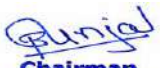


AMRUTVAHINI COLLEGE OF ENGINEERING, SANGAMNER
Department of Information Technology Engineering
Honors in Cyber Security (18 Credits)

Year	Semester	Course Code	Course Name	Credits
Second Year	Sem III	R25-IT-HOC-201	Internet Crimes and Cyber Security	3
	Sem IV	R25-IT-HOC-202	Ethical Hacking in AI Aera	3
Third Year	Sem V	R25-IT-HOC-301	Network Security and Digital Forensics	3
	Sem VI	R25-IT-HOC-302	Secure Software Development and Web Security	3
Final Year	Sem VII	R25-IT-HOC-401	AI for Cyber Security and Threat Intelligence	3
	Sem VIII	R25-IT-HOC-402	Security of Cyber Physical Systems	3


Chairman
 BoS, Information Technology
 Amrutvahini College of Engineering, Amrutnagar
 Sangamner-422608




Chairman
 Academic Council
 Amrutvahini College of Engineering, Amrutnagar
 Sangamner-422608

Program:	S. Y. B. Tech (Information Technology)			Semester:	III		
Course:	Internet Crimes and Cyber Security			Course Code:	R25-IT-HOC-201		
Teaching Scheme (Hrs. / week)			Credits (TH)	Examination Scheme			
Lecture	Practical	Tutorial		CCE	ESE	TW	PR
3	-	-	3	40	60	-	-
Course Description: Internet Crimes and Cyber Security is an Honors course designed to provide Information Technology Engineering students with a comprehensive understanding of cybercrime and the principles, technologies, and practices used to secure digital systems. The course introduces various forms of internet and cybercrimes, including hacking, identity theft, phishing, cyber fraud, malware attacks, ransomware, cyberbullying, and attacks on networks and critical information infrastructure. Students will explore fundamental concepts of cybersecurity, network and system security, cryptography, ethical hacking concepts, digital forensics, incident response, cyber laws, privacy, and ethical issues related to cyberspace. The course emphasizes the identification and analysis of cyber threats and vulnerabilities and introduces suitable security mechanisms and preventive measures. Course Relevance: Internet Crimes and Cyber Security as an Honors course is highly relevant for Information Technology Engineering students due to the rapid increase in cyber threats, online fraud, data breaches, identity theft, ransomware, and other digital crimes. The course will provide students with an understanding of the nature of cybercrimes, cybersecurity principles, cyber laws, digital forensics, ethical practices, and techniques for protecting information systems and networks.							
Prerequisite: Basic knowledge of computer networks, operating systems, and fundamental programming concepts.							
Bridge Content: Basic concepts of computer networks, Internet architecture, operating systems, web technologies, data security, and fundamental programming concepts to establish the foundation required for understanding cybercrimes and cybersecurity mechanisms.							
Course Objectives: 1. Understand the concepts, types, and impact of internet crimes and cybercrimes. 2. Identify and analyze various cyber threats, vulnerabilities, and attacks on computer networks and information systems. 3. Apply appropriate cybersecurity techniques and mechanisms to protect digital systems and data. 4. Understand and investigate the basics of digital forensics, incident response, and cybercrime investigation. 5. Analyze cyber laws, privacy, ethical issues, and legal frameworks related to cyberspace and cybersecurity.							

Course Outcomes: After learning the course, students will be able to:

CO	Course Outcome	Bloom's Level
CO1	Explain the concepts, types, techniques, and impact of internet crimes and cyber threats.	2
CO2	Identify and analyze vulnerabilities, cyber-attacks, and security risks in computer networks and information systems.	4
CO3	Apply appropriate cybersecurity mechanisms and practices to protect systems, networks, and digital data.	3
CO4	Analyze digital evidence, basic forensic procedures, and incident-response techniques for cybercrime investigation.	4
CO5	Evaluate cybersecurity practices with respect to cyber laws, privacy, ethics, and legal responsibilities.	5

Course Contents

Unit 1	Fundamentals of Internet Crimes, Cyber Threats and Cybersecurity		CO1
---------------	---	--	------------

Introduction to Cybersecurity, Definition and importance of cybersecurity, Internet Crimes, Evolution of cybercrime, Cybercrime vs. traditional crime, Types of Internet Crimes, Common Cyber Threats, Impact of Cybercrime, Basic Cybersecurity Threat Landscape: Threat, vulnerability, risk, and attack, Common vulnerabilities.

