Assignment 1- 10 Public database & tools for

OSINT and their usage-

What are Public Database in OSINT?

Ans: Public databases for OSINT represent meticulously organized collections of publicly accessible information that can be systematically searched and analyzed to bolster cybersecurity operations. They offer profound insights into an organization's digital footprint, revealing potential vulnerabilities or attack vectors that could be exploited.

How are they used in OSINT-

Reconnaissance	To map out an organization's digital assets, such as domain names, IP addresses and web technologies
Vulnerability Assessment	To identify outdated software, misconfigured systems, or open ports that could be exploited
Threat Intelligence	To track threat actors, monitor leaked data, and understand attack surfaces.

Incident Response	To gather evidence and understand the scope of a cyberattack by analyzing exposed data.

10 Public Database &Tools Examples in OSINT Cybersecurity

1. WHOIS Database: Provides registration details for domain names, including registrant information, nameservers, and registration dates

2. Shodan: A search engine for internet-connected devices, revealing open ports, services, and potential vulnerabilities on exposed IoT devices and other systems.

3. Censys: Offers detailed data and search capabilities for internet-facing systems, providing information on protocols, configurations, and associated vulnerabilities.

4. Builwith: A database that tracks the technologies, content management systems (CMS), web servers, and plugins used by websites, helping to identify potential vulnerabilities**.**

5. Maltego: An OSINT tool that aggregates data from various public databases to visually map relationships between entities like domains, IP addresses, people, and infrastructure.

6. Intelligence X: A search engine that includes leaked data, dark web content, and WHOIS records, providing access to historical information that may no longer be publicly visible

7. theHarvester: Gathers information like emails, subdomains, virtual hosts, and employee names from public sources like search engines and DNS servers.

8. Google Dorking: Not a database itself, but a technique to query

Google using advanced operators to uncover hidden content, misconfigurations, and sensitive documents that may reside in public databases or websites.

9. Public Domain Registries: Such as ICANN's WHOIS database, which are fundamental for domain and IP address registration and management.

10. Public Trading Data: Websites and databases that provide public information about publicly traded companies, which can be used to gain insights into organizational structure and financial information relevant to threat actors.