Course Title : Firewall Network Security

Course Code : EE4302

Units: 3

Level: B4

Course Aims & Objectives:
This course is designed to provide the student with basic knowledge of general security concepts and cryptography, including symmetric/asymmetric encryption algorithms, authentication methods, common network attacks and how to safeguard against them. The course also aim at providing the student with basic knowledge of infrastructure security, including various network devices and media, and the proper use of perimeter topologies such as DMZs, Extranets, and Intranets to establish network security.

Intended Learning Outcomes:
On completion of this course, the students will be able to:

1. Describe the basic concept of cryptography for network security applications, including the differences between asymmetric and symmetric algorithms, and the different types of PKI certificates and their usage
2. Identify different authentication methods, common network attacks and various communication security weaknesses and then know how to safeguard against them.
3. Use a broad range of network security monitoring tools for security assessments.
4. Use various network devices and perimeter topologies to design infrastructure security with DMZs, Extranets and Intranet to establish network security
5. Describe current and anticipated trends in Internet security.

Syllabus:
Introduction to the Concepts of Information Security
The Need for Security.; Security Approaches; Principles of Security; Security Policy.

Types of Attacks

Firewalls
Firewalls Design Principles: Traffic Control, Trade-Off Between Accessibility and Security, Protection For Vulnerable Services; Firewall Components: Firewall Administrator, Firewall Policy, Simple Packet Filers, Dynamic Packet Filtering; Proxy Firewalls: Application Gateways, Circuit-Level Gateway; Firewall Evaluation and Firewall Configuration.
Cryptographic Techniques
Plain Text and Cipher Text; Substitution and Transposition Techniques; Symmetric Key Cryptography with DES, Triple DES, RC4, RC5, Blowfish and AES; Asymmetric Key Cryptography with RSA; Digital Signatures; Public Key Infrastructure (PKI); Digital Certificates; Private Key Management.

User Authentication Mechanisms
Authentication Basics; Passwords; Authentication Tokens; Certificate-based Authentication; Biometric Authentication; Kerberos

Internet Security Protocols
Secure Socket Layer (SSL); Secure Hyper Text Transfer Protocol (SHTTP); Secure Electronic Transaction (SET); Electronic Money; Email Security; PGP; Wireless Application Protocol (WAP) Security; IPSec and VPN

Laboratory Experiment:
Lab 1: Port Scanning and Packet Sniffing
Lab 2: Linux Firewalls using iptable
Lab 3: SSH and Password Cracking
Lab 4: Intrusion Detection using Snort

Teaching pattern:
Duration of course: 1 semester
Suggested lecture/tutorial/laboratory mix: Lecture Hour: 26 hours
Tutorial /Laboratory Hour: 13 hours

Assessment pattern:
Examination duration: 2 hours, at the end of the semester
Percentage of coursework, examination, etc.: 50% CW; 50% Exam

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained, and a laboratory attendance of at least 75% recorded.

Pre-requisites: (Please quote course code & title)
EE3311 Networking II
or
EE3016 (old code: EE4010) WANs and Communication Protocols
and
CS3161 Operating System Principles

Pre-cursor: (Please quote course code & title)
Nil

Exclusive Course: (Please quote course code & title)
Nil

Equivalent Courses: (Please quote course code & title)
Nil
Equivalent to the Old Course Code and Title: *(Please quote course code & title)*
Nil

Textbook:

Reference Books:


