Viva Questions

Define osnit :

"Open Source Intelligence (OSINT) is information that is legally gathered from public sources. This information can be used to provide actionable insights for decision-makers."

OSINT can come from:

- Public online sources
- Offline resources
- Books, magazines, and newspapers
- Public government data, reports, budgets, hearings, telephone directories, press conferences, websites, and speeches

OSINT is a process that involves: Identifying data, Harvesting data, Processing data, Analyzing data, Reporting data.

OSINT can be used by:

- Security experts
- National intelligence agencies
- Cybercriminals

OSINT can be used to:

- Understand what information you are giving to potential attackers
- Passively acquire intelligence without alerting the target.

key benefits of OSINT include:

Cost-Effective: OSINT typically relies on publicly accessible data and open-source tools, making it a cost-effective method of information gathering compared to other intelligence-gathering methods.

Widespread Data Sources: OSINT draws information from a broad range of publicly available sources, including the internet, social media, government records, academic publications, news sources, and more.

Timeliness: OSINT allows for real-time or near-real-time data collection, making it suitable for monitoring and staying up-to-date on events, trends, or emerging threats.

Versatility: OSINT can be applied to various domains, including national security, law enforcement, corporate intelligence, competitive analysis, cybersecurity, and journalism.

Enhanced Decision-Making: The data gathered through OSINT can help organizations and individuals make informed decisions, assess risks, and identify opportunities.

Security and Threat Analysis: OSINT plays a crucial role in threat intelligence and security assessments, helping organizations detect and mitigate potential risks and vulnerabilities.

Competitive Intelligence: In the business world, OSINT can be used to gather information about competitors, market trends, consumer sentiment, and emerging technologies.

Investigative Tools: OSINT aids in investigations by providing background information on individuals, organizations, or events, helping law enforcement and private investigators.

Reputation Management: Businesses and individuals can use OSINT to monitor their online reputation and respond to potential issues or threats.

Research and Analysis: OSINT supports academic research and analysis by providing access to a vast pool of publicly available data.

Online threats

Online threats are cybersecurity risks that can cause undesirable events or actions via the internet. They can be made possible by:

- End-user vulnerabilities
- Web service developers/operators
- Web services themselves

Some examples of online threats include:

- Trojan horse
- Worms
- Viruses
- Spyware
- Phishing

OSINT Type

- Web-Based OSINT:
- Government and Public Records:
- Academic and Research Sources:
- Human Intelligence (HUMINT):

Search Techniques

- Broad and narrow searches.
- Search blocks.
- Combining search words with Boolean operators (AND, OR and NOT)
- Searching for part of words (truncation)
- Searching for phrases (quotation marks)
- Simple and advanced search forms.
- Improving your search

Metasearch

A metasearch engine (or search aggregator) is an online information retrieval tool that uses the data of a web search engine to produce its own results.

Automated Online Search Tool is an application that can be configured to automatically gather information from a specified number of Internet-based sources. Examples include Google Alerts, Yotify, Alerts.com, Twitter, and WatchThatPage.

NEWS SERACH

News search is the process of using search engines or specialized news search engines to find current news articles, reports, and information on specific topics or events. News search is a valuable tool for staying informed about the latest developments, trends, and events across various domains.

OSINT techniques include:

- Search engines, such as Google, Bing, and Yahoo
- Passive collection, which involves scraping publicly available websites, retrieving data from open APIs, or pulling data from deep web information sources

OSINT can be useful for:

- Searching global news for situational awareness
- Debunking fake news

Some OSINT tools include:

- Search engines, such as Google, Bing, and Yahoo
- Open APIs, such as the Twitter API
- VPN services, such as NordVPN and Private Internet Access.

Harvester

The Harvester is a tool that can be used by penetration testers to gather information from public sources. It's pre-installed in Kali Linux.

The Harvester uses public sources like:

- Search engines
- PGP key servers
- SHODAN computer database

The Harvester can gather information like:

Emails, Subdomains, Hosts, Employee names, Open ports, Banners.

The Harvester is a command-line tool that acts as a wrapper for search engines. It's intended to help penetration testers in the early stages of a penetration test.

Reverse image

Reverse image analysis, also known as reverse image search, is a technique used to find information about an image by searching for it based on the image's content rather than text-based queries.

TinEye

Open Source Intelligence (OSINT) tools can assist in identifying and verifying the authenticity of news and information.

FAKE NEWS DEECTION TOOL:

1. **Google Reverse Image Search**: Verify the authenticity of images used in news stories by performing a reverse image search on Google Images. This can help you determine if an image has been used in a misleading or unrelated context.

2. **TinEye**: TinEye is a dedicated reverse image search tool that can help you find the original sources of images or track their usage across the internet.

3. **Fact-Checking Websites**: Websites like Snopes, FactCheck.org, and PolitiFact are dedicated to fact-checking news stories and debunking false claims.

Analyzing a digital footprint using OSINT (Open Source Intelligence) tools involves the systematic collection of publicly available information about an individual, organization, or entity from various online sources

Semrush the best tool?

It ranked as one of Forbes Advisor's best SEO software. In addition to its comprehensive keyword research tool, it also offers a wide range of SEO-related tools such as rank tracking, website monetization, competitor SEO analysis, content optimization, social media management, local SEO and more.

What is geolocation tracking?

Geolocation refers to the identification of the geographic location of a user or computing device via a variety of data collection mechanisms.

Geolocation is **the process of using technology to identify the location of an object or person**. It can be used to track the movements and location of people, and for surveillance.

Geolocation uses various methods, including:

- GPS
- IP addresses
- Wi-Fi positioning

Footprinting is **an ethical hacking technique that involves gathering information about a targeted computer system, infrastructure, and networks**. The goal of footprinting is to identify opportunities to penetrate the system and find vulnerabilities.