



OSINT



INTRODUCTION

OSINT stands for Open Source Intelligence. Technical terms is defined as intelligence produced by collecting, evaluating and analyzing publicly available information with purpose of answering a specific intelligence question. It's the process of gathering information from publicly available sources to be used for intelligence purposes. These sources can include social media, news articles, government reports, websites, forums, and even public records. OSINT is widely used in fields like cybersecurity, law enforcement, and business for things like threat assessment, investigative research, or market analysis.

Executive summary

The OSINT workshop provided valuable insight into the significance of open-source intelligence in various fields, particularly in cybersecurity. It emphasized how publicly available information can be leverages for threat assessment, investigative research, and security monitoring.

One of the key takeaways was understanding OSINT's role in cybersecurity, such as tracking cybercriminals, monitoring security vulnerabilities, and identifying stolen data on the dark web. The workshop also introduced practical tools like SHERLOCK for username OSINT, which helps track user profiles across multiple platforms. Additionally, participants learned how to check for data breaches using Breach Directory and analyze hacker activities through Breach Forum.

Overall, the workshop highlighted the power of OSINT in cybersecurity and beyond, emphasizing the need for ethical usage and continuous learning in this rapidly evolving field

CONTENT

How OSINT used in cybersecurity?

Defensive uses – Threat intelligence

1. Tracking cybercriminals
2. Following security vulnerability discussions to stay ahead of potential threats.
3. Monitoring stolen data being sold or shared (usually on darkweb)

Username OSINT

Installing SHERLOCK

- If system runs on linux (Debian) : `sudo apt install sherlock.`
- If system runs on windows (with pip/ pipx installed) : `pipx install sherlock-project.`

SHERLOCK usage

- For searching one user : `sherlock insert_username1`
- For searching multiple users:
`sherlock insert_username1 inser_username2 insert_username3`
- Other tools : <https://instantusername.com>

Data breach Investigation

How to find out if our data has been breached?

- <https://breachdirectory.org>

Analyzing Database of Breachforum to Find Hackers

Breachforum is a forum for discussing hacking topics and distributed data breaches.

- Visit <https://bf.based.re> to find out hacker's username and email.

How to OSINT a website?

1. Identity of an online user : Username or alias
2. Identity of a website : Domain name or IP address
 - Extract domain from the URL of the website.
 - Use <https://lookup.icann.org> to analyze the domain.

How to retrieve deleted post from a website?

- Use <https://web.archive.org>

REFLECTION

During the workshop, I learned about OSINT (Open-Source Intelligence) and how public information can be used to track cyber attackers and analyze security vulnerabilities. I explored tools like Sherlock for searching social media accounts, and BREACH DIRECTORY website to check if my email or username was compromised ? I also learned how to retrieve a deleted post using the Wayback Machine. It was interesting and useful!

PREPARED BY...
TIC
TECH



SANJANA DEVI A/P RAVI
A24CS0184



RAYAN BAHA ELDIN
ELKHIR ELAWAD
A24CS4033



NURUL HUDA NABILAH
BINTI ABDUL RAHIM
A24CS0176



SARAH HAMIZAH BINTI
HASRAM
A24CS0296



MOHAMED MAHMOUD
RAMADAN
A23CS4045