PIS204:NETWORK SECURITY AND ETHICAL HACKING

L	T	P	Cr
3	0	2	4.0

Course Objectives: This course is designed to impart a critical theoretical and detailed practical knowledge of a range of computer network security technologies as well as network security tools and services related to ethical hacking.

Introduction: Security, Functionality and ease of use Triangle, Essential Terminology, Elements of Security, Difference between Penetration Testing and Ethical Hacking, Deliverables ethics and legality, Computer Crimes and Implications.

Reconnaissance: Information Gathering Methodology, Locate the Network Range, Active and Passive reconnaissance

Scanning: Scanning, Elaboration phase, active scanning, scanning tools NMAP, hping2. Enumeration, DNS Zone transfer. Detecting live systems on the target network, Discovering services running /listening on target systems, Understanding port scanning techniques, Identifying TCP and UDP services running on the target network, Understanding active and passive fingerprinting

Trojans and Backdoors: Effect on Business, Trojan, Overt and Covert Channels, Working of Trojans, Different Types of Trojans, Different ways a Trojan can get into a system, Indications of a Trojan Attack, Some famous Trojans and ports used by them

Sniffers: Definition of sniffing, Sniffer working, Passive Sniffing, Active Sniffing, Ethreal tool, Man-in-the-Middle Attacks, Spoofing and Sniffing Attacks, ARP Poisoning and countermeasures.

Denial of Service: Goal of DoS (Denial of Service), Impact and Modes of Attack.

Social Engineering: Social Engineering, Art of Manipulation, Human Weakness, Common Types of Social Engineering, Human Based Impersonation, Example of Social Engineering, Computer Based Social Engineering, Reverse Social Engineering, Policies and Procedures, Security Policies-checklist

Session Hijacking: Understanding Session Hijacking, Spoofing vs Hijacking, Steps in Session Hijacking, Types of Session Hijacking, TCP Concepts 3 Way and shake, Sequence numbers

Ethical Hacking- System Hacking and Hacking Wireless Networks: Aspect of remote password guessing, Role of eavesdropping ,Various methods of password cracking, Keystroke Loggers, Understanding Sniffers ,Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing. Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic,Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks.

Laboratory work: deals with launching different types of attacks and creating a network blueprint of an organization.

Recommended Books

1. Hackers Beware, Eric Core, EC-Council Press, 2003
2. Network Security Essentials, William Stallings ,Prentice Hall, 5th Edition, 2013
3. Firewalls and Internet Security, William R. Cheswick and Steven M. Bellovin, Addison-Wesley Professional, 2ndEdition, 2003.
4. Cryptography and Network Security, W. Stallings , Prentice Hall, 5th Edition, 2010