UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
ESCUELA DE CIENCIAS Y SISTEMAS

PROGRAMA DEL CURSO DE SEGURIDAD Y AUDITORIA EN REDES DE COMPUTADORAS

CODIGO:	966	**CREDITOS:**	4
ESCUELA:	Ciencias y Sistemas	**AREA:**	Ciencia de la Computación
PRERREQUISITO:	975	**POSTREQUISITO:**	
CATEGORIA:	Obligatorio	**SECCION:**	
HORAS POR SEMANA DEL CURSO:	4	**HORAS POR SEMANA DE LABORATORIO:**	2
DIAS QUE SE IMPARTE EL CURSO:	Miércoles Sabado	**DIAS DE LABORATORIO**	Sábado
HORARIO DEL CURSO:		**HORARIO DE LABORATORIO:**	

DESCRIPCIÓN DEL CURSO

El curso le da continuidad al estudio de las redes de computadoras y la implementación de los diferentes protocolos de aplicación del modelo TCP / IP.

Nos centraremos en el funcionamiento básico de cada protocolo con el objetivo de comprender sus vulnerabilidades y comprender de manera elemental los diferentes ataques básicos a redes de computadoras con el objetivo de configurar un entorno seguro y protegernos de dichos ataques.

OBJETIVOS GENERALES

- Objetivos Generales:

1. Entender la importancia de la seguridad en las redes de computadoras.
2. Dar al estudiante los conocimientos básicos de seguridad informática.

- Objetivos Específicos:

1. Comprender los fundamentos básicos de seguridad en una red de computadoras.
2. Analizar y comprender el funcionamiento del protocolo TCP/IP a nivel de paquetes analizados desde un sniffer.
3. Entender y saber implementar listas de acceso en routers y switchs Cisco.
4. Diseniar y configurar un firewall
5. Comprender e implementar una VPN con IPsec
6. Diseniar y configurar un IDS
7. Comprender la importancia de la seguridad en redes inalámbricas.

METODOLOGÍA

- Clases Presenciales en el Salon de Clases
- Practicas del Laboratorio
- Prácticas individuales y en grupos.
  Análisis y discusión de videos.

EVALUACIÓN DEL RENDIMIENTO ACADÉMICO:

Actividades	Puntos
2 Parciales	40
Análisis de Laboratorios y Escenarios	30
Asistencias, investigaciones, practicas individuales/grupo	5
Zona	75
Examen Final	25
Nota	

CONTENIDO PROGRAMÁTICO

1. Network Defense Fundamentals
1.1. Network Defense
1.2. Defensive Technologies
1.3. Objectives of Access Control
1.4. The Impact of Defense
1.5. Network Auditing Concepts

2. Advanced TCP/ IP
2.1. TCP/ IP Concepts
2.2. Analyzing the Three-way Handshake
2.3. Capturing and Identifying IP Datagrams
2.4. Capturing and Identifying ICMP Messages
2.5. Capturing and Identifying TCP Headers
2.6. Capturing and Identifying UDP Headers
2.7. Analyzing Packet Fragmentation
2.8. Analyzing an Entire Session

3. Routers and Access Control Lists
3.1. Fundamental Cisco Security
3.2. Routing Principles
3.3. Removing Protocols and Services
3.4. Creating Access Control Lists
3.5. Implementing Access Control Lists
3.6. Logging Concepts

4. Designing and Configuring Firewalls
4.1. Understanding Firewalls

4.2. Firewall Components
4.3. Create a Firewall Policy
4.4. Rule Sets and Packet Filters
4.5. Proxy Server
4.6. The Bastion Host
4.7. The Honeypot
4.8. Implementing Firewall Technologies

5. Implementing IPSec and VPNs
5.1. Internet Protocol Security
5.2. IPSec Policy Management
5.3. IPSec AH Implementation
5.4. Combining AH and ESP in IPSec
5.5. VPN Fundamentals
5.6. Tunneling Protocols
5.7. VPN Design and Architecture
5.8. VPN Security
5.9. Configuring a VPN

6. Designing and Configuring an Intrusion Detection System
6.1. The Goals of an Intrusion Detection System
6.2. Technologies and Techniques of Intrusion Detection
6.3. Host-based Intrusion Detection
6.4. Network-based Intrusion Detection
6.5. The Analysis
6.6. How to Use an IDS
6.7. What an IDS Cannot Do

7. Securing Wireless Networks
7.1. Wireless Networking Fundamentals
7.2. Wireless LAN (WLAN) Fundamentals
7.3. Wireless Security Solutions
7.4. Wireless Auditing
7.5. Wireless Trusted Networks

BIBLIOGRAFIA

Consultar Universidad Virtual