

Experiment No. 6

Title: Conducting recon with OSINT



Batch:A3**Roll No.:16010421119****Experiment****No.:6 Aim:** Conducting recon with OSINT tools.

Resources needed: OSINT Framework, Maltego, The OSINT Curious Project, Shodan, SpiderFoot, theHarvester, Recon-ng, Websites like public records databases, business registries, and government databases

Pre Lab/ Prior Concepts:

Students should know the Definition of OSINT, Legal and Ethical Considerations, Scope and Objectives, Public vs. Private Information, Tool Familiarity, Target Profiling, Understanding Search Operators, and Social Engineering Awareness.

Theory:

Open Source Intelligence (OSINT) is a critical facet of cybersecurity that involves collecting and analyzing publicly available information to gain insights into the online presence of individuals, organizations, or entities. Conducting reconnaissance with OSINT tools is a strategic process that unveils digital footprints, providing valuable data for threat intelligence, security assessments, and investigations.

Understanding OSINT: OSINT leverages publicly accessible information from social media, online forums, public records, and other openly available platforms. The key objective is to aggregate and analyze data to create a comprehensive profile of the target.

Legal and Ethical Considerations: Responsible conduct is paramount when engaging in OSINT activities. Practitioners must operate within legal boundaries and adhere to ethical standards, respecting privacy and avoiding any activities that might violate laws or infringe on individuals' rights.

Scope and Objectives: Defining the scope and objectives of OSINT activities is crucial. Whether it's gathering information about a potential threat, assessing the security posture of an organization, or investigating a specific incident, clear goals guide the reconnaissance process and ensure that efforts are focused and purposeful.

Tools of the Trade: Various OSINT tools facilitate the collection and analysis of information. Tools like Maltego, Shodan, theHarvester, and SpiderFoot automate data gathering, helping analysts visualize relationships between different data points and uncover hidden connections.

Information Validation: One of the critical aspects of OSINT is validating the obtained information. Analysts must employ techniques to verify the data's accuracy, relevance, and timeliness. Validation ensures that decisions based on OSINT findings are sound and reliable.

Target Profiling: OSINT enables the creation of detailed profiles of targets. Whether it's an individual, a company, or a threat actor, profiling involves collecting data about online activities, affiliations, interests, and potential vulnerabilities. This information aids in risk assessment and strategic decision-making.

Procedure:**Procedure for Conducting Reconnaissance with OSINT Tools**

Conducting reconnaissance with Open Source Intelligence (OSINT) tools involves systematically gathering and analyzing publicly available information to uncover digital insights. Here's a step-by-step procedure for conducting OSINT reconnaissance:

Step 1: Define Scope and Objectives: Clearly define the scope and objectives of OSINT activities. Determine the specific information to seek and the goals of reconnaissance. Whether it's profiling an individual, assessing an organization's online presence, or gathering threat intelligence, a well-defined scope guides the process.

Step 2: Identify Target: Identify the target for reconnaissance. This could be an individual, an organization, or a specific topic of interest. Understanding the target helps tailor OSINT efforts to gather relevant information.

Step 3: Select OSINT Tools: Choose appropriate OSINT tools based on the nature of target and objectives. Common OSINT tools include:

- Maltego: For visualizing relationships between different data points.
- Shodan: To search for internet-connected devices.
- theHarvester: For email and domain information gathering.
- SpiderFoot: An OSINT automation tool for comprehensive data collection.

Step 4: Craft Search Queries: Create specific search queries or tasks based on the information gathered and the chosen OSINT tools. Craft queries that leverage the functionalities of the selected tools to obtain relevant results.

Step 5: Execute OSINT Tools: Execute the chosen OSINT tools and queries to collect information. Use tools to search for data across various sources, including social media platforms, online forums, public records, and websites.

