OPEN SOURCE INTELLIGENCE

IST 110, GROUP 7

ZACHARY MATTIS

ODILIA KAMGA

WHAT IS OPEN SOURCE INTELLIGENCE?

- Intelligence (information) produced by collecting, evaluating and analyzing publicly available sources with the purpose of answering a specific intelligence question.

WHO USES OSINT?

- Governments
- Businesses

WHY USE OSINT?

- Security and Intelligence
  - Identify terrorism and cyber attacks
- Business and Market Research
  - Analyze competitors
  - Analyze industry trends

OSINT TECHNIQUES

- Domain Research
- OSINT RECONNAISSANCE

DOMAIN RESEARCH

WHAT IS IT?

- Gathering publicly available information about a specific domain name

WHAT IS IT USED FOR?

- Discover information about a specific domain name like when the domain expires
- Reveal unrelated connections if more than one domain are hosted on the same IP address

OSINT RECONNAISSANCE

WHAT IS IT?

- This is the process of gathering publicly available information about a target such as an individual, organization, or system using open sources.

CATEGORIES

PASSIVE

- Involves gathering information about a target network or device without directly engaging with the system.

ACTIVE

- Involves interacting with the target to extract information, which may leave logs or traces that could alert the target.

METHODS

PASSIVE

- Using search engines (Google Dorking)
- Passive DNS lookup to find historical domain information.
- Analyzing leaked data from breach databases.
- Querying public databases (WHOIS, Shodan, Censys).
- Searching social media profiles (LinkedIn, Twitter, Facebook).

ACTIVE

- Scanning a target’s network (Nmap, Zenmap, Shodan).
- Checking for vulnerabilities via web applications (OWASP ZAP, Burp Suite).
- Testing open ports and services.
- Engaging with employees through social engineering (email phishing, LinkedIn messages)