Exemplars / Practical, Applications and usage:

- **Phishing and Social Engineering Case Study** – Analyze a real-world phishing scenario and identify warning signs, attack methods, and preventive measures.
- **Malware and Ransomware Analysis** – Study a simulated malware/ransomware incident to understand its impact on systems, data, and organizations.

Assignments:

- **Cybercrime Case Study:** Select a real-world internet crime (phishing, ransomware, identity theft, online fraud, etc.) and analyze its **attack method, impact, vulnerabilities exploited, and preventive measures**.
- **Cyber Threat Awareness Report:** Prepare a report on **common cyber threats and security practices**, covering malware, social engineering, password attacks, DoS/DDoS, and methods for protecting users and organizations.

Unit 2	Cyber Threats, Vulnerabilities and Attack Analysis		CO2
---------------	---	--	------------

Cyber Vulnerabilities and Risk: Common vulnerabilities and security weaknesses, Attack surface and attack vectors, Network Security Threats: DoS/DDoS attacks, Man-in-the-Middle attacks, Packet sniffing and spoofing, System and Application Attacks: Password attacks and brute-force attacks, Social Engineering Attacks, Security Risk Analysis.

Exemplars / Practical Applications and usage:

- **Network Attack Analysis:** Analyze a simulated DoS or Man-in-the-Middle attack and identify the exploited vulnerability and possible security controls.
- **Web Vulnerability Analysis:** Study a deliberately vulnerable web application to identify common vulnerabilities such as SQL Injection and XSS.

Assignments:

- **Cyber Attack Analysis Report:** Select a real-world cyber-attack and analyze its **attack vector, vulnerability exploited, impact, and security measures**.
- **Vulnerability and Risk Assessment:** Prepare a vulnerability and risk assessment of a hypothetical organization covering **assets, threats, vulnerabilities, risk level, and recommended controls**.

Unit 3	Cybersecurity Mechanisms and Data Protection	Weeks 4-5	CO3
Network Security Fundamentals: Firewalls and proxy servers, Intrusion Detection and Prevention Systems (IDS/IPS), Authentication and Access Control: Password security and multi-factor authentication, Role-Based Access Control (RBAC), Cryptography: Symmetric and asymmetric encryption, Hashing and digital signatures, Public Key Infrastructure (PKI), Data and System Protection, Secure Internet Practices.			
Exemplars / Practical Applications and usage:			
• Firewall Configuration: Configure basic firewall rules to allow legitimate traffic and block unauthorized network access. • Encryption Application: Implement or demonstrate symmetric/asymmetric encryption to protect sensitive data during storage or transmission.			
Assignments:			
• Cybersecurity Protection Plan: Design a security plan for a small organization using firewall, authentication, encryption, backup, and access-control mechanisms. • Encryption and Security Implementation: Implement a basic encryption/decryption technique using a programming language or cybersecurity tool and demonstrate how it protects confidential data.			
Unit 4	Digital Forensics and Cybercrime Investigation		CO4
Introduction to Digital Forensics: Concept, objectives, and importance, Types of digital forensics, Digital evidence and its characteristics, Digital Evidence Handling, Forensic Investigation Process, Network and Email Forensics, Incident Response, Digital Forensic Tools			
Exemplars / Practical Applications and usage:			
• Disk Forensics: Analyze a forensic disk image using a tool such as Autopsy to identify files, metadata, and deleted-file information. • Network Forensics: Analyze a captured network traffic file using Wireshark to identify suspicious communication or unusual network activity.			
Assignments:			
• Digital Forensics Case Study: Analyze a real-world cybercrime case and document the digital evidence, investigation process, forensic techniques, findings, and conclusions. • Forensic Investigation Report: Perform analysis on a provided sample forensic dataset using an appropriate forensic tool and prepare a report containing evidence identification, analysis, observations, and findings.			
Unit 5	Cyber Laws, Privacy, Ethics and Cybersecurity Governance	Weeks 7-8	CO5
Cyber Laws and Regulations, Data Privacy and Protection, Cyber Ethics, Cybersecurity Governance, Emerging Legal and Ethical Issues: AI and cybersecurity, Social media privacy, Cyber surveillance, Digital evidence and legal admissibility.			

