Savitribai Phule Pune University, Pune

Maharashtra, India

Faculty of Science and Technology,

BoS- Electronics & Telecommunication Engg

National Education Policy (NEP)-2020 Compliant Curriculum

Honor Course in

Cyber Security & Governance

Applicable from: Third Year(T.E.) for

1. T.E. – E &TC Engg

2. T.E.- Internet of Things (IoT)

3.T.E - Electronics & Computer Engg

4. T.E. – Electronics Engg (VLSI Design & Technology)

5. T.E. - Electronics & Comm Engg (Advanced Comm Tech)

(With effect from Academic Year 2026-27)

Preface by Board of Studies - Electronics & Telecommunication Engineering

Dear Students and Teachers,

Dear Students and Teachers,

It gives me immense pleasure to present the Honor Course in Cyber Security & Governance for the under-graduate students of E&TC/ VLSI Design & Technology / IoT/ Advanced Communication Technology/ Electronics & Computer Engineering students under the Faculty of Science and Technology of Savitribai Phule Pune University. This course has been designed in alignment with the vision of the National Education Policy (NEP) 2020, emphasizing multidisciplinary learning, innovation, skill development, and industry-oriented education.

In the contemporary digital era, the rapid evolution of technology has seamlessly integrated cyberspace into every facet of human life, critical infrastructure, and global commerce. While this digital transformation has unlocked unprecedented opportunities for innovation, it has simultaneously ex-posed organizations and individuals to sophisticated, asymmetric cyber threats.

Under the aegis of the Board of Studies (BoS) in Electronics & Telecommunication Engineering, this curriculum for the Honors Course in Cyber Security & Governance has been meticulously designed for Third Year (TE) and Final Year (BE) engineering students. The primary objective of this specialized program is to bridge the gap between traditional Electronics & Computer Engineering and the highly specialized, rapidly evolving domain of information security.

I sincerely appreciate the valuable contributions of subject experts, academicians, industry professionals, and members of the Board of Studies who have devoted their expertise and efforts in framing this progressive curriculum. I am confident that this Honor Course will serve as a strong platform for nurturing future-ready engineers capable of contributing meaningfully to the rapidly evolving AI ecosystem.

I extend my best wishes to all students and faculty members for the successful implementation of this Programme.

Dr. S. D. Shirbahadurkar
Chairman,
Board of Studies, Electronics & Telecommunication Engineering
Savitribai Phule Pune University

Members of Board of Studies– E&TC Engineering	
Dr. Aditya Abhyankar	Dr. Rawal Awale
Dr. Bhagwat Jadhav	Dr. M.B. Mali
Dr. Sandeep Musale	Dr. Prachi Mukherji
Dr. Sunil Moon	Dr. Shailesh Kulkarni
Dr. Ramesh Pawase	Dr. Balasaheb Agarkar
Dr. Kishor Vikhe	Dr. P. Malathi
Dr. Manisha Dale	Dr. Urmila Patil

Honor Course in Cyber Security & Governance

Preamble

In alignment with the University Grants Commission (UGC) Curriculum and Credit Framework for Undergraduate Programme (CCFUP), National Education Policy (NEP) 2020, National Credit Frame-work (NCRF), and All India Council for Technical Education (AICTE) model curriculum guidelines, Savitribai Phule Pune University (SPPU) introduces Honors Courses in Engineering to promote multidisciplinary learning, advanced specialization, innovation, employability, entrepreneurship, and re-search orientation among undergraduate engineering students.

The Honors framework aims to:

- Provide domain specialization beyond the core engineering curriculum.
- Enhance industry readiness and interdisciplinary competence.
- Encourage research, innovation, and experiential learning.
- Support flexible and learner-centric education envisioned in NEP 2020.
- Facilitate pathways towards higher education, entrepreneurship, and emerging technologies.

About the Honors Programme

The Honors Programme in Cyber Security& Governance is a structured, industry-aligned curriculum offered to students enrolled in E &TC Engg, Internet of Things (IoT), Electronics & Computer Engg, Electronics Engg (VLSI Design & Technology), Electronics & Comm Engg (Advanced Comm Tech) and allied engineering disciplines. Commencement from the Semesters V through VIII, the Programme delivers one theory course and one laboratory-based practical course per semester, culminating in a capstone project, total four theory courses & four practical's with project, 18 credits overall.

The curriculum has been carefully designed in response to evolving National and International workforce demand projections for 2026–2030, preparing graduates to take on high-impact roles across offensive security, defensive cyber operations, cloud and AI-driven security, digital forensics, and governance, risk & compliance (GRC).

Employability Alignment (2026–2030 Boom Areas)

According to NASSCOM, Gartner, and global cybersecurity workforce studies, the following do-mains will see explosive demand through 2030:

- Cloud Security (AWS/Azure/GCP) — 35% YoY growth in job postings
- AI/ML Security & Adversarial Defence — Emerging, <5% professionals qualified globally
- SOC Analysts & Threat Intelligence — 3.5 million unfilled positions globally (2026)
- Penetration Testing & Red Teaming — Bug bounty payouts exceeding $1 billion annually
- DevOps Engineers — Mandatory in all BFSI, healthcare, and SaaS organizations
- Digital Forensics & Incident Response (DFIR) — Critical for regulatory compliance
- Cyber Law & GRC Analysts — Mandatory post DPDPA 2023 and GDPR enforcement

Upon successful completion of the Honors Programme in Cyber Security & Governance, graduates enter the global workforce equipped not only with technical expertise but also with the leadership capabilities required to address evolving cyber threats. Their careers begin with foundational roles such as Junior Security Analyst, Secure Software Developer, and Vulnerability Assessment Technician—critical positions that form the backbone of modern enterprise security operations. As they gain experience, graduates can pursue specialized pathways across both offensive and defensive security domains.

The offensive security track prepares professionals for high-demand roles including Penetration Tester, Red Team Operator, Web Application Security Specialist, and Bug Bounty Researcher. The defensive track develops expertise for Security Operations Centre (SOC) Analyst roles (L1–L3), Threat Intelligence, Incident Response, Security Monitoring, and SIEM Engineering.

For those drawn to investigation and cybercrime analysis, advanced opportunities exist in Digital Forensics, Malware Analysis, and Threat Research—fields experiencing significant growth due to increasing regulatory and compliance requirements worldwide. Recognizing the future direction of the industry, the Programme places special emphasis on the decade's fastest-growing disciplines: Cloud Security and AI Security. Graduates are prepared for roles such as Cloud Security Architect, AI Security Engineer, DevOps Engineer, Governance, Risk and Compliance (GRC) Analyst, and Cyber Law Consultant, with clearly defined pathways toward senior leadership positions including Security Architect and ultimately Chief Information Security Officer (CISO).

