NIRMA UNIVERSITY

Institute of Technology

B. Tech. Computer Science and Engineering

Semester-VII

L	T	P	C
2	0	2	3

Course Code	2CSOE80
Course Title	Cyber Security

Course Outcomes (COs):

At the end of the course, students will be able to -

1. illustrate core concepts related to hardware and software vulnerabilities
2. demonstrate various attacks using appropriate tools
3. evaluate vulnerabilities in the network and computer system

Syllabus

Teaching Hours

Unit I

Working of Hackers: Invading PCs, Script Kiddies, Working of Personal Hacker Protection **[06]**

Working of Spyware and Antispyware: Introduction to Spywares, Detection Escapism, Invading Privacy, **Hijacking** home page and search pages, working of dialers, working of keyloggers and rootkits, following spyware money trail, working of anti-spyware

Websites and privacy: Working of Cookies, Web bugs, Websites, Websites building personal profiles

Dangers of Internet Search: Working of Google, Individual Know-how

Unit II

Phishing Attacks: Working of Phishing, following phishing money trail, protection against phishing attacks **[06]**

Zombies and Trojan Horses: Working of Zombies and Bot Networks, Working of Trojan Horses, Zombie Money Trail, Working of Zombie and Trojan Protection

Security Dangers in Browsers: Hackers exploit Networks, Protection against browser based attacks

Worms and viruses: Working of viruses and worms, antivirus software

Unit III

Wi-Fi security dangers and protections: Working of Wi-Fi, Invading Wi-Fi Networks, hotspots, Evil Twin Hacks and Protections

[06]

Working of Spam: Dangers of spam, Hiding identity and identification, Working 1of Anti-spam software

Denial of Service Attacks and Protection

Virtual Private Networks, Web Blocking and Parental Controls, Personal Firewalls and Proxies

Unit IV

[06]

Vulnerability assessment: Nessus, OpenVAS, Nexpose, web application scanning tools

Penetration testing tools: Metasploit, Canvas, Writing custom exploits

Unit V

[06]

Defense in Depth: Host-based and Network-based defenses (Firewalls, Intrusion Detection/Prevention)

Network analysis: TcpDump, Wireshark, Netflow

Securing and hardening systems: Bastille, CIS, MS Baseline

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory work:

Laboratory work will be based on above syllabus with minimum 10 experiments to be incorporated.

Suggested Readings^:

1. How Personal and Internet Security Work by Preston Galla, Que Publications
2. Computer Security Concepts, Issues and Implementation by Alfred Basta and Wolf Halton, Cengage Learning
3. Grey Hat Hacking, Shon Harris, TMH

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list