IS241& 241L Network Security Engineering / Laboratory			
Credit Hours	3-1-4	**Prerequisites**	Nil

Course Learning Outcomes:

S No	CLO	Domain	Taxonomy Level	PLO
1	To understand and analyze the issues with host naming, addressing, and routing packets in networks of networks (internetworks)	Cognitive	2	1
2	Identify computer and network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks.	Cognitive	3	3
3	Analyze existing encryption, authentication and key agreement protocols, identify the weaknesses of these protocols	Cognitive	4	4
4	Design SSL or Firewall based solutions against security threats, employ security hardening techniques to the network elements	Cognitive	5	3
5	Construct networks to analyze network and security protocols and test firewalls	Psychomotor	4	5

Course Content:

The Threat Environment: Attackers and their Attacks: Basic Security Terminology, Employee and Ex-Employee threats, Traditional External Attacks and Attack Defenses. **IP Security:** IPSec architecture & concepts, IPSec AH, IPSec ESP, Key Management – Concepts, Manual Exchange, Internet Key Exchange, IPSec Strengths, Weaknesses and Implementation. **Access Controls:** Organization and Human Controls, Physical Access and Security, Biometric Authentication, Authentication, Authorization. **SSL/TLS. Firewalls:** Configuration, Static Packet Filtering, State full Packet Filter, NAT, Application Proxy firewall and Content Filtering, Firewall Architecture, Encrypted Tunnels, Firewall Management, Tools for Log reading. **Intrusion Detection & Prevention Systems:** Elements of Intrusion Detection, Approaches, Misuse Detection, Anomaly Detection, Monitoring Networks and Hosts, Security Information and Event Management (SIEM) systems, Host-based IDSs, Network IDSs, Antivirus Filtering and Unified Threat Management, Intrusion Response for

Threats. **Physical Network Security:** Physical Security Issues, Layer 2 Security Considerations, IP Addressing Design Considerations, ICMP Design Considerations, Routing Considerations. **Secure Network Design:** Basic design requirements and principles (basic network architecture and functions, general requirements on the security and reliability), Network specific faults, threats, and attacks, Security architectures (Secure and resilient routing, secure DNS, secure channels, trusted network access, resilient architectures), Operational security management – how to design and manage reliable networks.

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

Reference Materials:

1. James F. Kurose and K. W. Ross. Computer Networking: A top down approach, 7th Edition, 2016
2. Bruce S. Davie. Computer Networks: A Systems Approach, 5th Edition, 2012
3. William Stallings. Network Security Essentials: Applications and Standards. 6th Edition, 2016
4. Michael T. Goodrich and Roberto Tamassia. Introduction to Computer Security. 2011

In addition there will be lecture notes and selected articles.

IS241L Network Security Engineering Laboratory Experiments/ Exercises
Understand/ implement Windows Policies and risks associated with these policies.
Understand/ implement Windows Firewall rules.
Hardening Routers.
Scanning networks.
Passive Information gathering.
Analyzing Network Traffic with Wireshark.
Introduction to VMware and Virtual box.
Introduction to Kali Linux and its tools.
Eavesdropping Attacks and countermeasures.
Social Engineering attacks and countermeasures.
MAC/IP Spoofing and their countermeasures.

ARP Poisoning and countermeasures.
Email Spoofing.
Denial of Service Attack and countermeasures.
How to achieve anonymity (Proxies, VPN, TOR)
Introduction to Metasploit.
SQL injection.
Access Control Lists Implementation.
Cracking WPS/WEP/WPA.