Aligned with workforce projections for 2026–2030—an era marked by an estimated 3.5 million unfilled cybersecurity positions globally, heightened digital transformation, and expanding regulatory frameworks such as India's DPDPA 2023, GDPR, and the EU AI Act—this Programme ensures graduates do not simply enter the cybersecurity profession. They enter it prepared to lead, innovate, and shape the future of digital security.

General Rules and Guidelines

- An Honors Degree in Engineering shall mean an undergraduate engineering degree with - additional specialization credits earned by a student in the same or allied discipline beyond the regular B.E./B.Tech curriculum requirements.
- Honor program will commence in Semester V and will be spread over 4 semesters (V-VIII). Eligible students can opt for any one Honors or Minors certification offered in given academic year by the department. To avail Honors or Minors certification, students need to acquire additional 1 8 - 20 credits
- Eligibility: A student shall be eligible to register for an Honors Programme subject to the following conditions:

Sr.	Criteria	Requirement
1	Academic Eligibility	Passed all courses up to previous Semesters
2	Minimum CGPA	7.50 CGPA or above at the end of Second Year
3	Backlog Condition	No active backlog at the time of registration
4	Attendance	Minimum 75% attendance in regular Programme
5	Conduct	Good academic and disciplinary record

- The institute may relax the CGPA criterion in exceptional cases with approval of the Director/Principal
- It is absolutely not mandatory to any student to opt for Honors or Minors Program.
- Choice is given to individual student to undertake Honors/Minors programs from the third year engineering (Fifth Semester) to fourth year engineering (Eighth Semester)

- The registration for Honors /Minors Programme will lead to gain additional credits to such students.
- As per the standard practice, SGPA and CGPA calculations will be done with common base only by considering mandatory credits assigned for the Bachelor Programme as per the structure approved by the Academic Council SPPU.

Guidelines for Examination Scheme

Theory Examination: The theory examination shall be conducted in two different parts

Comprehensive Continuous Evaluation (CCE) and End-Semester Examination (ESE).

Comprehensive Continuous Evaluation (CCE) :

1. CCE of 30 marks based on all the Units of course syllabus to be scheduled and conducted at institute level.
2. Case studies included under each unit are intended to support applied learning and are part of Comprehensive Continuous Evaluation
3. These case studies will be assessed through internal assessment components such as presentations, assignments, or group discussions. They shall not be included in the End-Semester Theory Examination.
4. To design a Comprehensive Continuous Evaluation scheme for a theory subject of 30 marks with the specified parameters, the allocation of marks and the structure can be detailed as follows:

Sr.	Parameters	Marks	Coverage of Units
1	Unit Test	12 Marks	Units 1 & Unit 2 (6 Marks/Unit)
2	Assignments / Case Study	12 Marks	Units 3 & Unit 4 (6 Marks/Unit)
3	Seminar Presentation / Open Book Test/ Quiz	06 Marks	Unit 5

Format and Implementation of Comprehensive Continuous Evaluation (CCE)

- **Unit Test**
  - **Format :** Questions designed as per Bloom's Taxonomy guidelines to assess various cognitive levels (Remember, Understand, Apply, Analyze, Evaluate, Create).
  - **Implementation**: Schedule the test after completing Units 1 and 2. Ensure the question paper is balanced and covers key concepts and applications.
- **Assignments / Case Study** : Students should submit one assignment or one Case Study Report based on Unit 3 and one assignment or one Case Study Report based on Unit 4.
  - **Format:** Problem-solving tasks, theoretical questions, practical exercises, or case studies that require in-depth analysis and application of concepts.
  - **Implementation:** Distribute the assignments or case study after covering Units 3 and 4. Provide clear guidelines and a rubric for evaluation.
- **Seminar Presentation:**
  - **Format:** Oral presentation on a topic from Unit 5, followed by a Q&A session.

- **Deliverables:** Presentation slides, a summary report in 2 to 3 pages, and performance during the presentation.
- **Implementation:** Schedule the seminar presentations towards the end of the course. Provide students with ample time to prepare and offer guidance on presentation skills.

- **Open Book Test:**
  - **Format:** Analytical and application-based questions to assess depth of understanding.
  - **Implementation:** Schedule the open book test towards the end of the course, ensuring it covers critical aspects of Unit 5.

- **Quiz :**
  - **Format:** Quizzes can help your students practice existing knowledge while stimulating interest in learning about new topic in that course. You can set your quizzes to be completed individually or in small groups.
  - **Implementation:** Online tools and software can be used create quiz. Each quiz is made up of a variety of question types including multiple choice, missing words, true or false etc

- **Evaluation and Feedback:**
  - **Unit Test:** Evaluate promptly and provide constructive feedback on strengths and areas for improvement.
  - **Assignments / Case Study:** Assess the quality of submissions based on the provided rubric. Offer feedback to help students understand their performance.
  - **Seminar Presentation:** Evaluate based on content, delivery, and engagement during the Q&A session. Provide feedback on presentation skills and comprehension of the topic.
  - **Open Book Test**: Evaluate based on the depth of analysis and application of concepts. Provide feedback on critical thinking and problem-solving skills.

End-Semester Examination (ESE)

End-Semester Examination (ESE) of 70 marks written theory examination based on all the unit of course syllabus scheduled by university. Question papers will be sent by the University through QPD (Question Paper Delivery). University will schedule and conduct ESE at the end of the semester.

- **Format and Implementation:**
  - **Question Paper Design:** Below structure is to be followed to design an End-Semester Examination (ESE) for a theory subject of 70 marks on all 5 units of the syllabus with questions set as per Bloom's Taxonomy guidelines and 14 marks allocated per unit.
  - **Balanced Coverage**: Ensure balanced coverage of all units with questions that assess different cognitive levels of Bloom's Taxonomy: Remember, Understand, Apply, Analyze, Evaluate, and Create. The questions should be structured to cover:
  - **Detailed Scheme for 70 Marks:** Unit-Wise Allocation (14 Marks per Unit- as per the regular structure of mandatory course): Each unit will have a combination of questions designed to assess different cognitive levels. By following this scheme, you can ensure a comprehensive and fair assessment of students' understanding and application of the course material, adhering to Bloom's Taxonomy guidelines for cognitive skills evaluation n.