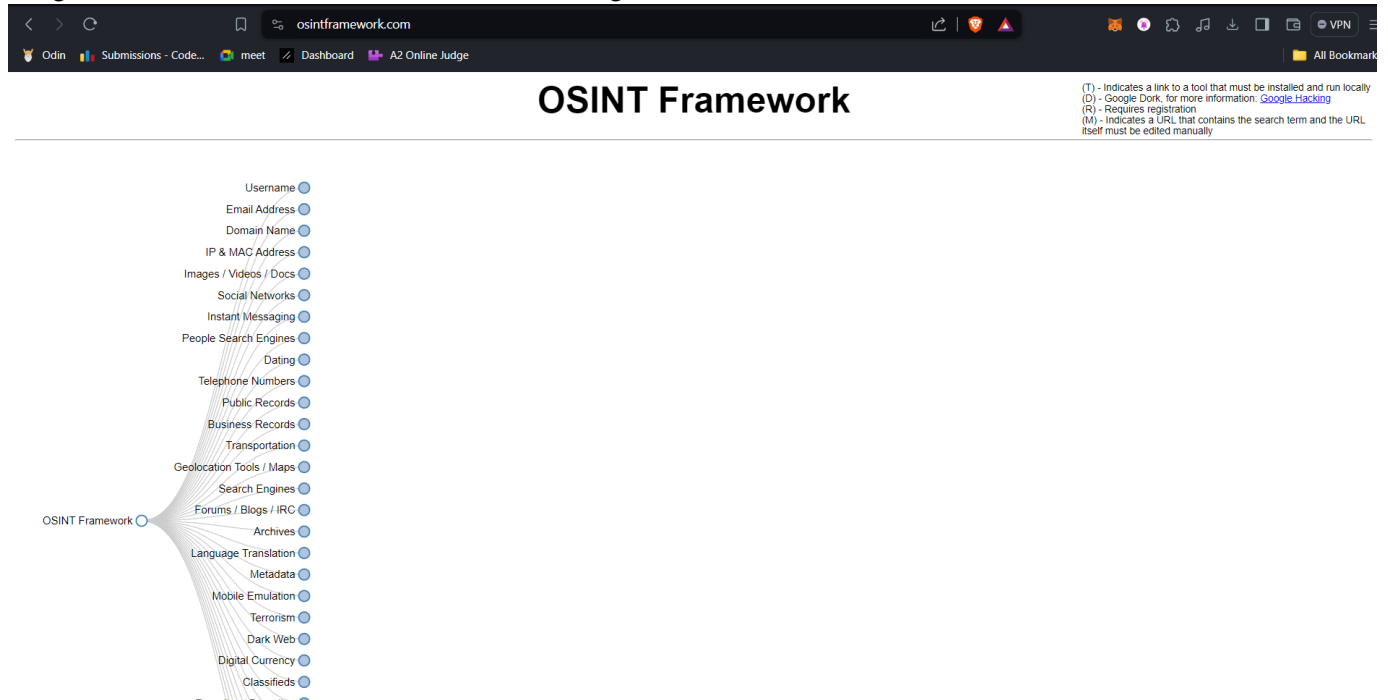
Step 6: Validate Information: Validate the collected information's accuracy, relevance, and timeliness. Cross-reference data obtained from different sources to ensure consistency and reliability. Validation is crucial to avoid relying on misinformation.

Step 7: Analyze and Correlate Data: Analyze the gathered data for meaningful insights. Correlate different data points to create a comprehensive profile of the target. Look for patterns, connections, and potential areas of interest.

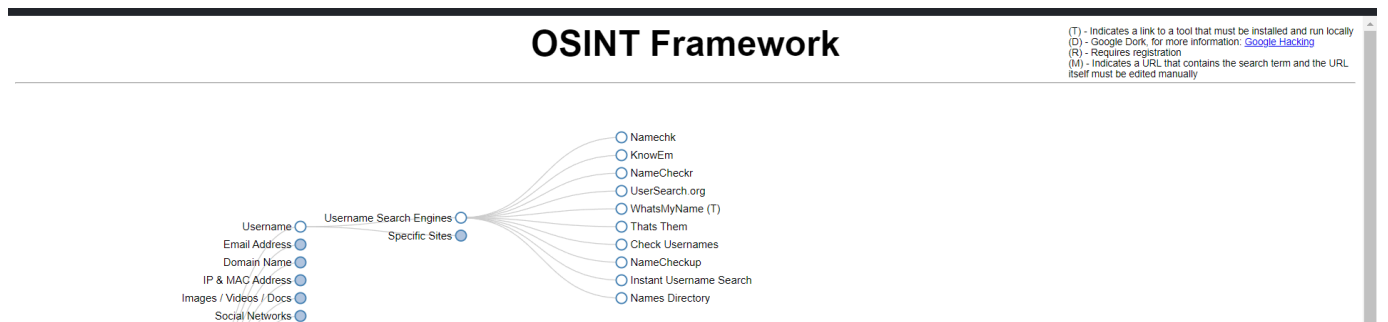
Output (Code with result Snapshot)

We will conduct recon on myself Arya Nair

We go to osint framework and find toolss which might be useful to us



then we look at the tools available for Username search



we try to use Namechek to find wether this user has any particular website

The screenshot shows the Namechk website. The header includes the Namechk logo and navigation links: Domain Names, Web Hosting, Website Builders, and Name Generators. The main search area has a text input field containing "Arya-Nair" and a search button. Below the search bar is a reCAPTCHA widget with the text "I'm not a robot". Below the search results, there is a section titled "Domains" which displays a grid of domain names for sale. Each domain name is followed by a green "BUY" button.