Exemplars / Practical Applications and usage:

- **Cybercrime Case Evaluation:** Evaluate a real-world cybercrime case with respect to applicable cyber laws, offences, penalties, and legal responsibilities.
- **Privacy Policy Analysis:** Analyze the privacy policy of a commonly used digital platform and evaluate its data collection, storage, sharing, and user-consent practices.

Assignments:

- **Cyber Law Case Study:** Select a real-world cybercrime case in India and evaluate the applicable IT laws, legal provisions, penalties, privacy concerns, and ethical issues.
- **Privacy and Cybersecurity Audit:** Evaluate the privacy and cybersecurity practices of a selected organization or online platform and prepare a report with **identified gaps, legal/compliance concerns, and recommendations..**

Textbooks:

1. **William Stallings**, *Cryptography and Network Security: Principles and Practice*, Pearson.
2. **Chuck Easttom**, *Computer Security Fundamentals*, Pearson.
3. **Nina Godbole and Sunit Belapure**, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley India.
4. **John Vacca**, *Computer and Information Security Handbook*, Elsevier.

Reference Books:

1. **Behrouz A. Forouzan**, *Cryptography & Network Security*, McGraw-Hill.
2. **Eoghan Casey**, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press.
3. **Niels Ferguson, Bruce Schneier and Tadayoshi Kohno**, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley.

MOOCs Links and additional reading material:

1. Cybercrime, identity theft, hacking, cyber fraud, deepfakes, cyber law and cybersecurity
https://onlinecourses.nptel.ac.in/noc26_lw01/preview?utm_source=chatgpt.com
2. Network attacks, security mechanisms and hands-on demonstrations
https://onlinecourses.nptel.ac.in/noc26_ee20/preview?utm_source=chatgpt.com

Strength of CO-PO-PSO Mapping

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PSO 1	PSO 2	PSO 3
CO1	2	2	-	-	2	2	2	-	1	-	2	2	3	1
CO2	3	3	2	3	3	2	1	-	1	-	2	3	3	2
CO3	3	3	3	2	3	2	2	1	1	-	2	3	3	2
CO4	3	3	2	3	3	3	2	1	2	-	2	3	3	2
CO5	2	2	2	2	2	3	3	1	3	1	3	2	3	3
Avg	2.6	2.6	2.5	2.5	2.6	2	2.5	1	1.6	1	2.2	2.6	3	2

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

Assessment Pattern							
a) Continuous Comprehensive Evaluation (CCE) – 40 Marks							
The Continuous Comprehensive Evaluation shall be carried out by the Department based on the student's performance throughout the duration of the SWAYAM-NPTEL course. - Performance in NPTEL Weekly Assignments: 30 Marks - Course Progress and Participation (completion of video lectures, timely submission of weekly assignments, and periodic progress monitored by the Faculty Mentor): 10 Marks							
b) End Semester Evaluation (ESE) – 60 Marks							
- Students shall register for and appear in the SWAYAM-NPTEL Proctored Certification Examination. - The marks obtained in the NPTEL Proctored Examination shall be converted proportionally to 60 marks using the following formula: - Students who successfully obtain the NPTEL certificate shall have the converted score considered as the End Semester Evaluation (ESE) marks. - Students who fail to obtain the NPTEL certificate, fail to appear for the NPTEL certification examination, or fail the certification examination shall appear for the Institute End Semester Examination conducted by the College. - If a student appears for both the SWAYAM-NPTEL Certification Examination and the Institute End Semester Examination, the higher of the two ESE scores shall be considered for the award of the final grade. - The decision of the Department regarding verification of NPTEL scores and award of marks shall be final and binding.							
BT Level	CCE						ESE
	CT1	CT2	Assignments	Course Project	Field Activity / Case Study	Quiz / presentation etc.	
K1	-	-	✓	-	-	-	✓
K2	-	-	✓	-	-	-	✓
K3	-	-	✓	-	-	-	✓
K4	-	-	✓	-	-	-	✓
K5	-	-	-	-	-	-	-
K6	-	-	-	-	-	-	-