NEP 2020 Compliant Curriculum Structure

Third & Final year Engineering (2024 Pattern)

Board: Electronics & Telecommunication Engineering

Curriculum Structure for Honor in Cyber Security & Governance

Year & Semester	Course Code	Course Name	Teaching Scheme		Examination Scheme					Credits		
			Theory	Practical	CCE	ESE	Term Work	Oral	Total	Theory	Practical	Total
T.E. - V	HCG 301ETC	Advanced Cryptography and Network Security	3	-	30	70	-	-	100	3	-	3
	HCG 302 ETC	Cybersecurity Fundamentals & Secure Coding Lab		2			25	25	50		1	1
T.E. - VI	HCG 351 ETC	Ethical Hacking & Penetration Testing	3	-	30	70	-	-	100	3	-	3
	HCG 352 ETC	Ethical Hacking & Penetration Testing Lab		2	-	-	25	25	50	-	1	1
B.E. - VII	HCG 401 ETC	Threat Intelligence and Security Operations	3		30	70	-		100	3		3
	HCG 402 ETC	Digital Forensics & Malware Analysis Lab		2	-	-	25	25	50	-	1	1
B.E. - VIII	HCG 451 ETC	Cloud Security, Artificial Intelligence and Digital Governance	3	-	30	70	-	-	100	3	-	3
	HCG 452 ETC	Advanced Security Lab		2	-	-	25	25	50	-	1	1
	HCG 453 ETC	Honors Project	-	4			50	50	100		2	2
Total			**12**	**12**	**120**	**280**	**100**	**100**	**700**	**12**	**6**	**18**

Savitribai Phule Pune University **Honor in Cyber Security & Governance**		
HCG 301 ETC - Advanced Cryptography and Network Security		
Teaching Scheme	**Credits**	**Examination Scheme**
Theory : 03 Hours/Week	03	CCE : 30 Marks End-Semester: 70 Marks

Course Objectives: The course aims to:

1. To understand the mathematical foundations of classical and modern cryptographic algorithms.
2. To study symmetric-key and asymmetric-key cryptosystems including DES, AES, RSA, and ECC.
3. To analyse key management protocols, digital signatures, and public key infrastructure.
4. To apply cryptographic techniques in securing network protocols (IPSec, SSL/TLS, PGP).
5. To understand ethical, legal, and privacy implications in information security.

Course Outcomes: Upon successful completion of this course, students will be able to:

- CO1: Analyse classical and modern cipher techniques to evaluate their security strengths and weaknesses.
- CO2: Implement and compare symmetric encryption algorithms (DES, AES, RC5) for practical scenarios.
- CO3: Apply asymmetric cryptography (RSA, ECC, ElGamal) and key exchange protocols to secure communications.
- CO4: Design PKI solutions using digital certificates, X.509, and Kerberos for enterprise authentication.
- CO5: Configure and verify secure network protocols including IPSec, SSL/TLS, S/MIME, and PGP.
- CO6: Evaluate legal and ethical dimensions of cryptography usage in national and global contexts.

Course Contents

Unit I -Security Fundamentals & Modular Arithmetic (09 Hours)

Security goals (CIA triad + Non-repudiation), Cryptographic attacks, Services and Mechanisms. Modular arithmetic: Euclid's GCD, Extended Euclidean Algorithm, Chinese Remainder Theorem (CRT). Security nomenclature, access control matrix, OS security basics.

Unit II Classical & Symmetric Cryptography (09 Hours)

Classical ciphers: Substitution, Transposition, Stream vs Block ciphers. DES: structure, rounds, S-boxes, key schedule, Triple-DES. AES: Sub Bytes, Shift Rows, Mix Columns, Add Round Key, key expansion. RC5 algorithm. Cryptanalysis: brute force, differential, linear attacks.

Unit III Advanced Encryption and Key Exchange Techniques (09 Hours)

RSA Cryptosystem- Key generation, encryption, decryption, computational efficiency, and security considerations, Diffie–Hellman Key Exchange-Key establishment process, security assumptions, and common attacks/vulnerabilities, ElGamal Public Key Cryptosystem- Key generation, encryption, decryption, and digital signature overview, Elliptic Curve Cryptography (ECC)-Fundamentals of ECC, Elliptic Curve Diffie–Hellman (ECDH), and performance advantages, Symmetric vs Asymmetric Cryptography: Comparative study based on key management, performance, scalability, and applications.

Hybrid Cryptographic Systems: Integration of symmetric and asymmetric techniques for secure communication protocols.

Unit IV Hash Functions, Digital Signatures & PKI (09 Hours)

Cryptographic hash functions: SHA-1, SHA-256, SHA-512, WHIRLPOOL, MD5. Iterated hash functions, collision resistance. Digital Signatures: RSA-based, DSA, ECDSA. Digital Signature Stan-dard (DSS). X.509 certificates, Public Key Infrastructure (PKI), Certificate Authorities (CAs), Kerberos, Needham-Schroeder protocol.

Unit V Network Security Protocols (09 Hours)

IP Security (IPSec): Authentication Header (AH), Encapsulating Security Payload (ESP), IKE, VPN. Web Security: SSL/TLS handshake, HTTPS, HSTS. Email Security: PGP, S/MIME, DKIM, SPF. DNS Security (DNSSEC). Firewalls: packet-filtering, stateful, application-layer. Intrusion Detection Systems (IDS/IPS).

Learning Resources

Text Books:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 8th Ed. (2022), ISBN 978-0-13-511374-1
2. Behrouz A. Forouzan, Cryptography and Network Security, TMH, 2nd Ed., ISBN 978-00-707-0208-0
3. Bruce Schneier, Applied Cryptography, Wiley India, 2nd Ed., ISBN 978-81-265-1368-0
4. CK Shyamala et al., Cryptography and Security, Wiley India, ISBN 978-81-265-2285-9
5. Nina Godbole & Sunit Belapure, Cyber Security, Wiley India, ISBN 978-81-265-2179-1
6. Alfred J. Menezes et al., Handbook of Applied Cryptography, CRC Press (free PDF at cacr.uwaterloo.ca)

Reference Books

1. https://nptel.ac.in/courses/106/105/106105031/ — Cryptography and Network Security (IIT Kharagpur)
2. https://www.coursera.org/learn/crypto — Cryptography I by Dan Boneh, Stanford (Coursera)
3. https://www.cybrary.it/course/cryptography/ — Cryptography Fundamentals (Cybrary)
4. https://www.khanacademy.org/computing/computer-science/cryptography — Khan Academy Cryptography
5. https://csrc.nist.gov/publications — NIST Cryptographic Standards Publications
6. https://www.openssl.org/docs/ — OpenSSL Documentation

Recommended Certifications

1. CompTIA Security+ (SY0-701) — Covers cryptography, PKI, and network security fundamentals
2. EC-Council Certified Encryption Specialist (ECES) — Deep focus on encryption algorithms
3. ISC2 SSCP — Systems Security Certified Practitioner (covers cryptography domain)
4. Google Cybersecurity Certificate (Coursera) — Entry-level, covers basic crypto & security
5. ISACA CISA — Covers information security management and cryptographic controls

Savitribai Phule Pune University **Honor in Cyber Security & Governance**		
HCG 302 ETC - Cybersecurity Fundamentals & Secure Coding Lab		
Teaching Scheme	**Credits**	**Examination Scheme**
Practical : 02 Hours/Week	01	Term Work : 25 Marks Oral 25 Marks

Course Objectives: The course aims to:

1. To provide hands-on experience with cryptographic algorithm implementation.
2. To develop practical skills in network scanning, packet analysis, and vulnerability detection.
3. To practice secure coding techniques to prevent common vulnerabilities (SQLi, buffer overflow).
4. To set up and explore security-focused Linux environments (Kali Linux).
5. To simulate real-world phishing attacks and understand social engineering defences.

