Technology Centre for Cyber Security

Syllabus:

Fundamentals of cyber security **(4 hours)**

Security trends – Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies – Model of network security - OSI security architecture.

Cyber Security Concepts **(4 Hours)**

Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis. Essential Terminologies: CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering (Social Engineering, Foot Printing & Scanning).

Lab session-1 **(3 Hours)**

Lab session using Tools like nmap, zenmap, Port Scanners, Network scanners.

Security algorithms **(4 hours)**

Asymmetric key Cryptography-Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls- Types of Firewalls, User Management, VPN Security

Lab session-2 **(3 Hours)**

Calculate the message digest of a text using the SHA-1 algorithm.

Infrastructure based security **(6 Hours)**

Network packet Sniffing, Network Design Simulation. DOS/ DDOS attacks. Asset Management and Audits, Vulnerabilities and Attacks. Intrusion detection and

Prevention Techniques, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation

Lab session-3 **(3 Hours)**

Implement the sniffing using any tool.

Lab session-4 **(3 Hours)**

Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w.

Lab session-5 **(3 Hours)**

Automated Attack and Penetration Tools Exploring N-Stalker

Malware **(6 Hours)**

Explanation of Malware, Types of Malware: Virus, Worms, Trojans, Rootkits, Robots, Adware's, Spywares, Ransom wares, Zombies etc., OS Hardening (Process Management, Memory Management, Task Management, Windows Registry/ services another configuration), Malware Analysis.

Lab session-6 **(6 Hours)**

Building Trojans

a. Defeating Malware

b. Rootkit Hunter

Sources extracted from

1. Anna University CNS Lab syllabus
2. AICTE emerging technology syllabus
3. IGNOU security certificate course syllabus