3IT81: CYBER SECURITY
CREDITS –3(LTP: 3,0,0)

Course Objective:
To learn importance of securing applications and to make aware about Cyber Security Cyber law, Cyber Crime.

Teaching and Assessment Scheme:

Teaching Scheme (Hours per Week)			Credits	Assessment Scheme				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE	CE	ESE	CE	
3	0	0	3	60	40	-	-	100

Course Contents:

Unit No.	Topics	Teaching Hours
1	**Introduction:** A brief history of the internet,Application security, Data security, Security technology-Firewall and VPNs, Access control, Security threats, Malicious software, Network and denial of services attack, Electronic payment system, E- Cash, Credit/Debit cards, Digital signature.	5
2	**Cyber Security And Cyber Crime Investigation:** Introduction to cyber security, Introduction to cyberspace, Survey of malware and its existence, Definition of security hole, Security patch, Viruses, Worms, Trojan horses, Social engineering, Avoiding Malwares, Spyware, Keyboard loggers, Ransomware, E-Mail and SPAM, Spoofing, Spammer's tools.	7
3	**Vulnerability Scanning:** Introduction to vulnerability, Vulnerability scanning, Different web vulnerabilities, Open Port and Service Id, Banner disclosure, Traffic probe, Web application testing, Penetration testing.	7
4	**Port Scanning:** Understanding port and services tools, Port scanning tool- Nmap, Netcat, Network sniffers and injection tools, Wireshark.	5
5	**Network Defense Tools:** Firewall basics, Packet filter Vs firewall, How a firewall protects a network, Packet characteristic to filter, Stateless Vs Stateful firewalls, Network address translation (NAT) and port forwarding, The basic of virtual private networks.	6
6	**Web Application Tools:** Scanning for web vulnerabilities tools: Nikto and W3af, Web application testing using DVWA, Manual SQL injection scanning using DVWA, Password Cracking and Brute-Force tools, Wi-Fi passwords cracking WEP & WAP/WAP2 with Aircrack-ng.	8

Unit No.	Topics	Teaching Hours
7	**Introduction to Cyber Crime:** Cyber Crimes, Types of cybercrime, Hacking, Attack vectors, Cyberspace, Traditional problems Associated with Computer Crime, Introduction to incident response, Cybercrime against individual, Cybercrime against property Cybercrime against organization, Cybercrimes against society, Cybercriminals.	7
	Total	**45**

List of References:

1. Mike Shema, *"Anti-Hacker Tool Kit (Indian Edition)"*, Mc Graw Hill.
2. Nina Godbole and Sunit Belpure, *"Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives",*Wiley Publication
3. Dafydd Stuttard and Marcus Pinto, *"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"*, WileyPublication

Course Outcomes (COs):

At the end of this course students will be able to …

1. Learn the concepts of confidentiality, availability and integrity in Information Security.
2. Explain the concepts cyber-attack, cybercrimes, cyber laws and also how to protect themselves and ultimately society from such attacks.
3. Develop Secure Web Application through vulnerability scanning and understanding the importance of data privacy and protecting data.
4. Distinguish and classify the forms of cybercriminal activity and the technological methods used to undertake such crimes.
5. Investigate assumptions about the behavior and role of victims in cyberspace, and use basic web-tools to explore behavior on-line.
6. Analyze and assess the impact of cybercrime on government, businesses, individuals and society.