Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	T	P	L	T	P	Total
OE3	Cybersecurity and Digital Forensics	1	-	2	1	-	1	2
		Examination Scheme						
		ISE		MSE		ESE		Total
		40		10		20		70

Pre-requisite Course Codes		Computer Basics, Networking basics
Course Outcomes	CO1	Identify and classify various cybercrimes with respect to organizational weaknesses in order to mitigate the security risk and estimate the impact on society and world
	CO2	Analyze the results of vulnerability scans of vulnerability assessment and generate report with penetration testing
	CO3	Apply Information Security Standards compliance during software design and development
	CO4	Interpret and apply Indian IT laws in various legal issues
	CO5	Describe the concept of Digital forensics and use various tools and techniques used for digital forensics investigations
	CO6	Integrate advanced security solutions and manage, provide policies, standards, procedures, guidelines, policy framework, assess and mitigate risk

M	Topics	CO
1.1	**Introduction to Cyber Security [3]**	**CO1**
1.2	Cybercrime definition and origins of the world, Cybercrime and information security, Classifications of cybercrime,	CO1
1.3	Cybercrime and the Indian ITA 2000, A global Perspective on cybercrimes.	CO4
2.1	**Cyber offenses & Cybercrimes: [5]** How criminal plan the attacks, Social Engg, Cyber stalking, Cyber café and Cybercrimes, Botnets, Attack vector,Credit Card Frauds in Mobile and Wireless Computing Era, Security,Challenges Posed by Mobile Devices	CO1
2.2	Tools and Methods Used in Cybercrime: Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks,Identity Theft (ID Theft)	
3.1	**Security Risk Assessment and Risk Analysis: [4]** Risk Terminology, Laws, Mandates, and Regulations,Risk Assessment Best Practices,The Goals and Objectives of a Risk Assessment, Best Practices for Quantitative and Qualitative Risk Assessment.	CO2,CO6
3.2	**Vulnerability Assessment and Penetration Testing (VAPT):** VAPT An Overview,Goals and Objectives of a Risk and Vulnerability Assessment,	CO2
3.3	Vulnerability Assessment Phases-Discovery,Exploitation/Analysis , Reporting Penetration Testing Phases-Discover/Map,Penetrate Perimeter,Attack Resources, Network and Web VAPT Process	CO2,CO6
5.1	**Digital Forensics: [5]** Need for forensics, Cyberforensics and Digital Evidence	CO5,CO6
5.2	Digital Forensics Life cycle, Computer forensics investigation, setting-up forensics laboratory, Special Tools and Techniques, Forensics Auditing and Compliance Requirements, Anti Forensics	CO5,CO6
5.3	Forensics of Hand-held devices,Tool-kits for Hand-held device forensics,Techno-Legal Challenges with Evidence from Hand-held Devices	CO5,CO6
4.1	**Cyber Security Laws and Legal Perspectives [3]**	CO4
4.2	Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals Under the IT Act, 2000, IT Act. 2008 and its Amendments	CO3,CO4
4.3	Information Security Standard compliances: SOX, GLBA, HIPAA, ISO, FISMA, NERC, PCI-DSS	CO3

Lab Planning:

Lab No	Lab Details
	Preparatory Laboratory: [a] Install and configure Virtual Environment- **VirtualBox** [b] Select Intrusion Dataset
1	**Lab-1A:** Network Scanning **(nmap)**, Web Server Vulnerability Scanning (**Nikto**) and Host scanning **(fping)** **Lab-1B:** Network Sniffing (**TCPDUMP/Wireshark/tshark/Ettercap**), Vulnerability Scanning (nmap ad CVE) and Security Visualization (**Etherape**)
2	**Lab-2A:** Infosec Coding using **Python Network Socket Programming** (Build the port scanner) **Lab-2B:** Network Scanning, Packet manipulation, Network Attacks using **Scapy**
3	**Lab-3: Backdoor-** Network Socket/ File Transfer and Reverse Shell using **Netcat**
4	**Lab-4:**Vulnerability Assessment and System Hacking (VAPT) **VA-Nessus/OpenVAS** and **Penetration Testing using Metasploit**
5	**Lab-5A:** Cyber Security and Machine Learning-Intrusion Detection **KDDCUP99/NSL-KDD/CIC-IDS2017 dataset** **Lab5B:** Anomaly detection- **network traffic analysis using tshark**
6	**Lab-6:** Cryptosystems- **PKI using Openssl and pycrypto,PGP (PEM), GPG**
7	**Lab-7A:**Intrusion Detection System (IDS) and Firewalls **Snort-NIDS, Logwatch-HIDS, Design and Development Anomaly detection using Simple Event Correlator (SEC) and Integration with Email (Postfix/Sendmail Server)** **Lab-7B:** Security Operation Center (SOC) and Security Event Information Event Management (SIEM): **Prelude-SIEM, Snort-NIDS, Suricata-NIDS, Logwatch-HIDS, OSSEC-HIDS, IPTABLES-Firewall and Syslog**
8	**Digital Forensics: Part-I** **Lab-8A:** Network Forensics using **Xplico and tshark** **Lab-8B:** Digital Forensics (Host/Disk) with **TCT/Sleuthkit**
8	**Digital Forensics: Part-II** **Lab-8C:** Memory Forensics using **Volatility** **Lab-8D:** Email Forensics using **Online utilities**

