Subject: Open Source Intelligence								
Program: M.Tech. in Cyber Security				**Subject Code:**			**Semester: II**	
Teaching Scheme				**Examination Evaluation Scheme**				
Lecture	**Tutorial**	**Practical**	**Credits**	**University Theory Examination**	**University Practical Examination**	**Continuous Internal Evaluation (CIE)-Theory**	**Continuous Internal Evaluation (CIE)-Practical**	**Total**
4	**0**	**2**	**5**	**40**	**40**	**60**	**60**	**200**

COURSE OBJECTIVES:

- The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing security.
- The course includes-Impacts of Hacking; Types of Hackers; Information Security Models; Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable, and Integration)

Content

Course Content

W - Weightage (%) , **T** - Teaching hours

Sr.	**Topics**	**W**	**T**
1	**OSINT Foundations :** Introduction to the Intelligence Lifecycle and C.R.A.W.L. (Communicate, Research, Analysis, Write and Listen) method o Identify and describe the goals, capabilities, and limitations associated with open source intelligence. § Describe and explain the OSINT investigations. § Identify and describe type of investigative uses for OSINT. o Begin to understand legal and technical boundaries. § Learn the CYA (Cover your Analyst) method § Threats vs. hyperbole	**25**	**11**
2	**OSINT PREPARED:** Introduction to managed attribution, and the technology models in place, and best practices for conducting OSINT safely online. o The basics of protecting yourself while conducting online investigations § Computer hygiene - Virus/malware protection o Identify and describe the capabilities and limitations associated with managed attribution. § Identify when managed attribution is necessary. § Understand the sock puppet account. o Begin to understand legal and technical boundaries. § Working undercover online, misrepresentation. § Solutions developed by hand, and by vendors, to solve for MA on the road.	**25**	**11**

3	**– Search Engine Researcher** o Describe and demonstrate how to use web-based and proprietary open source search tools to conduct investigations. o Establish a working knowledge of the use of language. § Geo tagging § Global tagging § Keywords, buzzwords, and lingo § Boolean logic and the lack of logic § Algorithms influence on your queries. o Identify and describe the best uses of search engines. § Google § Bing § Username Search tools **OSINT Social Media Researcher** o Explain and demonstrate how to conduct social media research to obtain and leverage sensitive personal data during an investigation. o Identify and describe the best uses of social media. § Deep platforms • Facebook • Twitter • Instagram • LinkedIn • Telegram • Reddit • Parler • Gab • 4chan • Other online communities o Explain and demonstrate how to locate social data on users who do not have social media accounts, or if they have protected accounts.	**25**	**12**
4	**OSINT TEHNICAL RESERCHER** Define and explain the different types of files that contain useful metadata as well as how to access, modify and delete metadata. § Images and EXIF data § Adobe and Microsoft metadata o Describe and explain how to conduct reverse image searches to identify the origin, modifications, and geolocation data associated with an image or video. § Images, Video and EXIF data o Describe and explain how to find the geolocation or a subject's IP address using Internet search tools. § Email headers and IP addresses § DNS database entries § WhoIs lookups and data interpretation § Traceroute o Introduce and describe the Dark Web § Define the dark web § Perils of dark web content, and the type of content located in the	**25**	**11**

	dark web § Search tools and approaches to the dark web		

TEXT BOOKS:

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press

REFERENCE BOOKS

1. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning
2. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning

List of Practicals:

List of Practical	
1.	**Practical-1** Network scanning and reconnaissance using Nmap and other tools to identify open ports, operating systems, and potential vulnerabilities.
2.	**Practical-2** Packet capture and analysis using Wireshark or tcpdump to capture and analyze network traffic for potential security threats.
3.	**Practical-3** Network hardening and configuration management, including implementing secure network configurations and managing network devices.
4.	**Practical-4** Advanced cryptography, including setting up and configuring digital certificates and testing for potential vulnerabilities in encryption algorithms.
5.	**Practical-5** Intrusion detection and prevention, including setting up and configuring Snort or other IDS/IPS systems and analyzing logs and alerts.
6.	**Practical-6** Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.
7.	**Practical-7** Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.
8.	**Practical-8** Configure S/MIME and show email-authentication
9.	**Practical-9** Implement encryption and decryption with openssl.

10.	**Practical-10** Security information and event management (SIEM) using tools like Splunk or ELK to collect and analyze logs from various systems and devices.