**Day 3 - Open source intelligence (OSINT) (20.6.)**

**1. Introduction to OSINT & Methodologies**

**Topics**

* Definition and scope of **OSINT**
* Intelligence cycle: **Planning → Collection → Analysis → Reporting**
* Legal and ethical considerations
* Difference between passive and active reconnaissance
* OSINT vs. closed-source or classified intelligence

**Required Infrastructure & Components**

* OSINT framework map (e.g. [osintframework.com](http://osintframework.com))
* Browser-based OSINT tools: whois, nslookup, theHarvester
* VPN or anonymization tools for safe passive research
* Sample investigation target (e.g., fake company or domain)

**To-Dos & Steps**

1. Understand the OSINT lifecycle and planning phase
2. Use passive techniques to gather infrastructure data (domain, DNS, IP)
3. Document findings in an OSINT investigation log
4. Discuss legal and ethical constraints using real-world cases
5. Compare OSINT to technical recon (e.g., Nmap, Shodan)

**Webinars**:

* [Recorded Future Webinar: OSINT Best Practices](https://www.youtube.com/watch?v=Q5Y5SQmKXW4) – 00:50
* [SANS Institute Webcast: Introduction to OSINT](https://www.youtube.com/watch?v=PNeCqw8OLeA) – 00:25

**YouTube**:

* [What is OSINT? Introduction to Open Source Intelligence | GOSINT Training](https://www.youtube.com/watch?v=Sa5LbKqCmFI) – 00:07
* [Intelligence Cycle Explained | OSINT Foundation](https://www.youtube.com/watch?v=B2wRbotog-Y) – 00:05

**Reading Material**:

* [OSINT](https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf) – 16 pages
* [OSINT Framework Map](https://osintframework.com/)
* [Bellingcat’s Guide to Online Investigations](https://www.bellingcat.com/)
* [CISA Best Practices for Open Source Information](https://www.cisa.gov/opensource)

**2. OSINT Tools & Frameworks**

**Topics**

* Key tools for OSINT:
  + **Maltego**, **Spiderfoot**, **theHarvester**, **Recon-ng**, **Google Dorks**
* Meta search engines & social media scraping
* Image & geolocation analysis (ExifTool, Google Images, Yandex)
* Dark web and breach data search basics
* Frameworks: OSINT Framework, IntelTechniques, Bellingcat approach

**Required Infrastructure & Components**

* Tool access (online or installed): e.g., Maltego CE, Spiderfoot HX
* Google Dorking cheat sheet
* Metadata-rich media files for analysis
* Investigation notebook or case file template

**To-Dos & Steps**

1. Explore the OSINT Framework and select tools for different recon categories
2. Run Google Dorks to extract indexed info from a sample domain
3. Use theHarvester or Spiderfoot for automated scans
4. Extract EXIF data from images and triangulate locations
5. Summarize all collected data in a mini case report

**Webinars**:

* Maltego Webinar Series: Graph-Based OSINT[Webinars](https://www.maltego.com/webinars/)
* [SANS OSINT Summit Talks](https://www.youtube.com/playlist?list=PLs4eo9Tja8bjQITK4k62hXOO6XByOTYll)

**YouTube**:

* [Maltego for OSINT Investigations | Maltego Official](https://www.youtube.com/watch?v=onHHXNDnkrs) – 00:19
* [SpiderFoot Automated OSINT Tool](https://www.youtube.com/watch?v=yw_KPBdAKHo) – 00:10
* [Google Dorking for Beginners](https://www.youtube.com/watch?v=Jsg9JOyoeg0) – 00:12
* [Metadata Analysis with ExifTool](https://www.youtube.com/watch?v=HU_euJyxYB4) – 00:43

**Reading Material**:

* [Maltego Community Edition Download (Free)](https://www.maltego.com/downloads/)
* [Spiderfoot Open Source Project](https://github.com/smicallef/spiderfoot)
* [Recon-ng Framework Documentation](https://github.com/lanmaster53/recon-ng)
* [Google Dorking Cheat Sheet](https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06)

**3. Social Engineering & Human-Focused OSINT**

**Topics**

* Footprinting individuals: usernames, emails, profiles, social media
* Tracking employee exposure on platforms like LinkedIn
* Social engineering pretexting & recon (phishing preparation)
* Data leakage sources: pastebins, breach data, resume dumps
* Psychology of trust exploitation & phishing targeting

**Required Infrastructure & Components**

* Dummy social media accounts or sanitized targets
* Tools like **Sherlock**, **WhatsMyName**, or manual recon techniques
* Pastebin search engines or breach checkers (HaveIBeenPwned)
* OSINT reporting template with human-centric section

**To-Dos & Steps**

1. Use Sherlock or similar to correlate usernames across platforms
2. Search for email exposure in public breach datasets
3. Analyze a public LinkedIn profile to map org structure
4. Build a target profile for a simulated phishing scenario
5. Discuss mitigation: awareness training & digital footprint hygiene

**Webinars**:

* [Trace Labs Webinar: Social Engineering and OSINT](https://www.youtube.com/watch?v=IfI2dil5vPw) – 00:24
* [SANS: Social Engineering Techniques and Mitigation Webinar](https://www.youtube.com/watch?v=YVqurfWzB-Q) – 00:41

**YouTube**:

* [Using Sherlock for Username OSINT](https://www.youtube.com/watch?v=YUBps_PHSSk) - 00:08
* [Breach Data for OSINT Investigations](https://www.youtube.com/watch?v=MU6515T5yc4) – 00:15
* [LinkedIn OSINT Techniques](https://www.youtube.com/watch?v=BRLQqn6ktVY) – 00:07

**Reading Material**:

* [Sherlock – Hunt Usernames Across Social Networks (GitHub)](https://github.com/sherlock-project/sherlock)
* [WhatsMyName – Username Enumeration](https://github.com/WebBreacher/WhatsMyName)
* [Have I Been Pwned: Email Breach Checking](https://haveibeenpwned.com/)
* [The Psychology of Social Engineering (Whitepaper)](https://www.researchgate.net/publication/328705687_The_Psychology_of_Social_Engineering)

**Afternoon Lab: TryHackMe – OSINT Rooms**

* **Google Dorking**: Practice using search engine tricks to uncover sensitive data
* **OSINT Challenge 1**: Investigate clues to track digital identities
* Collect artifacts, map relationships, and simulate reporting
* Compare results across teams or individuals for peer analysis
* [TryHackMe: OSINT Fundamentals Room](https://tryhackme.com/)
* [TryHackMe: Google Dorking Room](https://tryhackme.com/) *(Hands-on search engine hacking techniques)*
* [TryHackMe: OSINT Challenge 1](https://tryhackme.com/)

*Alternative labs*:

* [Hack The Box – Sherlock OSINT Challenges](https://www.hackthebox.com/)

**🎯 End-of-Day Goal**

Participants should be able to:

* Explain the OSINT process and ethical boundaries
* Use common OSINT tools for passive information gathering
* Identify human and organizational digital footprints
* Perform structured open-source investigations
* Apply OSINT in threat intelligence, red teaming, or awareness contexts