Revised Syllabus

DISCIPLINE SPECIFIC ELECTIVE COURSE : Cyber Security

Credit Contribution, Eligibility, Pre-requisites of the Course

Course title and Code	Credits	Credit distribution of the course			Eligibility Criteria	Pre-requisite of the course(if any)
		Lecture	Tutorial	Practical/ practice		
Cyber Security	4	3	0	1	Pass in Class XII	None

Learning Objectives

The course is designed to develop awareness and foundational knowledge in Cyber Security, enabling students to understand the basic architecture of cyber space and the techniques used to protect digital environments. It aims to equip students with the skills necessary to recognize threats, analyze vulnerabilities and implement basic protective measures.

Learning Outcomes

On successful completion of the course, students will be able to:

- Understand the fundamentals of cyber space and cybersecurity.
- Identify the vulnerabilities and potential security gaps across the various components of the digital ecosystem.
- Analyze and classify cyber threats like malware and intrusion attempts, using appropriate tools.
- Utilize cybersecurity tools and best practices to safeguard personal and institutional digital assets.

Unit 1 Introduction (12 Hours)

ref 1,2

Importance of Cyber Security, what security is and isn't, roles and responsibilities of cybersecurity professionals, types of hackers (black hats, white hats, and their types). Understanding threats and vulnerabilities, Advanced Persistent Threats(APT), humans as the point of vulnerability. Social engineering attacks (Phishing, Vishing and other non-email Phishing attacks).

Unit 2 Attack targets on the internet (9 Hours) ref 1

Working on the Internet, Attack methodology: Reconnaissance, Weaponization, Delivery, Exploitation and Installation, Command and control, Attack on objectives. Black Hats methodologies to find victims, how to hide from attackers

Unit 3 Phishing Tactics and Malware Infections (12 Hours) ref 1

Protection against Phishing, How Black Hats trick you with URLs, Typosquatting, Complex URLs and redirects, Modifying DNS records, Hoaxes, Why Black Hats love phishing and how to avoid phishing. Definition and types of Malware (Viruses, Worms, Trojans, Ransomware, Spyware and Adware), Rootkits and Bootkits, Polymorphic, Deployment and defense against Malware.

Unit 4 Password Thefts and Account Access Tricks (12 Hours) ref 1

Authentication, Types of Authentication, Multi-Factor Authentication, Authorization, Mandatory Access Control, Rule-Based Access Control, Role-Based Access Control, Attribute-Based Access Control, Discretionary Access Control, Auditing, Indicators of attack.

Essential/ Recommended Readings

1. How Cybersecurity Really Works. A Hands-on Guide for Total Beginners by Sam Grubb. No Starch Press, San Francisco, 2021.
2. Cybersecurity and Cyberwar: what everyone needs to know by P.W. Singer and Allan Friedman, Oxford University Press, United States of America, 2014.

Additional References:

1. Information Security Education & Awareness https://isea.gov.in/
2. Indian Computer Emergency Response Team https://www.cert-in.org.in/
3. Cyber Swachhta Kendra, https://www.csk.gov.in/
4. A Handbook for Preventing Computer Frauds and Cyber Crimes by Gaurav Gupta and Garima Gupta, Vilvam Publications Pvt Ltd., New Delhi, 2021.

Practical list:

1. Install and set up VMware on your machines. (4 hours)
2. Execute network commands: ipconfig, ifconfig, ping, tracert to find the IP address of your machine, to test if a machine is connected and is reachable and find the route to the destination. (2 hours)
3. Use Shodan tool to find vulnerabilities in the websites and detect their open ports. (4 hours)
4. Use VirusTotal to scan and analyse malicious files and URLs to detect malware. (4 hours)
5. Use MX toolbox to analyse phishing emails and email header analysis. (2 hours)

6. Do account protection settings in any operating system (Windows 10 /MacOS/Linux) (6 hours)
7. Use USBDeview to track USB usage on your machine for currently connected USB devices as well as previously connected devices. (2 hours)
8. Explore the following three government-backed portals for various purposes: (6 hours)
   a. https://cybercrime.gov.in - for reporting cybercrime
   b. https://stopncii.org/ - if someone is threatening to share intimate images
   c. https://sancharsaathi.gov.in/ - Block your lost/stolen mobile handset, know mobile connections in your name, **chakshu**—report suspected fraudulent communication, and know the genuineness of your mobile handset.