Day 1 Foundations of OSINT

LinkedIn: @muhammed-dardir

1. Introduction

- This Course is staring point in OSINT will cover tools, techniques, process, and workflow.
- Open Source Data (OSD): Raw data
- Open Source Information (OSIF): Processed information
- Open Source Intelligence (OSINT): Analyzed intelligence
- **What Is OSINT?**
  - OSINT is Open Source Intelligence, is the process of searching for, gathering, and analyzing data found from public sources
  - Data Is Just Data until Analyzed
- **The OSINT Cycle**
  - Requirements gathering
  - Retrieving data
  - Analyzing information: YOGA
  - Pivoting to a new perspective or Reporting analysis
- **Goals of OSINT Collection** — OSINT data enhances investigations

2. Diving into the Collecting Scenario

- Boss: We need you, OSINT man, to find the attacker that stole all our email.
- OSINT Man's boss shows him an email from the attacker whose name appears to be "R0s3buhd."
- Extract Data related to attacker from email as: name, email and domain.
- Search by attacker name in google and check social media.
- Cyber event postmortem: this occur after attack done and attacker leaked emails.

3. Taking Excellent Notes

- **Why we taking notes**
  - Document the work for the future
  - **Take Notes is important because Others may be using your work as a starting point as:**
    - Incident responders
    - Malware analysts
    - Law enforcement
    - Another OSINT analyst
- **Types of Documentation Tools**
  - **Visualizers**
    - Maltego
    - Gephi
    - i2 notebook.
  - **Note-taking Apps (manually)**
    - OneNote
    - Evernote
    - Google Keep
    - mindmap
  - **Documenting Apps** — Hunchly Google Chrome Extension
  - **Word Processors/Text Editor**
    - Notepad++
    - Sublime
    - vi/vim

4. Determining Your Threat Profile

- **Three main words to describe OSINT Process**
  - **Overt** — Public, non-anonymous
  - **Covert** — Low attribution, deniable, secretive
  - **Clandestine** — An operation sponsored or conducted by governmental
- **Check Browser Security**
  - eff.org
  - browserleaks.com
  - whoer.net
  - deviceinfo.me
- **Common Information Disclosure Issues Layers**
  - **Application Layer**
    - Being logged into a web site, service, or device with a personal or private account instead of an OSINT one.
    - Cookies, web bugs, and tracking content.
    - Spurious traffic from browser plug-ins/add-ons.
    - User agents from browsers and tools.
    - Check browser Security mention tools.
  - **Network Layer**
    - IPs: geographic location, network providers.
    - Using Tor: nodes are run by criminals and others by intelligence agencies.
  - **Google Tracking Searches**
    - How to use Google without being tracked 🔗
    - How Much Does Google Really Know About You? 🔗
    - - Removing Your Dat by ["Opt Out Doc"] project 🔗
  - **What Can We Do?/ How to secure your self?**
    - Understand our system and application network traffic.
    - Use proxies and Tor wisely.
    - Use appropriate search engines and web sites.
    - Clear cache, cookies, and history on our browsers.
    - Understand where our applications communicate and what they send.
    - Use appropriate OSINT user accounts for work requiring accessing authenticated resources.
    - Alter our applications so they provide inaccurate data to sites and network devices.
    - Create solid processes and follow them
  - **Hiding from the Internet: Michael Bazzell wrote a couple book**
    - Hiding From The Internet
    - Extreme Privacy

5. Setting Up an OSINT Platform

- **add in considerations when build OSINT**
  - Affordable: Cost
  - Trustworthy: uncompromising
  - Clean-able
  - Availability
  - Multi-User
  - Accessing
  - Graphical
  - Ease of update
- **VM** — Buscador 🔗
- **Browser Extension**
  - uBlock Origin
  - Firefox Multi-Account Containers
  - Location Guard
  - Hunchly Recording activity
  - Instant Data Scraper
  - User Agent Switcher
  - Download Everything
  - Search By Image
- **Recommendation**
  - Virtual Desktop Interfaces (VDIs)
  - Networking and Virtual Private Networks (VPNs)
  - Use Proxy
  - SmartPhone, use NOX
- **Data Storage**
  - Store notes, results, images, and other artifacts
  - Use Bitlocker in windows, LUKS in Linux.
- **Managing Those Passwords**
  - **Local file-based software** — KeePassXC 🔗
  - **Cloud-based managers** — 1Password 🔗

Practs

- **OSINTing People**
- **Mapping Minds and Cases**
- **Hunchly**
- **Searching for IP**
  - **Locate places that hold illegal files with SANS and GIAC intellectual property**
  - **Steps**
    - For this lab, you can and should use multiple search engines like https://google.com, https://duckduckgo.com, https://bing.com, and https://yandex.com.
    - Non-GIAC web sites that have pages like the following may house these files:
    - Dorks: sans filetype:pdf -site:sans.org -site:sans.edu -site:giac.org sec***
- **Managing Passwords - Optional**
- **Slacking It - Optional**

6. Effective Habits and Process

- **Getting Connected or Not: Do you connect to your target on social media**
- **Decide on TTPs**
  - Create an Standard Operation Procedure (SOP) with the TTPs used in various cases
  - Map TTPs out in advance to cover different paths
  - Michael Bazzell's web site has free flow charts that can be used to augment your processes
- **Flow charts for research on** — Email Addresses, Domains, Real Names and Usernames, Phones, Locations
- **Repeating the Process** — Collect data <-> Analyze data <-> Determine new collection goals

7. Leveraging Search Engines

- **Dorks: syntax for each search engine**
- **robots.txt**
- **DuckDuckGo.com**
  - Service 3g2upl4pq6kufc4m.onion
  - Privacy-focused search engine
  - Doesn't store searches, customize your content, or track your browser
- **Google's Trends tool**
- **Carrot** — Is an Open Source Search Results Clustering Engine.
- **Report**
  - The CIA's communications suffered a catastrophic compromise 🔗
  - 30 spies dead after Iran cracked CIA comms network with, er, Google search 🔗