Course Code	Course Name	Theory	Practical	Tutorial	Theory	Practical /Oral	Tutorial	Total
IoTCSBCL704	Open-Source Intelligence (OSINT) Lab	--	02	--	--	1	--	01

Course Code	Course Name	Theory Marks				Term Work	Practical/Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
IoTCSBCL704	Open-Source Intelligence (OSINT) Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
The course aims:	
1	To provide hands-on experiences for students to develop critical thinking, research skills
2	To incorporate ethical usage of OSINT tools.
3	To get familiar with OSINT framework and its usage on publicly available data.
4	To learn to use the OSINT tools for Social Media, Email, Image, or network analysis, websites and understand the usage for Digital Forensics .
5	To performs background/profile/corporate profile checks, corporate Open-Source Intelligence (OSINT) Assessment etc.
6	Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Gain knowledge about Open-Source Intelligence understand the threats and think critically about countermeasures.	L1, L2, L3
2	Conduct advanced searches to gather intelligence and apply advance OSINT search techniques and tools.	L1, L2, L4
3	Use OSINT tools for analysis fake news, image, video data	L1, L2, L3
4	Conduct advanced searches to gather intelligence from social media sites and understand the use of Public Records for corporate and business intelligence etc.	L1, L2
5	Gather information/metadata about Maps to performance detailed map profiling	L1, L2, L3
6	Get familiar with Technical Foot printing websites for mitigating various threats	L1, L2

Prerequisite:

1. Kali Linux Installation and VM deployment.
2. Networking and security fundamentals

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	The Evolution of Open-Source Intelligence,	Open-Source Information Categories OSINT Types, Digital Data Volume, OSINT Organizations, Parties Interested in OSINT Information, International Organizations, Information Gathering Types, Benefits of OSINT, Challenges of Open-Source Intelligence Legal and Ethical Constraints	**1**	LO1
I	Introduction To Online Threats and Countermeasures	Online Threats-. Securing the Operating System: Hardening the Windows OS, Staying Private in Windows, Destroying Digital Traces General Privacy Settings- Avoiding Pirated Software, Handling Digital Files Metadata, Physically Securing Computing Devices	**1**	LO1
II	Using Search Engines to Locate Information	Search Engine Technique - Keywords Discovery and Research, - Google, Privacy-Oriented Search Engines, Other Search Engines, Business Search Sites, Metadata Search Engines, Code Search FTP Search Engines Automated Search Tools, Dorks	**2**	LO2
III	Searching for Digital Files	News Search - Customize Google News, News Websites, Fake News Detection - Document Search, Image, Video, File Extension and File Signature List, Productivity Tools	**2**	LO4
IV	People Search Engines and Public Records	Social Media Intelligence: What Is Social Media Intelligence? Social Media Content Types, General Resources for Locating Information on Social Media Sites Pastebin Sites People Search Engine, Public Records and example of Public Records, Searching for Personal Details, General People Search , Online Registries, Vital Records, Criminal and Court Search, Property Records, Tax and Financial Records, Social Security Number Search Username Check, E-mail Search and Investigation Data Compromised Repository Websites, Phone Number Search	**6**	LO4
V	Online Maps:	The Basics of Geolocation Tracking, How to Find the GPS Coordinates of Any Location on a Map How to Find the Geocode Coordinates from a Mailing Address, General Geospatial Research Tools Commercial Satellites, Date/Time Around the World, Location-Based social media, Conducting Location Searches on social media Using Automated Tools, Country Profile Information Transport Tracking	**6**	LO5
VI	Technical Foot printing:	Website History and Website Capture Website Monitoring Services - RSS Feed Investigate the Target Website, Investigate the Robots.txt File, Mirror the Target Website Extract the Links Check the Target	**6**	LO6

		Website's Backlinks Monitor Website Updates Check the Website's Archived Contents Identify the Technologies Used, Web Scraping Tools Investigate the Target Website's File Metadata, Website Certification Search, Website Statistics and Analytics Tools, Website Reputation Checker Tools, Passive Technical Reconnaissance Activities, WHOIS Lookup, Subdomain Discovery, DNS Reconnaissance, IP Address Tracking		

Textbooks:

1. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence by Nihad A. Hassan (Author), Rami Hijazi (Author)

2. OSINT Techniques - Resources for Uncovering Online Information - 10th Edition (2023) by Michael Bazzell

3. Operator Handbook: Red Team + OSINT + Blue Team Reference by Joshua Picolet

References:

1. We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of Newsby Eliot Higgins
2. Extreme Privacy: What It Takes to Disappear in America by Michael Bazzell

Tools:

- https://cheatsheet.haax.fr/open-source-intelligence-osint/
- https://inteltechniques.com/tools/
- https://hunter.io/
- https://www.shodan.io/

https://github.com/laramies/theHarvester

- https://www.osintcombine.com/osint-bookmarks
- https://osintframework.com/
- https://learn.baselgovernance.org/enrol/index.php?id=79
- https://inteltechniques.com/
- https://www.bellingcat.com//
- https://www.tracelabs.org/

List of Experiments/Mini-Project.

Sr. No.	Detailed Content
1.	. Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information. . Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization. . Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing
2	Using OSINT tool such as (Harverster) you can gather information like emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key server.
3	Use OSINT DORKS (create and execute search queries) to verify the accuracy of the information by cross-referencing various sources and critically evaluating the reliability and credibility of the New article.

4	To perform the reverse Image analysis for finding physical location where the content was captured. Use OSINT tool to use image metadata, landmarks, street signs, or other visual cues to identify the geolocation accurately.
5	Using OSINT tools gather Tactical information using WHOIS lookup tools or websites like DomainTools (domain, registration details, owner's contact information, registration date, and expiration date.) Archives, Text, Reverse Image Search, Images and EXIF data, Source code, Others TLD, Mentions of target, Check info such as via RSS,SSL certificates, Robots/Sitemap, Port scans, Reverse IP lookup
6	Utilize website crawling OSINT tools to gather a comprehensive list of URLs, internal links, and structure of the website
7	Use OSINT Tools to identify the technologies and frameworks used by the website, such as content management systems (CMS), server software, programming languages, or analytics tools and create vulnerability reports.
8	Determine the geolocation (country, city, or approximate location) of each IP address (at least 10) One can use online IP geolocation tools, databases, and various techniques to gather information and accurately identify the physical location associated with each IP
9	Conduct a comprehensive OSINT investigation about well-known company and gather information about the company's history, key executives, financial data, partnerships, news mentions, and any other relevant details using online databases, news articles, corporate websites, and industry reports
10	Analyze the company's competitors to understand their market positioning, strengths, and weaknesses. Tools like SEMrush, Similar Web, or Alexa or any other OSINT tool can provide website traffic, keyword analysis, and competitor comparisons
11	Fake News detection - Analyze at least 5 OSINT tools to detect, verify, authenticate, fake news and report.
12.	Example Mini Project suggestion - Digital Footprint Analysis using OSINT Tools: Assess and analyze your own digital footprints wrt, Personal Information, data (full name, age, date of birth, address, phone number, and email address), images, videos (online directories, social media profiles (at least 3 social media accounts), personal websites, Online Professional Presence and analyze 1.Posts, comments, photos, and other content that they have shared publicly or with specific privacy settings 2.Analyze their online interactions, connections, interests, and activities. 3. Analyze the nature of the content, locations, events, or people, as it can provide insights into activities, hobbies, or relationships. 4. Analyze work experience, educational background, skills, recommendations, and any professional associations or achievements.