Day4 Networks, Government, and Business

LinkedIn: @muhammed-dardir

6. Recon Tool Suites and Frameworks

SpiderFoot

Introduction
- OSINT automation tool
- Make collect data easy via module from various CTI platform.
- have 160+ module

SpiderFoot: Open Source vs HX
- SpiderFoot Open Source: single target, Local installation
- SpiderFoot HX: Mullite target, cloud

Data we can collect it
- **People**
  - Accounts   Checks account names across over 150 different web sites.
  - Social Networks "Identify presence on social media networks such as LinkedIn, Twitter and others."
  - Instagram and MySpace Gather information from those social media platforms
- **Domains/IPs**
  - Censys and Shodan Search the Censys.io and shodan.io web sites (require API keys)
  - Archive.org "Identifies historic versions of interesting files/pages from the Wayback Machine."
  - Whois "Perform a WHOIS look up on domain names and owned netblocks"

Configuration
- From setting add HTTP timeout of 5 seconds, Make User agent string

Scaning
- **Starting a SpiderFoot Scan**
  1. Enter scan name
  2. Enter seed target data as see487.info
  3. Choose the modules or "use case" you wish to use
  4. Click Run
  - As the scan runs, analysts can view the progress in the "Status" area.
  - The "Browse" button shows results discovered in a table format, Clicking the hyperlinks allows the analyst to see details
  - Use Proxy if you need to bypass Spiderfoot detection
- **Starting a SpiderFoot HX Scan**
  1. Choose profile or modules
  2. Enter scan name
  3. Enter seed target data
  4. Or import targets from a file
  5. Click "Run Scan Now"

Recon ng

Introduction
- Viewing the settings of how Recon ng works is performed at the global and module levels using the "options list" command
- Recon ng has internal SQLite database(s) it uses to store data it retrieves.
- To check All modules: marketplace search
  - marketplace install OR marketplace all.
- To see what a module does and other details of an installed module, load it and then get info: module load Netcraft

Starting a Recon ng Scan
- Create a new workspace: workspaces add case1
- Choose the module: modules load whois_pocs
- Enter seed target data: options set SOURCE faa.gov
- Run
- Show result: show TABLENAME

Recon ng OPSEC Gotchas
- In order to see which modules are used most, Recon ng uses Google Analytics at launch
- When run, the app will send information with your IP and modules you run from your system to Google
- You may not want this information disclosed
- recon ng no analytics

7. Government Data

Introduction
- GIS (Geographic Information System): GIS overlays layers of data on maps: gis site::gov.* filetype:pdf
- Open Data (or "OpenData") is simply that data that a government or organization shares without restrictions
- Variety of data in these systems, from terrorism databases to IP addresses and domains to people data

Open Data
- https://www.start.umd.edu/gtd/
- https://www.usa.gov/
- https://www.virginia.gov/
- https://www.norfolk.gov/

8. Researching Companies

When performing OSINT on a company, you will want to gather
- **Basic data (who, what, where)**
  - Who runs the company?, Who works at the company?, Who are the customers?, Who are the business partners?, Who are the suppliers?, Who are the people in the news?
  - Where are the company's offices/locations? (Gathering addresses, phone numbers, and emails for each office can be helpful), Where are they incorporated or registered?, Where do they do business?, Where are their internet facing computer systems?
  - What does the company "do"? (The primary and secondary functions of the company), What computer systems do they use and how? (Email, cloud, web, IM, billing), What are the important business relationships and ties to and from the company?
- Profiles and news of the company
- Formal/government business filings about the company
- Public reviews/perceptions
- What business systems are accessible the internet