This course serves as a prerequisite for / maps with the following future courses: The course provides a foundation for advanced study in Artificial Intelligence, Machine Learning, Natural Language Processing, Intelligent Systems, Industrial Engineering Analytics, Production Scheduling, and Facility Layout Optimization.

Job Mapping:

- AI / Machine Learning Associate
- Industrial Engineering Analyst
- Operations / Scheduling Analyst
- NLP / Intelligent Systems Associate

Program:		S. Y. B. Tech (Information Technology)		Semester:		IV	
Course:		Ethical Hacking in AI Era		Course Code:		R25-IT-HOC-202	
Teaching Scheme (Hrs. / week)			Credits (TH)	Examination Scheme			
Lecture	Practical	Tutorial		CCE	ESE	TW	PR
3	-	-		3	40	60	-
Course Description: The course further extends conventional ethical hacking to the AI era , addressing AI-assisted security analysis, Generative AI security, LLM vulnerabilities, prompt injection, AI red teaming, agentic-AI security and AI-based threat detection.							
Course Relevance: This course addresses the growing need for cybersecurity professionals capable of identifying, analyzing, and mitigating evolving cyber threats. It integrates ethical hacking and penetration-testing techniques with contemporary AI, Generative AI, LLM, and AI red-teaming concepts to prepare students for emerging cybersecurity roles and industry challenges.							
Prerequisite: Basic knowledge of Programming, Computer Networks and Operating Systems							
Bridge Content: Basics of Computer Networks, Operating Systems, Programming, Web Technologies, Databases, Cryptography and Cybersecurity fundamentals.							
Course Objectives: • Develop fundamental knowledge of ethical hacking, cybersecurity, networking and security-testing methodologies. • Provide practical understanding of reconnaissance, scanning, enumeration and vulnerability assessment. • Develop the ability to analyse system, network, malware, social-engineering and web-security vulnerabilities. • Provide knowledge of cryptography, authentication and security mechanisms used to protect information systems. • Introduce penetration-testing tools and frameworks used for authorized security assessment.							
Course Outcomes: After learning the course, students will be able to:							
CO	Course Outcome						Bloom's Level
CO1	EXPLAIN the fundamentals of ethical hacking, cybersecurity, networking, hacking methodologies and legal and ethical aspects of security testing.						2
CO2	APPLY reconnaissance, information gathering, network scanning, enumeration and vulnerability assessment techniques using appropriate ethical hacking tools in an authorized environment.						3
CO3	ANALYZE system vulnerabilities, malware, password attacks, network attacks, social engineering and denial-of-service attacks and recommend suitable countermeasures.						4
CO4	ANALYZE cryptographic techniques, authentication mechanisms, digital signatures, certificates and security protocols for protecting information systems.						4