Course Outcomes: Upon successful completion of this course, students will be able to:

- CO1: Install and operate Kali Linux for security testing and exploration of built-in tools.
- CO2: Implement DES, AES, RSA, and SHA algorithms using programming languages or Cryptool.
- CO3: Perform network reconnaissance using Nmap/Zenmap to identify hosts, ports, and services.
- CO4: Analyse network traffic and identify security issues using Wireshark.
- CO5: Conduct SQL injection and XSS attacks in a controlled environment using BurpSuite.
- CO6: Simulate phishing campaigns and prepare incident response documentation

List of Laboratory Experiments / Assignments

1. Kali Linux Setup & Tool Exploration : Install Kali Linux (VM/dual-boot), explore bash commands, networking tools (ifconfig, netstat, nmap, curl), and the Kali tools menu structure.
2. Euclidean Algorithm & Modular Arithmetic : Implement Euclid's GCD and Extended Euclidean Algorithm. Compute multiplicative inverses. Verify using manual calculation.
3. DES & AES Implementation : Implement DES and AES encryption/decryption using Python or Java. Test with standard NIST test vectors. Analyse key schedule.
4. RSA Implementation :Generate RSA key pairs, perform encryption and decryption. Demonstrate digital signature and verification.
5. SHA-256 / SHA-512 Hash Functions : Implement SHA-256 using libraries (Python hashlib). Demonstrate hash collision resistance. Compare MD5 vs SHA-256 outputs.
6. Cryptanalysis with Cryp Tool ; Use CrypTool to perform cryptanalysis on symmetric (Caesar, Vi-genère, DES) and asymmetric ciphers. Visualise algorithm steps.
7. Network Scanning with Nmap/Zenmap : Perform host discovery, port scanning (SYN, UDP), OS detection, and service version scanning on a lab network. Export and interpret reports.
8. Packet Analysis with Wireshark : Capture and filter HTTP, HTTPS, DNS, and ARP traffic. Identify credentials in plaintext protocols. Reconstruct TCP streams.

9. SQL Injection with Burp Suite : Perform manual and automated SQL injection on DVWA (Damn Vulnerable Web Application). Use Burp Suite Intruder to brute-force login forms.
10. Phishing Simulation with GoPhish : Set up GoPhish server, design a spear-phishing campaign against lab accounts, capture credentials, and document results. Discussion on defences.
11. Firewall Configuration (iptables/UFW) : Configure Linux iptables rules to allow/deny specific traffic. Test with Nmap and Wireshark. Document rule chains.
12. Ransomware Tabletop Exercise Group exercise: simulate ransomware attack on a fictional enterprise. Identify attack vectors, containment steps, recovery plan, and lessons learned.

Savitribai Phule Pune University **Honor in Cyber Security & Governance**		
HCG 351 ETC- Ethical Hacking and Penetration Testing		
Teaching Scheme	**Credits**	**Examination Scheme**
Theory : 03 Hours/Week	03	CCE : 30 Marks End-Semester: 70 Marks

Course Objectives: The course aims to:

1. To understand the methodology and phases of ethical hacking and penetration testing.
2. To study attack techniques including network exploitation, privilege escalation, and lateral movement.
3. To learn web application vulnerability assessment (OWASP Top 10).
4. To understand attacker tools, tactics, techniques, and procedures (TTPs) using MITRE ATT&CK.
5. To learn professional reporting standards and responsible disclosure practices.

Course Outcomes: Upon successful completion of this course, students will be able to:

- CO1: Execute a structured penetration test following CEH/PTES methodology across all phases.
- CO2: Perform network and system exploitation using Metasploit and manual techniques.
- CO3: Identify and exploit OWASP Top 10 web vulnerabilities in controlled environments.
- CO4: Apply social engineering and phishing attack frameworks ethically.
- CO5: Conduct post-exploitation activities including pivoting, persistence, and data exfiltration concepts.
- CO6: Produce professional penetration testing reports with risk ratings and remediation recommendations.

Course Contents

Unit I - Ethical Penetration Testing and Security Assessment (09 Hours)

Penetration testing frameworks and methodologies- PTES, OWASP Testing Guide, CEH penetration testing methodology, MITRE ATT&CK framework, NIST Penetration Testing Guidelines, penetration testing ethics, and rules of engagement, Phases of penetration testing- Planning and reconnaissance, scanning and enumeration, exploitation, post-exploitation, and report preparation, Passive reconnaissance techniques- Open Source Intelligence (OSINT), Google Dorking, Shodan, Maltego, the Harvester, WHOIS, and DNS enumeration, Active reconnaissance techniques- Network discovery and host enumeration using Nmap, Net discover, and Masscan.

Unit II Scanning, Enumeration & Vulnerability Assessment (09 Hours)

Port scanning techniques: SYN, NULL, FIN, Xmas, UDP scans. Service fingerprinting and OS detection. Vulnerability scanners: Nessus, OpenVAS, Nikto. Banner grabbing, SMB/SNMP/LDAP enumeration. CVE, CVSS scoring, vulnerability prioritisation. Metasploit db_nmap and auxiliary modules.

Unit III System Exploitation & Privilege Escalation (09 Hours)

Exploitation frameworks: Metasploit (msfconsole, meterpreter, payloads, encoders). Buffer overflow exploitation: stack-based, heap-based. Shell code, NOP sleds, return-oriented programming (ROP) basics. Privilege escalation: Linux (SUID, sudo misconfigs, kernel exploits), Windows (token impersonation, UAC bypass). Pass-the-Hash, Pass-the-Ticket. Credential dumping with Mimikatz.

Unit IV Web Application Penetration Testing (09 Hours)

OWASP Top 10 (2021): Injection, Broken Auth, XSS, IDOR, SSRF, Security Misconfig, Vulnerable Components, etc. Tools: BurpSuite Pro, OWASP ZAP, SQLMap, Nikto. Cross-Site Scripting (reflected, stored, DOM). CSRF, Clickjacking, XXE, Directory Traversal, File Upload vulnerabilities. API security testing basics.

