OPEN-SOURCE INTELLIGENCE

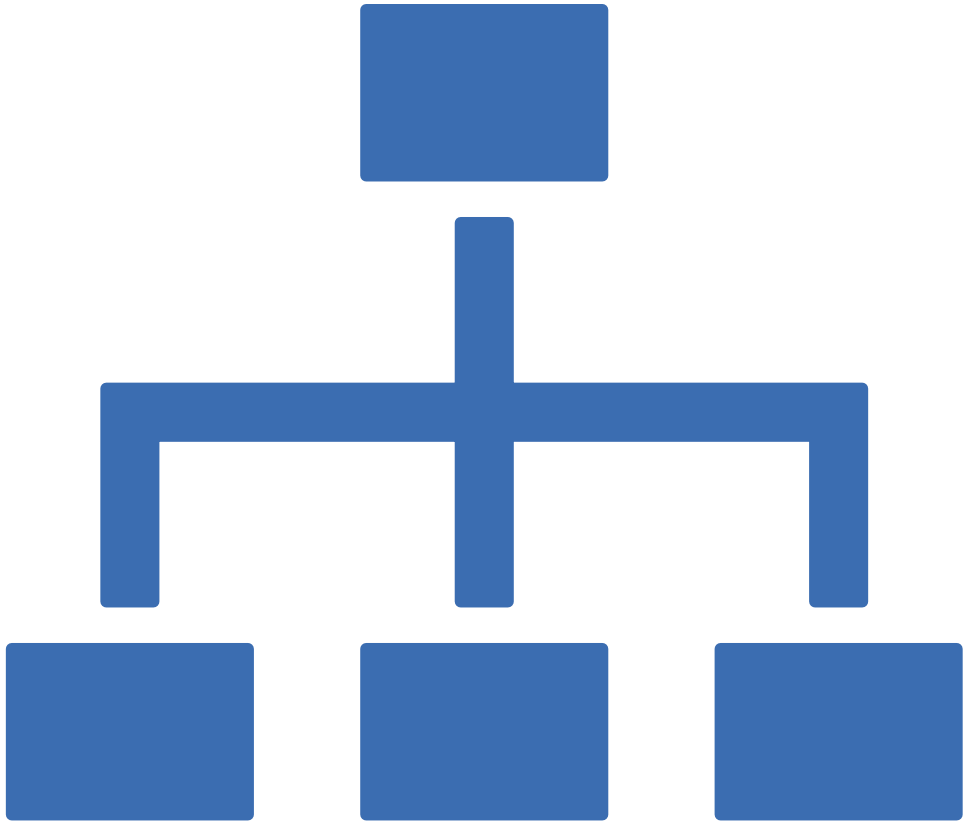
CyberSmarts

WHAT IS OSINT?

- Open-Source Intelligence
  - Retrieval, analysis, and access of publicly available data to gain knowledge of an entity-person, place, or thing.
  - Topics can range to, and from an endless array of subjects such as businesses, cultures, missing persons, devices, websites/servers.

WHAT'S OUR USE?

- Find people, places, and/or things:
  - Find data about yourself, or an organization of interest such as a prospective employer, or even a public figures.
  - Find information on the culture of a town, or even scan a device or server's IP address to find out information about the device(s) connected.



OTHER USES

- Reconnaissance
  - OSINT is usually performed during the Reconnaissance phase of hacking and pertinent information collected from this phase is carried over into the network Enumeration phase
  - Due to the vast amounts of information available to sift through on the Web, attackers must have a clear and defined search framework as well as a wide array of OSINT collection tools to facilitate this task and assist with processing the data; otherwise, they risk getting lost in the overwhelming sea of information that has become the Internet.

OSINT RECONNAISSANCE PHASES

- OSINT reconnaissance can be further broken down into the following 5 sub-phases
  - Source Identification: - As the starting point, in this initial phase the attacker identifies potential sources from which information may be gathered from. Sources are internally documented throughout the process in detailed notes to come back to later if necessary.
  - Data Harvesting: - In this phase, the attacker collects and harvests information from the selected sources and other sources that are discovered throughout this phase.
  - Data Processing and Integration: - During this phase, the attacker processes the harvested information for actionable intelligence by searching for information that may assist in the investigation

OSINT RECONNAISSANCE PHASES CONT.

- Data Analysis: – In this phase, the attacker performs data analysis of the processed information using OSINT analysis tools.
- Results Delivery: – In the final phase, OSINT analysis is complete and the findings are presented/reported to other members of the red Team.

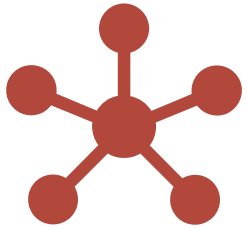
PRECAUTIONS

- Conflicting sources of information:
  - Misinformation, disinformation -> Invalid information
- All information that is out there is also available for cybercriminals
  - When you look at the mind map showing possible information sources and tools, you can begin to imagine all the potential malicious uses of that data
  - Identity frauds, social engineering, CEO frauds, targeted attacks with customized malware

OSINT TOOLS

Search Engines

Images



Social Networks

SEARCH ENGINES

- Depending on the context, you may want to use a different search engine during an investigation
  - Google and Bing (Europe and NA)
  - Baidu (Asia)
  - Yandex (Russia and Eastern Europe)

IMAGES

- For images, there are two things you want to know:
  - How to find any additional information on an image
  - How to find similar images
- To find additional information, the first step is to look at Exif data. Exif data is data embedded into an image when the image is created and it often contains interesting information on the creation date, the camera used, sometimes GPS data etc.
- To find similar images, you can use any image search engine of your choice, such as Google Images, Bing Images, and more.

SOCIAL NETWORKS

- Twitter: the API gives you the exact creation time and tool used to publish tweets. x0rz' tweets_analyzer is a great way to have an overview of the activity of an account. There are ways to find a Twitter id from an email address but they are a bit tricky
- LinkedIn: the most useful trick in LinkedIn is how to find a LinkedIn profile based on an email address
- Other Social Networks: Just find publicly available information

GOOGLE DORKING!? (ADVANCED GOOGLE SEARCHING)

- Dorking!?
  - Using advanced search features(operators) of Google. *Not limited to Google*
  - 'filetype:', 'inurl:', 'cache:'
    - "filetype: dat inurl: 'password'"

NETWORK MAPPING

- Nmap:
  - Open-source network scanning program. Network administration tool.
  - Provides details about the IP addresses connected to the network, and provides a log of opened ports, the operating system, etc.

'nmap 192.168.1.0'

RESOURCES:

Every and any search engine or database.

- Facebook
- Google
- Bing
- Yandex
- Lexus Nexus