Arya-Nair.com	BUY	Arya-Nair.net	BUY	Arya-Nair.me	BUY
Arya-Nair.org	BUY	Arya-Nair.us	BUY	Arya-Nair.info	BUY
Arya-Nair.la	BUY	Arya-Nair.asia	BUY	Arya-Nair.biz	BUY
Arya-Nair.tv	BUY	Arya-Nair.ws	BUY	Arya-Nair.nyc	BUY

we look at all the websites that our registered and check whether we get our target person, as you can see we found the target of this particular user

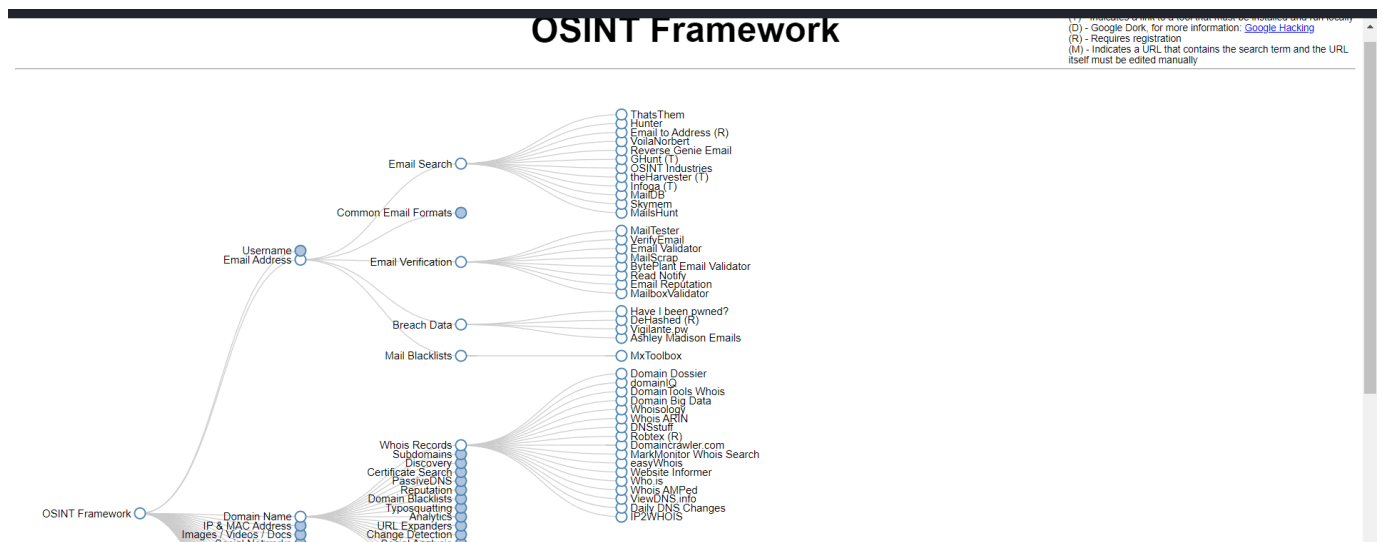
Arya-Nair.gs	BUY	Arya-Nair.net.nz	BUY	Arya-Nair.org.nz	BUY
Arya-Nair.com.mx	BUY	Arya-Nair.com.tw	BUY	Arya-Nair.org.tw	REGISTERED
Arya-Nair.idv.tw	BUY	Arya-Nair.in	REGISTERED	Arya-Nair.co.in	BUY
Arya-Nair.net.in	BUY	Arya-Nair.org.in	BUY	Arya-Nair.firm.in	BUY
Arya-Nair.gen.in	BUY	Arya-Nair.ind.in	BUY	Arya-Nair.me.uk	BUY

after opening arya-nair.in we browse through the website and try to find relevant information



in this case we found the whatsapp number as well the email address of this user

then we would look into various osint tools for email address




We use Have i been pwned to check whether the user data has been breached somewhere or not

we see the breaches of the companies


Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.




Domino's India: In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases




Dubsplash: In December 2018, the video messaging service Dubsplash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken languages, Usernames



MemeChat: In mid-2022, "the ultimate hub of memes" MemeChat suffered a data breach that exposed 7.4M records. Alleged to be due to a misconfigured Elasticsearch instance, the data contained 4.3M unique email addresses alongside usernames.

Compromised data: Email addresses, Usernames



Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by [dehashed.com](#).

Compromised data: Email addresses, Names, Passwords

Hence by using OSINT tools we get the breaches where the user details may have been leaked as well as the user email and phone number

Post Lab Questions: -

1. Evaluate the effectiveness of the OSINT tools used in the reconnaissance. Which tools proved most valuable, and how did they contribute to achieving the defined objectives?

I used have I been pawned and namecheck which allowed my to find the required information of the particular user. Both the tools were very helpful and helped me achieve my goal

2. Assess your documentation practices. What information did you include in your records, and I included all the necessary information to replicate the same actions so the users can find the exact same information when they try on their own

Outcomes: CO2 Comprehend purpose of Anonymity and Foot printing

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Successfully used OSINT tools to find details about a particular user that we wanted to find

Signature of faculty in charge with date

References:

1. <https://securitytrails.com/blog/osint-tools>
2. <https://www.codecademy.com/article/passive-active-reconnaissance>
3. <https://www.csnp.org/post/using-osint-reconnaissance-to-protect-your-organization>