CO5	EVALUATE web-security and AI-assisted ethical-hacking solutions for vulnerability identification, threat detection, penetration testing and cybersecurity defense.	5
Course Contents		
Unit 1	Foundations of Ethical Hacking and Network Security	Weeks 1-3
Introduction to cybersecurity and ethical hacking, types of hackers, ethical hacking methodology, cyber attack surface, computer networking fundamentals, OSI and TCP/IP models, IP addressing and subnetting, routing concepts, network protocols, network security principles, CIA triad, firewalls, IDS/IPS, ethical and legal aspects of hacking, and introduction to AI in cybersecurity. Exemplars / Practical Applications and usage: ● Role of ethical hacking and cybersecurity principles in protecting organizational networks and information systems. ● Application of network security mechanisms such as firewalls, IDS/IPS and network segmentation for preventing cyber threats. Assignments: 1. Study and explain the ethical hacking lifecycle and analyze a real-world cyberattack case with respect to attack methodology, security risks, and ethical considerations. 2. Analyze an enterprise network security architecture and explain the role of firewalls, IDS/IPS, network segmentation, and other security mechanisms.		
Unit 2	Reconnaissance, Scanning and Vulnerability Assessment	Week 4-6
Information gathering and reconnaissance, passive and active reconnaissance, OSINT, WHOIS and DNS reconnaissance, network and port scanning, host and service discovery, Nmap, vulnerability scanning, vulnerability classification and prioritization, enumeration, banner grabbing, AI-assisted reconnaissance, AI-based vulnerability analysis, and setup of an isolated ethical hacking laboratory. Exemplars / Practical Applications and usage: ● Use of Nmap, OSINT and reconnaissance techniques for identifying hosts, services and potential security weaknesses in authorized environments. ● Application of vulnerability assessment and risk prioritization for identifying and mitigating security vulnerabilities. Assignments: 1. Perform authorized network reconnaissance and scanning using Nmap in a controlled laboratory environment and document the identified hosts, ports, services, and security findings. 2. Conduct a vulnerability assessment of an authorized or intentionally vulnerable system and classify, prioritize, and recommend suitable mitigation measures for the identified vulnerabilities.		
Unit 3	System Hacking, Malware and Network Attacks	Weeks 7-9
System hacking concepts, authentication and password attacks, password security, privilege escalation, system vulnerabilities and hardening, malware types including viruses, worms, Trojans, ransomware and spyware, malware analysis, ARP spoofing, man-in-the-middle attacks, packet sniffing and traffic analysis using Wireshark, social engineering and phishing attacks, denial-of-service and DDoS attacks, detection and mitigation techniques.		

Exemplars / Practical Applications and usage: ● Analysis of malware, ransomware, phishing, ARP spoofing and social-engineering attacks to understand attack techniques and security risks. ● Application of network monitoring, malware analysis and attack mitigation techniques for detecting and responding to cyber threats.			
Assignments: 1. Select and analyze a real-world malware or ransomware attack and explain its attack vector, impact, indicators of compromise, detection methods, and preventive measures. 2. Study a simulated ARP spoofing, phishing, or social-engineering attack in a controlled environment and identify appropriate detection and mitigation techniques.			
Unit 4	Cryptography, Authentication and Advanced Security	Week 10-12	CO4
Fundamentals of cryptography, plaintext and ciphertext, encryption and decryption, symmetric and asymmetric cryptography, AES and RSA, cryptographic hash functions, password hashing, digital signatures, digital certificates, PKI, steganography, biometric authentication, DNS and email security, AI-based anomaly detection, behavioral authentication, intelligent fraud detection and AI-enhanced security analytics.			
Exemplars / Practical Applications and usage: ● Application of AES, RSA, hashing, digital signatures and digital certificates for secure communication and information protection. ● Use of multi-factor authentication, biometrics and AI-based security analytics for strengthening authentication and access control.			
Assignments: 1. Demonstrate AES, RSA, and cryptographic hashing techniques and compare their applications, security characteristics, and limitations. 2. Analyze the role of digital certificates, digital signatures, and multi-factor authentication in securing online transactions and information systems.			
Unit 5	Web Security, Penetration Testing and AI-Era Ethical Hacking	Weeks 13-15	CO5
Metasploit framework and penetration-testing concepts, web-server security, HTTP/HTTPS, SQL injection, cross-site scripting, web authentication and session security, Burp Suite and web application testing, Generative AI and LLM security, prompt injection, sensitive-information disclosure, AI-assisted vulnerability assessment, AI red teaming, agentic-AI security, AI-based threat detection, AI-assisted penetration testing, security case studies and preparation of ethical-hacking assessment reports.			
Exemplars / Practical Applications and usage: ● Use of Metasploit, Burp Suite and web security testing techniques for identifying vulnerabilities in authorized web applications. ● Application of AI/Generative AI, LLM security, prompt-injection analysis and AI red teaming for evaluating and improving the security of AI-enabled applications.			
Assignments: 1. Perform a security assessment of an intentionally vulnerable web application to identify SQL Injection and XSS vulnerabilities and recommend appropriate countermeasures. 2. Analyze security risks in a controlled Generative AI/LLM application, such as prompt injection or sensitive-information disclosure, and propose suitable security controls.			
Textbooks:			

