PIS 214: SECURING WINDOWS AND LINUX

L	T	P	Cr
3	0	2	4.0

Course Objectives: This course aims to provide an understanding of the general security concepts of windows and Linux systems, network security tools and implementation of organizational security.

Introduction to General Security Concepts: Principles of Information Security, Information Security Standards, Regulations, and Compliance, Authentication, Authorization, and Accounting

Windows Security Model: Security Principles, SID, Footprinting, Scanning, Enumeration, Command Line Control, GUI Control, Guessing SMB Passwords, Extracting Passwords, Password Cracking, File Searching, Sniffing, Port Redirection, Island Hopping.

Clean Up Services on a Windows System: Creating Rogue User Accounts, Trojan Logon Screens, Remote Control, Planting Backdoor and Trojans, Hardening Windows.

Exploiting Vulnerable Services and Clients in Windows: Hacking SQL Server, Hacking Web applications, Hacking Terminal Servers, Physical Attacks, Denial of Service.

Proactive Measures on a Linux System: Insecurity scanners, Scan Detectors, Hardening your Linux. Log file Analysis, File System Integrity Checks.

Mapping a Linux Machine and Network: DNS issues, Traceroutes, Port Scanning, OS detectionCAN and CVE, Enumerating RPC Services, File Sharing with NFS, SNMP.

Local User Attacks on a Linux System: Users and Privileges,Attacks against poor Programming, Password cracking, Passwordless remote access with r-commands, host based authentication and user access, passwordless logons with SSH.

External Attacks on a Linux System: Social Engineering, Trojans, Viruses and Worms, Physical Attacks, Sniffing Traffic, Buffer Overflows, Vulnerable Scripts, Using Netstat, Using Lsof, Using nmap, turning off services, DNS exploits, session hijacking, DoS,DDoS.

Mail and FTP Security: Identify Website's Identity , HTTP Vs HTTPS , Mail Security, FTP, Active and Passive FTP, Port Scanning through third party FTP Servers, Enabling third party FTP Servers, Insecure Stateful FTP firewall rules, Anonymous FTP problem.

Access Control and Firewalls: Network Security and Logical Access Control, Firewalls For Network Protection, VPN For Network Security, Host Based Firewall Vs Network Based Firewall, Deploying Firewall, Creating Isolated Network Presence Using Virtualization

Laboratory Work: using tools to exploit vulnerabilities (nmap, Metasploit) as well as ensure security (Kerberos, syslog) in windows and Linux operation system.

Recommended Books

1. Security for Microsoft Windows System Administrators, Introduction to key Information Security concepts, Derrick Rountree, Elsevier, Reprint 2011
2. Security Strategies In Linux Platforms And Applications (Information Systems Security & Assurance) , Michael Jang,Jones& Bartlett Learning, 1st Edition, 2010
3. Linux Security Cookbook, Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes, O'Reilly, 2nd Edition,2012