

Branch Name:	IMCA
Program Code:	CS301
Course Title:	Cyber security Practical
Course Code:	1CS3010702P
Pre-requisite Course:	Computer Networks, Operating Systems, Programming in C/C++ or Java, Discrete Mathematics, Database Management Systems. Students need basic knowledge of network protocols, OS concepts, and programming.

Course Objective:

1. Explain security fundamentals including CIA triad, threat models like STRIDE/DREAD, and risks in cloud/IoT/social media.
2. Implement classical/symmetric/asymmetric ciphers (Caesar, AES, RSA), hashing (SHA, HMAC), and PKI/digital signatures.
3. Deploy and analyze network defenses like firewalls, IDS/IPS (Snort), SSL/TLS, IPsec VPNs, and email security (PGP/SMIME).
4. Apply access controls (RBAC/ABAC), authentication (MFA), malware analysis, and policies including BCP/DRP and wireless security.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
-	-	3	3	-	-	25	25	50

List of Experiments:

Note: The experiment list provided beneath is for reference only. The course teacher may Change/formulate it as per his/her methodology and requirement.

Sr. No	Practical Experiments
1.	Capture live network traffic and map protocols to OSI/TCP-IP layers.
2.	Generate and capture DDoS SYN flood traffic.
3.	Scan a target machine for open ports/services/vulnerabilities.
4	Create and host phishing login form locally.
5	Encrypt/decrypt files using DES.
6	Demonstrate key-dependent encryption outputs.
7	Compare ECB vs CBC block cipher patterns.
8	Encrypt a PDF file using different Block Cipher modes (AES)
9	Complete RSA encrypt/decrypt cycle.
10	Configure inbound port blocking rules.
11	Deploy stateful firewall rules on Ubuntu.

12	Detect and analyze port scan in Wireshark.
13	Implement Linux DAC file permissions.
14	Simulate ARP spoofing on local network.
15	Exploit SQLi on DVWA vulnerable web app.

Text Books:

- 1 "Cryptography and Network Security: Principles and Practice" by William Stallings, Pearson, 7th Ed. (Ch. on OpenSSL examples, Wireshark labs)
- 2 "Cryptography and Network Security" by Forouzan & Mukhopadhyay, McGraw-Hill, 3rd Ed. (Tool demos, firewall configs) (2015).
- 3 "Network Security and Cryptography" by Bernard Menezes, Cengage, 1st Ed. (CLI crypto exercises) (2010).

Reference Books:

1. "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, Mike Speciner, Pearson Education, 2nd Edition (2002)
2. "Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar, Jan Pelzl, Springer, 1st Edition (2010)
3. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard, Marcus Pinto, Wiley, 2nd Edition (2011)
4. "Network Security Bible" by Eric Cole (Editor), Wiley, 2nd Edition (2009)

List of Open Source Software/learning website:

- [Wireshark.org](https://www.wireshark.org/)
- [Nmap.org](https://nmap.org/)
- <https://www.cybrary.it/>
- <https://owasp.org/>
- https://cryptohack.org
- <https://www.hackthebox.com/>
- <https://tryhackme.com/>

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Describe CIA triad, OSI/TCP-IP models, threats (malware/phishing/DDoS), risk models (STRIDE/DREAD), and legal aspects (IT Act/GDPR).	2. Understand
CLO2	Implement and compare ciphers (Caesar/Vigenère/AES/RSA), hash functions (SHA/HMAC), and PKI/digital signatures.	3. Apply 4. Analyze
CLO3	Configure firewalls, IDS/IPS (Snort), SSL/TLS handshakes, IPsec VPNs, and secure email (PGP/SMIME/DNSSEC).	3. Apply
CLO4	Design access controls (RBAC/ABAC), authentication (MFA), analyze malware/ransomware, and develop security policies/BCP/DRP.	5. Evaluate
CLO5	Analyze security threats, vulnerabilities and cyber-attack patterns in modern systems.	4. Analyze
CLO6	Design integrated security solutions for protecting organizational networks and data.	6. Create

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO11	PO12	PSO1	PSO2
CLO1	H	M	M	-	-	-	-	-	-	M	H	L	M	L
CLO2	H	H	M	M	H	-	-	-	-	M	-	L	H	M
CLO3	H	M	H	M	M	-	-	-	-	M	-	-	M	M
CLO4	H	M	M	H	M	M	-	-	-	-	M	L	H	H
CLO5	M	H	M	H	M	M	-	-	-	M	-	L	M	M
CLO6	H	H	H	H	H	M	-	-	M	M	M	L	H	H

H:High, M:Medium, L:Low