Unit V Wireless, Social Engineering & Post-Exploitation (09 Hours)

Wireless attacks: WEP/WPA2 cracking with Aircrack-ng, Evil Twin AP, PMKID attack. Social engineering: phishing, vishing, smishing, pretexting frameworks (SET – Social Engineering Toolkit). Post-exploitation: persistence mechanisms, lateral movement, pivoting with proxychains, data exfiltration, covering tracks (anti-forensics). C2 frameworks overview (Cobalt Strike concepts).

Learning Resources

Text Books:

1. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014, ISBN 978-1-59327-564-8
2. Peter Kim, The Hacker Playbook 3: Practical Guide to Penetration Testing, Secure Planet, 2018
3. Dafydd Stuttard & Marcus Pinto, The Web Application Hacker's Handbook, 2nd Ed., Wiley, ISBN 978-1-118-02647-2
4. Jon Erickson, Hacking: The Art of Exploitation, 2nd Ed., No Starch Press, ISBN 978-1-59327-144-2
5. OccupyTheWeb, Linux Basics for Hackers, No Starch Press, 2018, ISBN 978-1-59327-855-7
6. Gerard Johansen, Digital Forensics and Incident Response, 3rd Ed., Packt Publishing, 2022

Online Resources

1. https://tryhackme.com — Guided cybersecurity labs and learning paths (free + paid)
2. https://www.hackthebox.com — Penetration testing practice machines
3. https://portswigger.net/web-security — PortSwigger Web Security Academy (free, OWASP topics)
4. https://owasp.org/www-project-top-ten/ — OWASP Top 10
5. https://attack.mitre.org — MITRE ATT&CK Framework
6. https://nptel.ac.in/courses/106/105/106105217/ — Ethical Hacking (IIT Kharagpur, NPTEL)
7. https://www.offensive-security.com/metasploit-unleashed/ — Metasploit Unleashed (free)

Recommended Certifications

1. EC-Council CEH (Certified Ethical Hacker) — Industry standard for ethical hacking
2. Offensive Security OSCP (PWK + Exam) — Highly respected hands-on pen testing cert
3. CompTIA PenTest+ — Vendor-neutral penetration testing certification
4. eJPT (eLearnSecurity Junior Penetration Tester) — Entry-level, fully practical
5. TCM Security PNPT (Practical Network Penetration Tester) — Practical, report-based exam
6. Bug Bounty certifications: HackerOne, Bugcrowd platform training

Savitribai Phule Pune University **Honor Course in Cyber Security & Governance**		
HCG 352 ETC- Ethical Hacking & Penetration Testing Lab		
Teaching Scheme	**Credits**	**Examination Scheme**
Practical : 02 Hours/Week	01	Term Work: 25 Marks Oral: 25 Marks

Course Objectives:

1. To gain hands-on experience with reconnaissance and scanning tools.
2. To perform exploitation on intentionally vulnerable systems (VMs).
3. To practice web application penetration testing using DVWA, BWAPP, and Juice Shop.
4. To develop skills in wireless security assessment and social engineering simulations.
5. To write professional penetration test reports.

Course Outcomes (COs):

- CO1: Conduct full reconnaissance (passive + active) on target systems and document findings.
- CO2: Use Meta sploit to exploit known CVEs on vulnerable VMs and gain meterpreter sessions.
- CO3: Exploit all OWASP Top 10 vulnerabilities on DVWA and OWASP Juice Shop.
- CO4: Crack WEP/WPA2 keys using Air crack-ng in a controlled wireless lab environment.
- CO5: Perform privilege escalation on Linux and Windows VMs.
- CO6: Produce structured penetration test reports with CVSS-rated findings.

List of Assignment /Experiments

1. Environment Setup: Kali + Metasploitable + DVWA Configure a lab with Kali Linux attacker, Metasploitable2/3, and DVWA. Verify network connectivity and tool availability.
2. OSINT & Passive Reconnaissance Use theHarvester, Maltego CE, Shodan, and WHOIS/DNS tools to gather intelligence on a provided domain. Document findings.
3. Nmap Advanced Scanning & Reporting Perform SYN, version, OS, and script scans (-sV, -O, -sC) on Metasploitable. Export XML results and parse with Metasploit db_import.
4. Vulnerability Scanning with OpenVAS/Nessus Run a full vulnerability scan against lab VMs. Analyse results, filter critical CVEs, and prepare a vulnerability assessment report.
5. Metasploit Exploitation Exploit vsftpd 2.3.4 backdoor and UnrealIRCd on Metasploitable2. Establish meterpreter session, capture screenshots, and dump hashes.
6. Buffer Overflow Exploitation (Linux) Exploit a custom vulnerable C program with a stack-based buffer overflow. Craft shellcode payload, bypass NX with ret2libc.
7. SQL Injection – Manual & SQLMap Perform blind, error-based, and union-based SQLi on DVWA. Automate with SQLMap to dump database contents.

8. XSS & CSRF Exploitation Exploit reflected, stored, and DOM XSS on DVWA. Craft CSRF attack PoC. Test CSP headers using Burp Suite.
9. Privilege Escalation (Linux & Windows) Exploit SUID binaries, cron jobs, and sudo misconfigurations on a Linux VM. Perform token impersonation on Windows (VM).
10. Wireless Security: WPA2 Cracking Use Air crack-ng suite (airodump-ng, aireplay-ng) to capture WPA2 handshake on a lab AP and crack with a dictionary attack.
11. Social Engineering Toolkit (SET) Use SET to create a phishing page cloning a popular site. Capture credentials. Discuss defenses: MFA, awareness training.
12. Full Penetration Test + Report Mini CTF on a provided vulnerable VM. Students complete all phases (recon exploit post-exploit) and submit a professional penetration test report.

Savitribai Phule Pune University **Honor in Cyber Security & Governance**		
HCG 401 ETC- Threat Intelligence and Security Operations		
Teaching Scheme	**Credits**	**Examination Scheme**
Theory : 03 Hours/Week	03	CCE: 30 Marks End-Semester: 70 Marks

Course Objectives: The course aims to:

1. To understand the structure, tools, and workflows of a Security Operations Centre (SOC).
2. To study SIEM platforms and log management for threat detection.
3. To analyse cyber threat intelligence (CTI) methodologies and intelligence lifecycle.
4. To develop incident response capabilities using established frameworks (NIST, SANS).
5. To apply AI/ML-driven approaches for anomaly detection and automated threat hunting.

