Intelligence Collection

Cybersecurity Student Association

News Update

- Aruba AP's hit with 4 critical buffer overflow vulnerabilities (9.8/10)
  - Look up!
- CUPS Vulnerability allows for remote execution of Linux code
  - Requires users to initiate a print job.
- Largest Water Utility in the U.S. hacked
  - Affected billing functions (is that so wrong)
- Internet Archive hacked (again)
- Iran physically attacks Israel, suspected cyber-attacks follow
  - Allegedly leaking information on Israeli officials

Open-Source Intelligence (OSINT)

What it is: Gathering and analyzing public data for intelligence purposes

Importance: Most common way to gather intelligence on a target.

Collection Methods: Media reports, books, social media, arrest records, court filings, public census information

Tools & Resources: https://github.com/giuliacassara/awesome-social-engineering

https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/human-intelligence-humint/

OSINT Continued

- 3 cores to OSINT
  - Learning what information is available
    - DNS Information, Job information, Technology stacks, Personal information
  - How the information is available
    - OSINT Framework, Google, Wayback Machine, DNS Dumpster
  - How it can be leveraged – Why OSINT is so crucial
    - social engineering pretext, pentesting vectors, and general problem solving.
- You should not focus on collecting as much data as possible, but instead make specific decisions for data collection

Human Intelligence (HUMINT)

What it is: Gathering information directly from people.

Importance: Provides insights that are not available through technical means.

Collection Methods: Interviews, observations, covert operations.

Tools & Resources: https://github.com/giuliacassara/awesome-social-engineering

https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/human-intelligence-humint/

Signals Intelligence (SIGINT)

What it is: Collecting data from intercepted communications and electronic signals.

Importance: Helps in understanding and intercepting potential threats.

Collection Methods: Interception of communications (COMINT), electronic signals (ELINT).

Tools & Resources:
https://github.com/GreyS3c/SIGINT-SAK
https://github.com/arall/sigint

https://isecjobs.com/insights/sigint-explained/

Cyber Intelligence (CYBINT)

What it is: Data collected from cyber activities.

Importance: Critical for identifying and mitigating cyber threats.

Collection Methods: Network traffic analysis, malware analysis, threat data feeds.

Tools & Resources: https://github.com/okhosting/awesome-cyber-security

https://www.fortinet.com/resources/cyberglossary/cyber-threat-intelligence

Combining Multiple Sources

Triangulation

- Cross-reference, consistency check

Analyze information

- How it changes over time, relationships between information, relationships between people and organizations.

Fuse Data into one unified dataset

- Easier to analyze and action on

OSINT Collection Methods

Search engines and social media

- Social-analyzer
- Google Dorking

Public Records and Databases

- Voter Registration, Genealogy tools (MyHeritage, Ancestry, Family Search)
- Phone Books
- https://www.shodan.io/
- https://ipinfo.io/
- https://scamalytics.com/

News Sources

OSINT Tools

- Maltego, theHarvester, recon-ng, WIGLE
- https://github.com/jivoi/awesome-osint
- https://github.com/Jieyab89/OSINT-Cheat-sheet