Business Profile Sites
- **Buzzfile** is a business intelligence site showing data about companies and their leaders Some sites focus on the financial aspects of the company and others on more general information.
- **manta** site also aggregates data about US small businesses.
- **opencorporates** As the largest open database of companies in the world, our business is making high quality, official company data openly available
- **Nonprofit Research**
  - charitynavigator.org
  - guidestar.org (USA)
  - projects.propublica.org (USA)
  - gov.uk/find charity information (UK)
- **Business Filings (EDGAR)** AnnualReports.com
- **Infobel** Companies or people can be searched by name or category, Shows phone numbers, addresses, and map when details are requested
- **Databases for journalists (and OSINTers!) to search: https://id.occrp.org/databases/.**
- **Gov.uk** Companies House
- **Corporation Wiki** provide Relationship Map, Companies and Connections Tables, Known Addresses and Sources.
- **LittleSis.org** Another site dedicated to publishing data in support of factual journalism is LittleSis.org
- **Salary.com** Many executive salaries and compensation packages need to be reported in regulatory documents

Check Everyone on the internet has an opinion, and many will be happy to share theirs with you
- Careerbliss.com
- Comparably.com
- Glassdoor.com
- Indeed.com

1. Whois

Introduction
- When domain names are recorded with ICANN, data about who is registering it is submitted
- Web GUI 🔗
- CLI

Whois and GDPR
- When GDPR began to be enforced in May 2018, most of the whois systems in the world began filtering their content
- Who is less useful now.
- Even though we cannot see some data in the whois systems, we can search for people, phone numbers, and emails by this site viewdns.info we can search by name if this name register any domain or not.

Whois and Organizations
- What if we used the whois system to find information about people at an organization?
- By using Reverse Whois by perform search in whois with '*@org_Name.com': viewdns.info.

Going Directly to the Source ARIN
- IP Address Block 🔗
- First and/or Last Names — Search by first and last name to get registered mail for org
- Name of Org 🔗
- Name of the Domain of the POCs 🔗
- DNS Resolver 🔗
- Whoxy 🔗
- domain big data 🔗
- We Can Retrieve JSON via the Command Line — curl H "Accept: application/json" "http://whois.arin.net/rest/pocs;domain=dhs.gov" | json_pp

SpiderFoot ARIN Module Enable the following modules (at least): pass domain and get, Steve Micallef wrote a module for SpiderFoot to access the ARIN API and retrieve data.
- ARIN
- DNS resolver
- Emails
- Name Extractor

2. IP Addresses

Web App
- Webupdates (RIPE) 🔗
- APNIC 🔗
- he.net 🔗

How to Find Geolocation from IP Address
- www.whatismyipaddress.com
- www.infosniper.net
- www.ip2location.com
- IPs Aren't Always Where You Think

3. DNS

From the command line
- nslookup
- Resolve DnsName (PowerShell)
- dig
- host

web applications
- Robtex.com
- ViewDNS.info
- dnsdumpster.com

Common DNS Subdomain Enumeration Methods
- Dictionary "Attack"
- Zone Transfer
- Reverse or PTR Lookup

Tools
- DNSRecon
- Aquatone: take screenshot
- Typosquatting: dnstwist "tool to create squatting domain"
- Sublist3r
- web app (Intelx.io)

Cyber Threat Intel and OSINT Pulsedive 🔗 — aggregates data about IP addresses, domain names, malware, and IOCs

4. Findings Online Devices
- https://www.shodan.io
- https://censys.io

5. Wireless Networks

Wireless Wi Fi Primer
- SSID: SSID Service Set Identifier. This is the name of the wireless network. Ex: ThePrincessBride
- BSSID: BSSID Basic Service Set Identifier. Unique ID of a wireless transmitter in MAC address format. Ex: 00:20:91:a1:33:11
- beacon: Announcements from access points broadcasting SSIDs. Ties SSID to BSSID (access point).
- probe requests: Announcement from client requesting a certain SSID. Ties request for SSID to a BSSID (client).
- We have RFID, Bluetooth, Zigbee, cellular, and NFC transmitters in our devices

WarXing — Used to record geolocation by wireless

WiGLE.net — web site allows us to search for submitted geolocated Wi Fi networks

Wireless and OSINT Scenarios
1. Stationary location Wi Fi AP
2. Stationary location with different networks over time
3. Hotspot phone or MiFi device
4. Same BSSID in multiple places

DFIR Android Mobile Device Geolocation
- Mobile data from cell towers and Wi Fi networks can help geolocate devices.
- In DFIR, mobile device data is extracted using software like Cellebrite