Course Outcomes: Upon successful completion of this course, students will be able to:

- CO1: Describe SOC tiers, roles, KPIs, and operational processes including shift handover and escalation.
- CO2: Configure and use SIEM tools (Splunk/ELK) to correlate logs and trigger alerts for security events.
- CO3: Develop threat intelligence reports using STIX/TAXII, MITRE ATT&CK, and CTI frameworks.
- CO4: Execute incident response plans for ransomware, APT, phishing, and insider threat scenarios.
- CO5: Apply threat hunting methodologies using IOC/TTP-based approaches on SIEM data.
- CO6: Evaluate AI/ML-based security tools for anomaly detection, UEBA, and SOAR automation.

Course Contents

Unit I - Security Operations Centre (SOC) Fundamentals (09 Hours)

SOC types (in-house, MSSP, hybrid), tiers (L1/L2/L3), roles and responsibilities. SOC metrics: MTTD, MTTR, false positive rate, alert fatigue. Security event vs security incident. Log sources: Windows Event Logs, Syslog, NetFlow, DNS logs, proxy logs. Log management and SIEM architecture. Ticketing systems and escalation procedures.

Unit II SIEM, Log Analysis & Threat Detection (09 Hours)

SIEM platforms: Splunk, IBM QRadar, Microsoft Sentinel, ELK Stack (Elasticsearch, Logstash, Kibana). Log correlation rules and use-case development. Detection engineering: Sigma rules, YARA rules. Network traffic analysis: baseline establishment, anomaly detection. Use cases: brute force, lateral movement, data exfiltration, C2 beaconing detection. Dashboard and reporting.

Unit III Cyber Threat Intelligence (CTI) (09 Hours)

CTI lifecycle: planning, collection, processing, analysis, dissemination, feedback. Intelligence types: strategic, operational, tactical, technical. CTI frameworks: MITRE ATT&CK, Cyber Kill Chain, Diamond Model, STIX 2.1/TAXII 2.1. Threat actor profiling: APT groups, TTPs, motivations. Dark web intelligence and OSINT for CTI. CTI platforms: MISP, Open CTI, Threat Connect. IOC management.

Unit IV Incident Response & Digital Forensics Basics (09 Hours)

NIST SP 800-61 and SANS IR methodology: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned (PICERL). Playbooks for: ransomware, phishing, insider threat, DDoS, APT. Evidence collection principles, chain of custody. Memory forensics with Volatility: process listing, network connections, artefact extraction. Disk forensics: timeline analysis, deleted file recovery. Legal admissibility.

Unit V Threat Hunting Methodologies and Security Analytic (09 Hours)

Threat hunting frameworks and maturity models-Threat Hunting Maturity Model (HMM), threat hunting lifecycle, and hypothesis-driven hunting, Threat hunting approaches-IOC-based, TTP-based, analytics-driven, and behavior-based hunting, Threat hunting Tools-Velociraptor, OS Query, Sysmon (Windows Event Logs), and Windows Defender Advanced Hunting. Lateral movement and persistence Detection-Techniques for identifying lateral movement, persistence mechanisms, and privilege escalation indicators, Cloud threat Hunting using AWS Cloud Trail, Azure Monitor Logs, and Google Cloud Logging. Threat hunting reporting-Documentation of findings, reporting, feedback loop for detection engineering, and Purple Teaming concepts and collaborative security validation.

Learning Resources

Text Books:

1. Chris Sanders & Jason Smith, Applied Network Security Monitoring, Syngress, 2013, ISBN 978-0-12-417208-1
2. Scott J. Roberts & Rebekah Brown, Intelligence-Driven Incident Response, O'Reilly, 2017, ISBN 978-1-491-93470-9
3. Bruce Nikkel, Practical Linux Forensics, No Starch Press, 2021, ISBN 978-1-71850-196-1
4. Joseph Muniz et al., The Modern Security Operations Center, Pearson IT, 2021, ISBN 978-0-13-579914-5
5. David J. Bianco & Robert M. Lee, The Practice of Network Security Monitoring, No Starch Press
6. Valentina Costa-Gazcón, Practical Threat Intelligence and Data-Driven Threat Hunting, Packt, 2021

Online Resources & URLs

1. https://attack.mitre.org — MITRE ATT&CK for threat intelligence and hunting
2. https://www.splunk.com/en_us/training.html — Splunk Free Training (SIEM)
3. https://tryhackme.com/path/outline/soclevel1 — SOC Level 1 Path (TryHackMe)
4. https://www.cyberdefenders.org — Blue team CTF challenges
5. https://blueteamlabs.online — Blue team lab practice
6. https://www.misp-project.org — MISP Threat Intelligence Platform
7. https://docs.velociraptor.app — Velociraptor threat hunting tool docs
8. https://nptel.ac.in/courses/106/105/106105244/ — Introduction to Cybersecurity (NPTEL)

Recommended Certifications

1. CompTIA CySA+ (CS0-003) — Cybersecurity Analyst, covers SOC and threat hunting
2. Splunk Core Certified User / Power User — SIEM-specific certification

3. Microsoft SC-200: Security Operations Analyst — Azure Sentinel and Microsoft Defender.EC-Council C|TIA (Certified Threat Intelligence Analyst) — CTI-focused
4. SANS GCIA (GIAC Certified Intrusion Analyst) — Deep network analysis
5. Blue Team Labs Online Certification — Practical, scenario-based
6. IBM QRadar SIEM Foundation (Coursera) — Vendor-specific SIEM

Savitribai Phule Pune University **Honor Course in Cyber Security & Governance**		
HCG 402 ETC - Digital Forensics & Malware Analysis Lab		
Teaching Scheme	**Credits**	**Examination Scheme**
Practical : 02 Hours/Week	01	Term Work: 25 Marks ,Oral : 25 Marks

Course Objectives:

- To develop practical skills in memory and disk forensics using industry tools.
- To perform static and dynamic malware analysis in isolated sandbox environments.
- To conduct network forensics by analysing captured packet data for evidence.
- To practice SOC workflows including alert triage, escalation, and incident documentation.
- To create forensically sound reports suitable for legal proceedings.

Course Outcomes (COs):

- CO1: Perform memory forensics using Volatility to extract processes, network artefacts, and malware.
- CO2: Conduct disk forensics on forensic images using Autopsy/FTK to recover artefacts.
- CO3: Analyse malware samples statically (strings, PE analysis) and dynamically (sandbox, behaviour).
- CO4: Investigate network forensics cases using Wireshark and Network Miner.
- CO5: Triage SIEM alerts and execute IR playbooks for common attack scenarios.
- CO6: Produce forensically sound investigation reports with chain-of-custody documentation.