Google Dorking

Uses advanced search methods to find information on Google

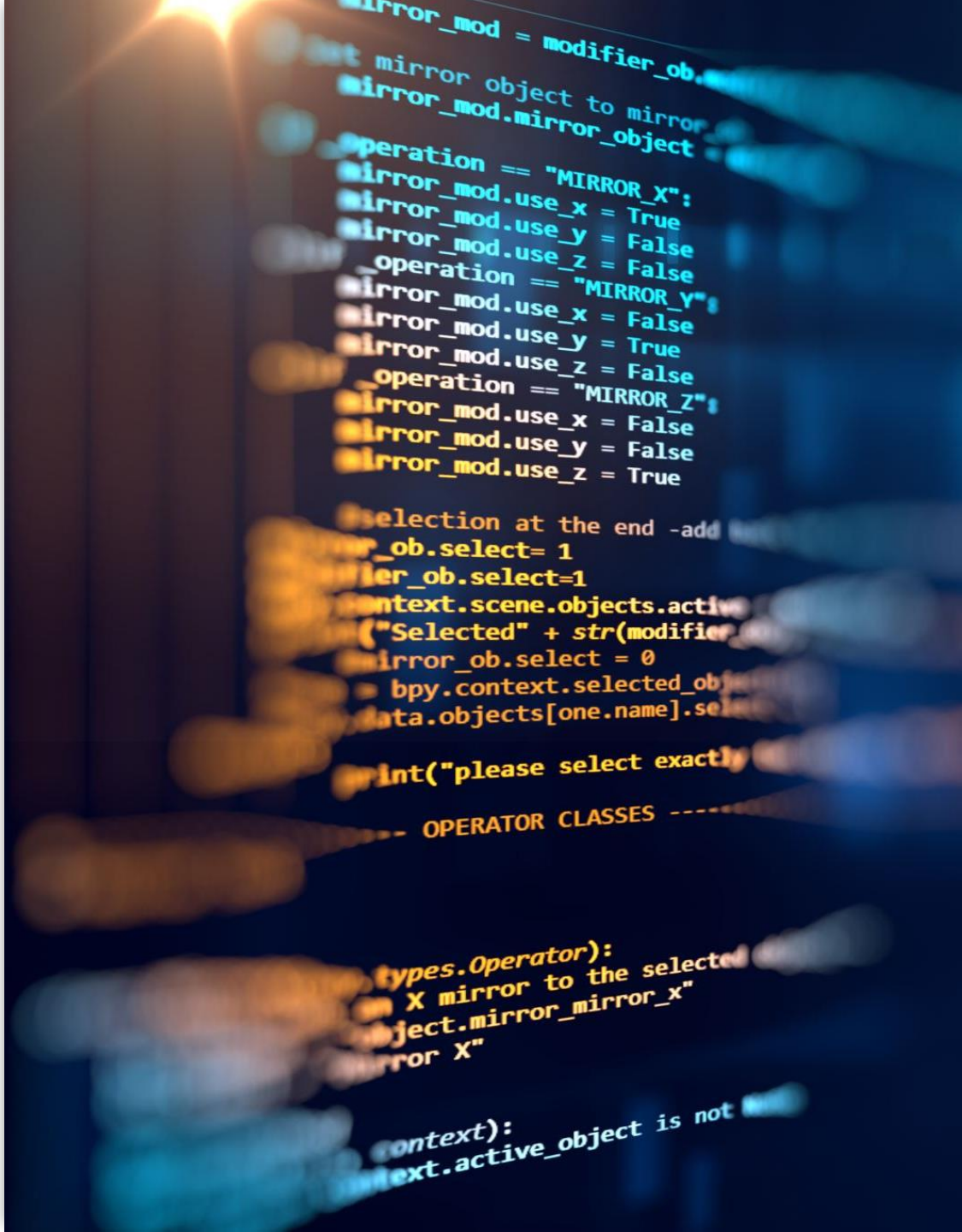
Information typically isn't available in standard searches

Advanced search operators refine searches

What kind of intelligence gathering is this?

Basic Operators

- Filetype: filetype:pdf
- Inurl: inurl:login
- Intext: intext:”password”
- Intitle: intitle:”index of”
- Link: link:example.com
  - Finds pages linking to example.com
- Site: site:example.com
  - Searches within a site



Hands on time! (Links in Slack)

Access login.salesforce

Look for PDFs of Nasa.gov

- Find one called “How far can you See?”

Find a file directory of byu.edu

- Hint: “index of”

Find the phpinfo.php for any website

Find ANY webcam online (bonus points depending on how far away from the US it is)

- Hint: index.shtml

Find the 2015 Lethal Injection Procedures for the state of Tennessee

Shodan Introduction

What is Shodan?

