CONTINUES .....

✅13. Advance Online Utilities >> **https://centralops.net/co/**

✅14. Protocol analyzer (**wireshark**) >> **https://www.wireshark.org/**

✅15. DNS related tools >> **https://viewdns.info/**

✅16. OSINT Framework >> **https://lnkd.in/gXaz_Wry**

✅17. Malfrat's OSINT >> **https://lnkd.in/e4nhK2hK**

✅18. OpenAI >> **https://lnkd.in/gjq7tcMG**

✅19. Find Emails (**hunter**) >> **https://hunter.io/**

✅20. Find People (**check usernames**) >> **https://lnkd.in/g4bcUH_b**

✅21. Secure **Password**? >> **https://lnkd.in/gbRCEmRW**

✅22. Internet Archieve >> **https://archive.org/web/**

✅23. Reverse Image search >> **https://tineye.com**

✅24. Link and data mining >>**https://lnkd.in/gf9BUFWk**

CONTINUES .....

✅25. Data breaches (**pwned**) >> **https://lnkd.in/gvbzhceV**

✅26. Search Engine for IoTs (**shodan**) >> **https://www.shodan.io/**

✅27. Cyberspace Search >> **https://www.zoomeye.org/**

✅28. Search Engine >> **https://search.censys.io/**

✅29. Website Profiler Tool >>**https://builtwith.com/**

✅30. Malware Samples and IoCs >> **https://abuse.ch/**

✅31. **WhatsMyName** >> **https://whatsmyname.app/**

✅32. Email Info >>**https://epieos.com/**

✅33. File Search engine >> **https://filepursuit.com/**

✅34. Domain investigation >> **https://lnkd.in/e2c27zc7**

✅35. CyberGordon >> **https://cybergordon.com/**

✅35. **IP Check** >> https://centralops.net/co/

ADVANCED SEARCH OPERATORS:

Google's advanced operators are essential for precise results:

site:: Search within a specific website or domain (e.g., site:wikipedia.org AI).

inurl:: Locate URLs with a specific keyword in the URL (e.g., inurl:pdf confidential).

filetype:: Find files of a particular type (e.g., filetype:pdf security guidelines).

VirusTotal

VirusTotal is a free online service that provides a comprehensive and powerful tool for scanning files and URLs to detect and analyze potential threats, such as viruses, malware, Trojans, and other malicious content.

VIRUSTOTAL HASHES

Lookup this SHA-256 hash on virus total

b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d

https://www.virustotal.com/gui/home/upload

SHODAN - THE SEARCH ENGINE FOR THE INTERNET OF THINGS

Shodan:

Shodan is a specialized search engine designed for the Internet of Things (IoT).

It scans the internet for connected devices, including webcams, routers, and industrial systems.

Capabilities:

Shodan can reveal open ports, vulnerabilities, and even the physical locations of connected devices.

THE WAYBACK MACHINE - TIME TRAVEL FOR THE WEB

The Wayback Machine:

The Wayback Machine is an internet archive that stores historical snapshots of websites over time.

ZOOMEYE

Zoomeye is an open-source search engine designed for scanning the internet to identify exposed devices and services.

It plays a crucial role in open-source intelligence (OSINT) and cybersecurity research.

KEY FEATURES

Device Identification: Zoomeye helps discover a wide range of devices, including webcams, routers, and servers.

Service Identification: It identifies specific services running on those devices, exposing potential vulnerabilities.

Geolocation: Determine the approximate physical location of devices.

Real-time Data: Zoomeye provides continuously updated information.

Advanced Search Queries: Create tailored search queries to refine results based on criteria like device type, location, and open ports.

RESPONSIBILITIES OF A CTI

- Collect up-to-date and accurate data from the dark web, intelligence feeds, intelligence sources, etc.
- Analyze the collected data and understand the technical aspect of security
- Identify business risks then disseminated to business executives
- Identify, monitor, assess, and defend against various attacks performed by threat actors
- Stay ahead of adversary by understanding latest attack TTPs
- Extract threat intelligence that includes contextual information, IoCs, TTPs, consequences, and

  actionable intelligence about evolving threats
- Understand the motive of the adversaries by analyzing the characteristics and habits of threat actors
- Guide organizations in building effective defense and mitigation strategies
- Collaborate with IT, incident handling, and SOC teams by generating timely threat reports

TYPES OF CTI

INTELLIGENCE AREAS

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cybersecurity systems.

STAKEHOLDERS:
- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:
- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

"Race Car Driver"

STRATEGIC

Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

"The Owner"

KEY IOC'S

1. Unusual Outbound Network Traffic
2. Unusual Activity through Privileged User Account
3. Geographical Anomalies
4. Multiple Login Failures
5. Increase in Database Read Volume
6. Large HTML Response Size
7. Multiple Requests for the Same File
8. Mismatched Port-Application Traffic
9. Suspicious Registry or System File Changes
10. Unusual DNS Requests
11. Unexpected Patching of Systems
12. Signs of DDoS Activity
13. Bundles of Data in Wrong Places
14. Web Traffic with Superhuman Behavior

OSINT FRAMEWORK

https://osintframework.com/

ASSIGNMENT

Watch the following CyberChef video and Identify 3 things learnt from that videos.

https://www.youtube.com/watch?v=pJvQgUk01k4&t=616s