1. Wilhelm, T., & Engebretson, P. (2026). The basics of hacking and penetration testing (3rd ed.). Elsevier.
2. Hickey, M., & Arcuri, J. (2020). Hands-on hacking: Become an expert at next-gen penetration testing and purple teaming. Wiley.

Reference Books:

1. Banoth, R., & Godishala, A. K. (2026). Cybersecurity red teaming: Penetration testing strategies. Springer.
2. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

MOOCs Links and additional reading material:

1. Internet Crimes and Cyber Security

🔗 https://onlinecourses.nptel.ac.in/noc26_lw01/preview

2. Artificial Intelligence in Industrial and Management Engineering

🔗 https://onlinecourses.nptel.ac.in/e-learning/preview/noc26_ge105

Strength of CO-PO-PSO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	1	1	1	2	-	3	-	1	-	1	2	1
CO2	3	3	2	2	3	2	-	2	1	1	1	3	3	2
CO3	3	3	2	3	3	2	1	3	1	1	1	3	3	2
CO4	3	3	2	2	3	2	-	2	-	1	1	3	2	2
CO5	3	3	3	3	3	2	1	3	2	2	2	3	3	3
Avg	3.0	2.8	2.0	2.2	2.6	2.0	1.0	2.6	1.0	1.2	1.0	2.8	2.6	2.0

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

Assessment Pattern

a) Continuous Comprehensive Evaluation (CCE) – 40 Marks

The Continuous Comprehensive Evaluation shall be carried out by the Department based on the student's performance throughout the duration of the SWAYAM-NPTEL course.

- Performance in NPTEL Weekly Assignments: 30 Marks
- Course Progress and Participation (completion of video lectures, timely submission of weekly assignments, and periodic progress monitored by the Faculty Mentor): 10 Marks

b) End Semester Evaluation (ESE) – 60 Marks

7. Students shall register for and appear in the SWAYAM-NPTEL Proctored Certification Examination.
8. The marks obtained in the NPTEL Proctored Examination shall be converted proportionally to 60 marks using the following formula:
9. Students who successfully obtain the NPTEL certificate shall have the converted score considered as the End Semester Evaluation (ESE) marks.
10. Students who fail to obtain the NPTEL certificate, fail to appear for the NPTEL certification examination, or fail the certification examination shall appear for the Institute End Semester Examination conducted by the College.
11. If a student appears for both the SWAYAM-NPTEL Certification Examination and the Institute End Semester Examination, the higher of the two ESE scores shall be considered for the award of the final grade.
12. The decision of the Department regarding verification of NPTEL scores and award of marks shall be final and binding.

BT Level	CCE						ESE
	CT1	CT2	Assignments	Course Project	Field Activity / Case Study	Quiz / presentation etc.	
K1	-	-	✓	-	-	-	✓
K2	-	-	✓	-	-	-	✓
K3	-	-	✓	-	-	-	✓
K4	-	-	✓	-	-	-	✓
K5	-	-	-	-	-	-	-
K6	-	-	-	-	-	-	-

This course serves as a prerequisite for / maps with the following future courses: The course provides a foundation for advanced study in Artificial Intelligence, Machine Learning, Natural Language Processing, Intelligent Systems, Industrial Engineering Analytics, Production Scheduling, and Facility Layout Optimization.

Job Mapping:

- AI / Machine Learning Associate
- Industrial Engineering Analyst
- Operations / Scheduling Analyst
- NLP / Intelligent Systems Associate