List of Laboratory Experiments / Assignments

1. Forensics Lab Setup Install and configure forensics workstation: Autopsy, Volatility 3, FTK Imager, REMnux, FlareVM, SIFT Workstation. Configure isolated lab network.
2. Disk Imaging & Evidence Preservation Create forensic images using FTK Imager (E01 format). Verify MD5/SHA hash integrity. Document chain of custody. Mount read-only with write blocker.
3. File System Forensics with Autopsy Investigate a provided disk image for deleted files, browser history, recent documents, USB artefacts, and timeline events using Autopsy.
4. Windows Registry & Log Forensics Analyse Windows registry hives (SAM, SYSTEM, SOFTWARE) for user accounts, installed programs, USB devices, and run keys using Reg Ripper.
5. Memory Forensics with Volatility 3 Analyse a memory dump: list processes (pslist, pstree), network connections (netstat), find injected code (malfind), extract strings and cmd lines.
6. Static Malware Analysis Analyse a provided malware sample: compute hashes, run through VirusTotal, extract strings, analyse PE headers with PE Studio, identify packed/obfuscated sections.
7. Dynamic Malware Analysis (Sandbox) Execute malware in Cuckoo Sandbox or Any.run. Observe file system changes, registry modifications, network callbacks, and process injection. Document IOCs.
8. Network Forensics with Wireshark & Network Miner Analyse a provided PCAP file. Identify C2 communication patterns, data exfiltration, lateral movement, and malware download events.

9. SIEM Alert Triage (Splunk/ELK) Investigate pre-loaded log data in Splunk. Identify brute force, successful compromise, and lateral movement. Write correlation rules and document investigation.

10. Ransomware Incident Response Simulate a ransomware incident: identify patient zero, map infection spread, recover shadow copies, document remediation steps, and produce an incident report.

11. CTF — Blue Team Challenge Solve a provided CTF challenge set involving forensics artefacts, PCAP analysis, memory images, and log analysis. Submit flags and write-up.

12. Forensic Investigation Report Complete a full forensic investigation of a provided scenario. Submit a professional report covering scope, methodology, findings, evidence, and recommendations.

Savitribai Phule Pune University **Honor in Cyber Security & Governance**		
HCG 451 ETC - Cloud Security, Artificial Intelligence and Digital Governance		
Teaching Scheme	**Credits**	**Examination Scheme**
Theory : 03 Hours/Week	03	CCE : 30 Marks End-Semester: 70 Marks

Course Objectives: The course aims to:

1. To understand cloud security architecture, shared responsibility, and major CSP security services.
2. To study AI/ML-driven security mechanisms and adversarial threats against AI systems.
3. To explore DevSecOps practices and security integration in CI/CD pipelines.
4. To understand governance, risk, and compliance (GRC) frameworks for cybersecurity.
5. To analyse cyber law, regulations, and compliance requirements at national and international levels.

Course Outcomes: Upon successful completion of this course, students will be able to:

- CO1: Design cloud security architectures using native security services of AWS, Azure, and GCP.
- CO2: Apply AI/ML techniques for intrusion detection, malware classification, and fraud detection.
- CO3: Identify and mitigate adversarial attacks against machine learning models (evasion, poisoning).
- CO4: Implement DevSecOps practices: SAST, DAST, container security, and IaC security scanning.
- CO5: Evaluate GRC frameworks (ISO 27001, NIST CSF, GDPR, SOC2) and apply risk assessment methods.
- CO6: Analyse cyber law provisions (IT Act, GDPR, CCPA, DPDPA) and their implications for engineering practice.

Course Contents

Unit I - Cloud Security Architecture (09 Hours)

Cloud service models (IaaS, PaaS, SaaS) and shared responsibility model, cloud deployment models, Cloud security threats-misconfigurations, insecure APIs, excessive permissions, cloud hopping, data breaches, identity and access risks, AWS security services-IAM, Security Groups, Cloud Trail, Guard Duty, Macie, KMS, AWS Config, Azure security services- Azure AD, Defender for Cloud, Microsoft Sentinel, Key Vault, Azure Policy, Google Cloud Platform (GCP) security- Security Command Center, VPC Service Controls, Cloud IAM, Cloud security solutions- CASB, CSPM, CWPP, Cloud Workload Security, Zero Trust architecture in cloud environments, cloud compliance and governance.

Unit II AI & Machine Learning for Cybersecurity (09 Hours)

ML pipeline for security: feature engineering, model training, evaluation. Supervised: malware classification (Random Forest, SVM, deep learning). Unsupervised: anomaly detection (Isolation Forest, Auto encoders). NLP for log analysis and phishing detection. Graph-based approaches for fraud and APT detection. Federated learning for privacy-preserving threat intelligence sharing. AI-powered tools: Darktrace, Vectra, CrowdStrike Falcon.

Unit III Adversarial AI & AI Security (09 Hours)

Adversarial ML: evasion attacks (FGSM, PGD, CW), poisoning attacks, model inversion, membership inference. Defences: adversarial training, input sanitisation, differential privacy, model distillation. Deepfakes and synthetic media threats. LLM security: prompt injection, jailbreaking, data poisoning in RAG systems. AI governance: NIST AI RMF, EU AI Act implications. Securing AI pipelines and MLOps.

Unit IV DevSecOps & Secure Software Development (09 Hours)

DevSecOps culture and shift-left security. Secure SDLC (SSDLC): threat modelling (STRIDE, DREAD), secure design patterns. Static Application Security Testing (SAST): Semgrep, SonarQube, Checkmarx. Dynamic Application Security Testing (DAST): OWASP ZAP, BurpSuite. Software Composition Analysis (SCA): OWASP Dependency-Check, Snyk. Container security: Docker bench, Trivy, Kubernetes security. Infrastructure as Code (IaC) security: Checkov, Terrascan. CI/CD pipeline security: GitHub Actions secrets management, SBOM.

Unit V Governance, Risk & Compliance (GRC) (09 Hours)

GRC frameworks: ISO/IEC 27001/27002, NIST Cybersecurity Framework (CSF 2.0), COBIT 5, CIS Controls v8. Risk management: risk identification, qualitative and quantitative assessment, risk treatment (accept, mitigate, transfer, avoid). Security auditing and continuous monitoring. Compliance standards: PCI-DSS v4, HIPAA, SOC 2 Type II, FedRAMP. Vendor risk management and third-party assessment. BCDR: BCP, DRP, RTO, RPO.