Sessions as per Google Classroom:

Session	Date	Topics Details
1	**5/1/21**	**I. Key areas covered: 4th Jan 2021** **1. Technology & Cybercrimes and Cybersecurity** **2. Cybersecurity Technologies** **3. Cybersecurity Risk Management** **4. Digital Forensics** **5. Legal Perspectives of Cybercrimes** **6. Advanced Topics in Cybersecurity & Digital Forensics** **II. Course Objectives** **III. Cyber Careers** **IV. Cyber Certifications** **V. Course Overview** **VI. Laboratory Overview** **VII. System Requirements** **For cyber careers refer the following link:** **https://www.cyberaces.org/careers.html** **Objectives of Cybersecurity Degree Program** **https://www.cyberinternacademy.com/7-objectives-you-will-learn-in-a-cybersecurity-degree-program/** **** **Classroom Link:** **https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MTk1MzY2NTk4MjI5/details**
2	**12/1/21**	**Cyberattacks refer ppt 12th Jan** **Classroom Link:** **https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MjI0NTM4OTM4NzY2/details**
3	**19/1/21**	**Session-3: Cyber Security [19th Jan 2021]** **https://meet.google.com/hhp-ifbp-kme** **What makes a network vulnerable?** **Critical Infrastructure** **Cyber Players and Their Motives** **Cyber Security Challenges** **Security Services and Mechanisms** **Classroom Link:** **https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MjU3MTA0Mzk5OTgx/details**

4	2/2/21	Session-4: 2nd Feb,2021, 8.00-9.00 am Security Requirements Security Services Security Mechanisms Relationships between Security Services and Security Mechanisms Multi-layer Security-Defense-in-Depth Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MjY1MzA4OTc0OTQ1/details
5	9/2/21	Session-5: 9th Feb,2021 Vulnerability Assessment and Penetration Testing (VAPT) Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MjcwMDgwOTMxMjUw/details
6	16/2/21	Session-6: 16th Feb 2021(8am to 9 am) Risk Assessment & Security Standards [1] Why Risk Assessment? [2] Review of VAPT (NetVAPT + WebVAPT) [3] VAPT template [4] Brief introduction to Cloud VAPT & reading material. [5] Practice QUIZ Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/Mjc0OTkyNjQ1Mjc5/details
7	23/2/21	Session-7: 23rd Feb 2021 (In class reading) Security Information and Event Management- SIEM [1] Introduction to SIEM [2] Why is SIEM important [3] How does it work [4] Selecting SIEM for your organization References: [1] The Essential Guide SIEM https://www.exabeam.com/siem-guide/ [2] Need for SIEM https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM Youtube on SIEM: [1] https://www.youtube.com/watch?v=ZuLazPqFtBE&feature=emb_rel_pause [2] https://www.youtube.com/watch?v=fXBnjhpDXPE Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/Mjc5ODkyNTgyNjE4/details
8	2/2/21	Session-8: 2nd March, 2021 (In class reading) [1] Revision [2] NIST Cybersecurity Framework https://www.nist.gov/cyberframework [3] SANS CSC https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995 Online youtube Video: https://www.youtube.com/watch?v=nFUyCrSnR68 Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MjcyNzQ1NTMwMjk1/details
9	9/3/21	Session-9: 9th March 2021 on Network Forensics Analysis using Open Source Tools [1] Introduction to Digital Forensics [2] Types of Digital Forensics https://www.guru99.com/digital-forensics.html [3] Network Forensics (NF) [4] Open Source Tools for NF Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/Mjg4NDAyOTUyODAw/details
10	16/3/21	Session-10 : 16th March 2021 Digital Forensics and Incident Response (DFIR) Digital Forensics- Job Opportunities [1] https://www.eccouncil.org/what-is-digital-forensics/ [2] https://cybersecurityguide.org/careers/digital-forensics/ [3] https://cybersecurityguide.org/careers/digital-forensics/ Classroom Link: https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/Mjk2ODUxMzAzMDc5/details
11	23/2/21	Session-11: 23rd March 2021 Network Forensics Analysis Tools (NFATs) General Framework of Network Forensics Analysis