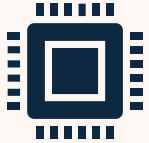
Shodan is a search engine for internet-connected devices.

Unlike traditional search engines that index web pages, Shodan indexes information about devices connected to the internet.

Importance

Shodan helps identify vulnerable systems and devices.

It is widely used by cybersecurity professionals to assess the security of networks and devices.



How it Works

Shodan scans the internet for devices and collects information such as IP addresses, open ports, and services running on those ports.

The data is then indexed and made searchable.

Use Cases

Network security assessments

Identifying exposed devices

Researching the Internet of Things (IoT) security

Shodan Key Features

- **Search Filters:** Shodan offers a variety of search filters that help users pinpoint specific devices, services, or vulnerabilities. This includes filtering by device type, operating system, country, port, etc.
- **Banner Information:** Shodan collects "banner" information from devices, including details like the software version, operating system, open ports, and other metadata. This information can help identify potential vulnerabilities.
- **Exploit Finder:** Shodan can help identify systems running software versions known to have vulnerabilities. This can be extremely valuable in preventing security breaches.
- **Network Mapping:** With Shodan, you can identify all internet-facing assets associated with a specific IP or company. This can be crucial in understanding the full extent of an organization's potential attack surface.
- **Internet of Things (IoT) Device Discovery:** Shodan is particularly useful for discovering Internet of Things (IoT) devices. Since many IoT devices are not securely configured by default, Shodan can help identify these potential security risks.

Shodan Tutorial

Account Creation: register with student email to get premium account

Premium Account: Maps, Images, and **vuln** filter access

Explore Section

Shodan Basic Search Examples

apache	This search will return servers running Apache software.
Microsoft-IIS/7.5	This will return servers running version 7.5 of Microsoft's Internet Information Services web server software.
nginx	This will return servers running Nginx, a popular open-source web server.
cisco-ios	This will return devices running Cisco's IOS operating system, often used in networking hardware like routers and switches.
default password	This might show devices or services where default passwords are still used.

Shodan Filters

ip:	Filters results by a specific IP address. Ex: ip:192.168.2.1
asn:	Filters results by a specific ASN (Autonomous System Number) ID. Ex: asn:AS8160
hostname:	Filters results by a specific hostname or find values that match the hostname. Ex: hostname:google.com
port:	Filters results by a specific port number of a service or find particular ports that are open. Ex: port:21
net:	Filters results from a specified CIDR (Classless Inter-Domain Routing) block. Ex: net:192.0.2.0/24
isp:	Filters results by devices assigned a particular address (space) from a specified ISP (Internet Service Provider). Ex: isp:Bell
city:	Filters results by a specific city or find devices in a particular city. Ex: city:Vancouver
country:	Filters results by a specific two-digit country code or find devices in a particular country. Ex: country:CA
os:	Filters results by a particular operating system or search based on the operating system. Ex: os:Linux
product:	Filters results by a particular software or product identified in the banner. Ex: product:Apache
version:	Filters results by a specified software version. Ex: version:2.2.5
geo:	Search for specific GPS coordinates. Ex: geo:42.3601,-71.0589 (command line only)
before/after:	Find results within a specific timeframe. Ex: after:2022-01-01 (command line only)

Shodan Challenges

1. Find an Nginx Server running version 1.14.0
2. Find a device that is running Apache on port 80 on a Linux OS in the US
3. Find a device that is AirPlay-enabled on port 5353, and is associated with the University of Utah
4. Find a device that has port 445 open, does not require authentication, is located in Canada, and contains the term "Documents"
5. Find a Minecraft Survival server running on port 25565 in Spain
6. Find a device in Provo running services on port 4443 that are vulnerable to a command injection issue in the `c_rehash` script of OpenSSL (vulnerability)

Shodan Resources

- https://github.com/jakejarvis/awesome-shodan-queries
- https://www.shodan.io/search/examples
- https://www.shodan.io/search/filters
- https://upskilld.com/learn/shodan-query-syntax-and-filters/