Learning Resources

Text Books:

1. Ric Messier, Cloud Security Concepts, Technology and Architecture, McGraw-Hill, 2023
2. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, CRC Press, 2021
3. Kim Wuyts et al., Threat Modelling: Designing for Security, Wiley, 2024
4. Glenn Kessler, The Cloud Security Handbook, BCS Publishing, 2022
5. Punit Bhatia, GDPR and Data Protection: Practical Guide, Independently Published
6. Pavan Duggal, Cyber Law: The Indian Perspective, Saakshar Law Publications, Latest Edition
7. Ian Goodfellow et al., Deep Learning (free at deeplearningbook.org) — for adversarial ML chapters

Online Resources & URLs

1. https://aws.amazon.com/training/learn-about/security/ — AWS Security Training (free digital)
2. https://learn.microsoft.com/en-us/certifications/sc-900/ — Microsoft Security Fundamentals
3. https://cloud.google.com/learn/training/security — Google Cloud Security Training
4. https://owasp.org/www-project-devsecops-guideline/ — OWASP DevSecOps Guideline
5. https://www.nist.gov/cyberframework — NIST CSF 2.0
6. https://meity.gov.in/content/information-technology-act — India IT Act (MeitY)
7. https://nptel.ac.in/courses/106/105/106105245/ — Cloud Computing Security (NPTEL)
8. https://adversarial-ml-tutorial.org — Adversarial ML Tutorial (Zico Kolter & Aleksander Madry)

Recommended Certifications

1. AWS Certified Security – Specialty (SCS-C02) — Cloud security in AWS environment
2. Microsoft SC-900 + SC-300 (Identity & Access) + SC-200 — Cloud security pathway
3. Google Professional Cloud Security Engineer — GCP-specific security cert
4. CompTIA Cloud+ (CV0-004) — Vendor-neutral cloud security
5. ISACA CRISC (Certified in Risk and Information Systems Control) — GRC-focused
6. ISC2 CCSP (Certified Cloud Security Professional) — Premier cloud security cert
7. CEH (AI/Cloud modules) or eJPT Cloud path — Practical cloud pentesting
8. GDPR Practitioner Certificate (BCS/IAPP CIPM/CIPP-E) — Data protection & cyber law

Savitribai Phule Pune University **Honor in Cyber Security & Governance**		
HCG 452 ETC - Advanced Security Lab		
Teaching Scheme	**Credits**	**Examination Scheme**
Practical : 02 Hours/Week	01	Term Work : 25 Marks Oral: 25 Marks

Course Objectives: The course aims to:

1. To integrate knowledge from all Honors semesters into a comprehensive capstone security project.
2. To provide hands-on experience with cloud-native security tools and services.
3. To apply AI/ML models for real-world security problem solving.
4. To implement DevSecOps pipelines with automated security gates.
5. To develop presentation and documentation skills for professional security deliverables.

Course Outcomes: Upon successful completion of this course, students will be able to:

- **• CO1: Design and implement a cloud security architecture on AWS/Azure with IAM, logging, and monitoring.**
- **• CO2: Build and evaluate an ML-based intrusion detection or malware classification model.**
- **• CO3: Implement a DevSecOps CI/CD pipeline with SAST, DAST, and container scanning.**
- **• CO4: Conduct a cloud penetration test on a provided vulnerable cloud environment (CloudGoat/AzureGoat).**
- **• CO5: Develop an adversarial ML attack and corresponding defence mechanism.**
- **• CO6: Present a capstone security project with full documentation, risk assessment, and live demo.**

List of Laboratory Experiments / Assignments

1. AWS/Azure Security Services Exploration Configure IAM roles/policies, enable CloudTrail, GuardDuty, and Security Hub (AWS) or Defender for Cloud (Azure). Generate and investigate findings.
2. Container Security with Docker & Trivy Build a Dockerised web application. Scan image with Trivy for CVEs. Fix vulnerabilities, update Dockerfile. Compare before/after scan reports.
3. SAST with SonarQube / Semgrep Run SAST analysis on a provided Python/Java vulnerable application. Interpret findings, fix critical issues, and verify resolution with re-scan.
4. DevSecOps CI/CD Pipeline Build a GitHub Actions pipeline with integrated Semgrep SAST, OWASP Dependency-Check SCA, and Trivy container scan. Pipeline fails on critical findings.
5. Cloud Penetration Testing (CloudGoat) Exploit intentionally vulnerable AWS environment using Rhino Security Labs CloudGoat. Document attack paths, escalation, and lateral movement.
6. ML-Based Intrusion Detection System Train a Random Forest / Neural Network on NSL-KDD or CIC-IDS2018 dataset. Achieve >95% accuracy. Visualise feature importance and confusion matrix.

7. Adversarial Attack on ML Model Implement FGSM adversarial attack on a malware classifier. Demonstrate evasion. Implement adversarial training as defence. Measure accuracy drop.
8. Phishing URL Detection with NLP Build an NLP-based phishing URL detector using TF-IDF + Logistic Regression and BERT fine-tuning. Compare accuracy, precision, recall, F1-score.
9. GRC Risk Assessment Simulation Perform a risk assessment for a provided organisation scenario using NIST CSF. Identify assets, threats, vulnerabilities. Produce a risk register and treatment plan.
10. DPDPA / GDPR Compliance Audit Audit a provided web application design against DPDPA 2023 / GDPR principles. Identify violations, suggest remediation, and draft a compliance report.

Savitribai Phule Pune University		
HCG 453 ETC - Honors Projects		
Teaching Scheme	**Credits**	**Examination Scheme**
Theory : 04 Hours/Week	02	Term Work: 50 Marks Oral : 50 Marks

The Honors Project shall enable students to:

- Apply Cyber Security concepts to real-world problems.
- Develop research, design, implementation, and validation skills.
- Address emerging cyber threats and security challenges.
- Promote innovation, entrepreneurship, and product development.
- Encourage industry-sponsored and research-oriented projects.
- Publish research findings, patents, software tools, or security frameworks.
- Enhance employability in Cyber Security domains.

Phases of Honors Project

1. **Capstone Project – Phase 1** (Design) Students submit project proposal: problem statement, objectives, architecture diagram, tools, dataset/environment, expected outcomes, and timeline.
2. **Capstone Project – Phase 2** (Implementation + Presentation) Final demonstration of capstone project. Viva voce conducted by panel. Submission: code, report, demo video, and presentation slides.

Types of Projects

The project shall belong to one or more of the following categories:

- A. Research Projects:
  - Threat Detection Models
  - Malware Analysis
  - Security Analytics
  - AI for Cyber Security

  - Quantum-safe Cryptography
- B. Development Projects
  - Security Tools
  - Intrusion Detection Systems
  - Vulnerability Scanners
  - SIEM Dashboards
  - Secure Application
- C. Industry Projects
  - Industry-defined security problems
  - Security compliance automation
  - Cloud security implementation
- D. Product Development Projects
  - Commercially viable security products
  - Start-up oriented cyber solutions
  - E. Social Impact Projects
  - Cyber awareness platforms
  - Security solutions for rural and government sectors