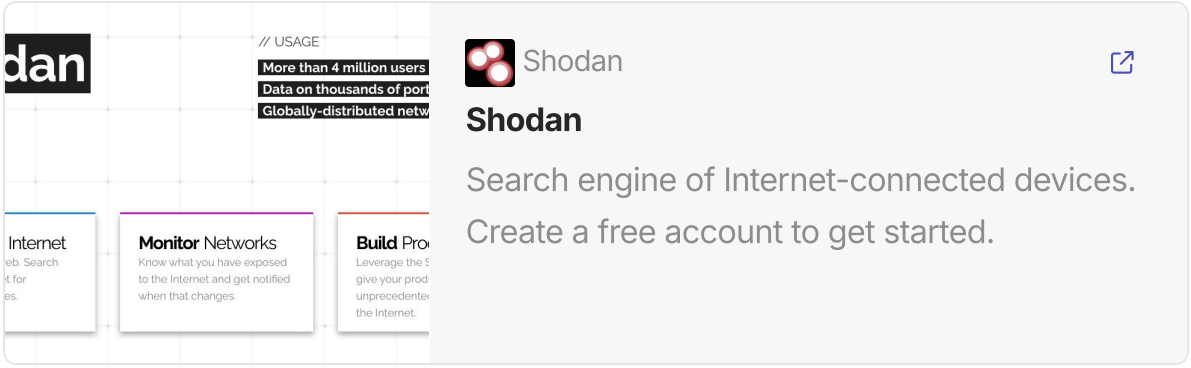


Run through of the challenges above:

- Email that we encountered and this is what gets put into Epieos: CipherBre4ker@gmail.com
- To find the birthday we simply go back through the calendar to find the date.
- To find the cat's name and the accounts favourite colour we simply use their reddit account.

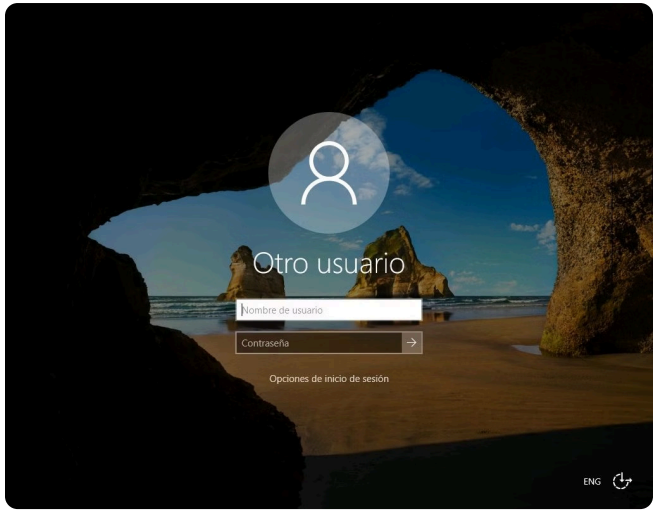
Shodan and CTFs

Shodan can be used in OSINT challenges:



Not very common but a good skill to know if you come across something similar to what is on the right. I haven't seen it often but it is still useful if there are those challenges

- Find the IP address of the image on the right.



⚠ **Do NOT attempt to gain access or manipulate the devices that you find.**

Give this one a go:

Find the co-ordinates of this given cafe within Perth:

Little Willy's

▼ Answer and how to solve it:

> Answer: -31.94747 15.8574288
>
> How to solve it: Google maps https://www.google.com/maps

Extra Tools:

inteltechniques.com

IntelTechniques Search Tool

Search Engines Facebook Twitter Instagram LinkedIn Communities Email Addresses Usernames Names Addresses Telephone Numbers Maps Documents Pastes Images Videos Domains IP Addresses Business & Government Vehicles Virtual Currencies...

osintframework.com

OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally (D) - Google Dork, for more information: Google Hacking (R) - Requires registration (M) - Indicates a URL that contains the search term and the URL itself must be edited manually

Try some on your own:

Below is a website that you can to and practice some exercises they range from easy to hard so feel free to try out at your own pace:

Sofia Santos | OSINT Analysis & Exercises

List of OSINT Exercises – Challenge Yourself!

Looking to expand your OSINT skills or put your existing ones to the test? Give it a go on my list of free OSINT challenges! What are the OSINT Exercises? These OSINT...

Questions???

Hope you learned something