		Digital Forensics Science and Incident Response Methodology **Activities assigned:** **[1] Digital Forensics Concept Map** **[2] Setting up Digital Forensics Laboratory** **Classroom Link:** https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MzA2NDI2MTY5MjA2/details
12	**30/3/21**	**Session-12: 30th March 2021** **In-class reading: Reading material branch wise and discussion** **Use Cases in Digital Forensics** **Standards and best practices for digital forensics** **References:** **1. Introduction to Network Forensics: ETRX/EXTC/COMPUTER/IT** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf/at_download/file **2. ICS/SCADA Environment- ETRX and EXTC Students** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-ex1-toolset.pdf **3. Detecting exfiltration on a large finance corporation environment: Computer Students** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-ex2-toolset.pdf/at_download/file **4. Analysis of an airport third-party VPN connection compromise- IT Students** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-ex3-toolset.pdf/view **5. Smart Grid Security Related Standards Guidelines and Regulatory Documents** https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/at_download/file **6. Standards and best practices for digital forensics** https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html **Classroom Link:** https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MzEwOTcxOTMxNTYw/details
13	**6/4/21**	**Session-13: 6th April 2021Cloud Computing Security** **Cloud Computing Security** **[1] Introduction to Cloud Computing** **[2] Cloud Computing Service Architecture as Layers (Iaas, PaaS, SaaS)** **[3] Benefits of using the cloud for your business** **[4] Multi-tenancy** **[5] Cloud Deployment Architecture (Public, Private, Hybrid)** **[6] The risk associated with Cloud Computing** **[7] Cloud Computing Security Challenges** **References:** **[1]** https://www.lucidchart.com/blog/cloud-computing-basics **[2]** http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 **Classroom Link:** https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MzEyODU4MjI5MDkw/details
14	**14/4/21***	**Session-14: 17th April 2021** **Cybercrime and Cyber Laws** **Indian Information Technology Act 2000** **Refer the online resources:** **1.** https://www.youtube.com/watch?v=J-F0-49qLU8 **2.** https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india **Classroom Link:** https://classroom.google.com/c/MjQ5MjE1OTA5MzY0/p/MzE3MDkyNTc0ODQ0/details

Recommended Books:

[1] Nina Godbole, Sunit Belapure, Cyber Security, Wiley India, New Delhi.

[2] The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi

[3] The Information technology Act, 2000; Bare Act- Professional Book Publishers, NewDelhi.

[4] Cyber Law & Cyber Crimes By Advocate Prashant Mali; Snow White Publications, Mumbai

[5] Nina Godbole, Information Systems Security, Wiley India, New Delhi

[6] Kennetch J. Knapp, Cyber Security & Global Information Assurance Information Science
Publishing.

[7] Michael Gregg & David Kim,Inside Network Security Assessment: Guarding Your IT Infrastructure, Pearson Publication

[8] M. L. Srinivasan, CISSP in 21 Days - Second Edition PACT Publication

[9] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Pearson Publication
[10] Douglas J. Landoll, The Security Risk,Assessment Handbook-Second Edition ,Auerbach Publications
[11] Websites for more information is available on : The Information Technology ACT, 2008-TIFR : https://www.tifrh.res.in
[12] https://www.sans.org/reading-room/whitepapers/compliance/compliance-primer-professionals-33538
[13] Open Source Security Tools: A Practical Guide to Security Applications by Tony Howlett, Pearson Education
[14] https://www.virtualbox.org
[15] Hands-On Information Security Lab Manual by Michael Whitman, Cengage publication
[16] https://www.offensive-security.com/metasploit-unleashed/