

GESTIÓN Y CONFIGURACIÓN DE FIREWALLS



CÓDIGO CURSO: TS-01-01

DURACIÓN: 15h (5 sesiones de 3 horas). 5h teóricas y 10h prácticas

DESTINATARIOS: Ingenieros de sistemas y técnicos

OBJETIVOS: Profundos conocimientos de las políticas de seguridad usadas en entornos abiertos (Intranet, extranets e internet), protocolos de seguridad (VPNs), defensa y configuración de Firewalls Linux. En este curso, el alumno adquirirá los conocimientos necesarios para poder diseñar e implementar políticas de seguridad eficaces sobre sistemas abiertos e interconexión de los mismos.

CURSOS RECOMENDADOS: TS-01-04, TS-01-05

UNDIDADES DIDÁCTICAS:

Unidad didáctica 1

Nombre: Arquitectura Internet y política de Firewalls

Duración: 3h

Descripción: En esta unidad el alumno conocerá la arquitectura que forma la red Internet; protocolos, servicios, entidades, etc. Así mismo, y una vez conocidas las características de Internet, se darán a conocer los conceptos de Firewall, políticas de Firewalls, tipos, etc.

Prácticas: Se harán seguimiento de los paquetes TCP/IP desde un ordenador a otro, ante distintas peticiones de servicios. Se demostrará el funcionamiento de la pila TCP/IP

Evaluación: Se realizará una prueba auto evaluatoria de tipo test al finalizar la unidad

Temario:

Tema 1.1: Internet; arquitectura y servicios

Tema 1.2: Protocolo TCP/IP

Tema 1.3: Protocolo SMB

Tema 1.4: Conceptos y política de Firewall

Tema 1.5: Tipos de Firewall



Unidad didáctica 2

- Nombre:** Protocolos de seguridad y criptografía (RSA, SSL, SSH, VPN, etc)
- Duración:** 3h
- Descripción:** En esta unidad el alumno conocerá los protocolos de seguridad que se han diseñado para asegurar las conexiones y transmisión de datos por Internet. También conocerá los algoritmos más conocidos en materia de seguridad, así como las distintas tecnologías que existen para establecer redes privadas virtuales (VPN).
- Prácticas:** Se analizarán los paquetes que son intercambiados en los servicios SSH y SSL. También se establecerán túneles PPTP y IPSec con el exterior, observando el procedimiento y analizando los paquetes intercambiados.
- Evaluación:** Se realizará una prueba auto evaluatoria de tipo test al finalizar la unidad
- Temario:**
- Tema 2.1: Criptografía: conceptos
 - Tema 2.2: Algoritmo de cifrado RSA
 - Tema 2.3: Protocolo SSL y HTTPS
 - Tema 2.4: Protocolo SSH
 - Tema 2.5: Protocolo PPTP (VPN)
 - Tema 2.6: Protocolo IPSec (VPN)

Unidad didáctica 3

- Nombre:** Técnicas y herramientas de ataques/defensa a redes IP
- Duración:** 3h
- Descripción:** En esta unidad el alumno conocerá los distintos tipos de ataques que se basan en la arquitectura IP y qué tipo defensas se pueden aplicar. Así mismo, también conocerá las aplicaciones y herramientas utilizadas en la defensa de los sistemas de información.
- Prácticas:** Se realizarán diversos tipos de ataques a estaciones de la red local, implantando las defensas adecuadas y observando el tráfico de paquetes originados.
- Evaluación:** Se realizará una prueba auto evaluatoria de tipo test al finalizar la unidad
- Temario:**
- Tema 3.1: Ataques Denegación de Servicio (DOS)
 - Tema 3.2: Ataques Denegación de Servicio Distribuido (DDOS)
 - Tema 3.3: Defensas sobre DOS y DDOS
 - Tema 3.4: Ataques y defensa sobre SMB (NTML)
 - Tema 3.5: Ataques de Spoofing
 - Tema 3.6: Sistemas Detección Intrusos (IDS)





Unidad didáctica 4

Nombre: Configuración de Firewall con sistemas Linux

Duración: 6h

Descripción: En esta unidad el alumno aprenderá a configurar un sistema de seguridad IP basado en arquitecturas Linux. Conocerá las herramientas que Linux proporciona para crear Firewalls, así como su instalación y configuración.

Prácticas: Se realizarán instalaciones de Firewalls en las estaciones del aula

Evaluación: Se realizará una prueba auto evaluatoria de tipo test al finalizar la unidad

Temario:

Tema 4.1: Linux y la seguridad

Tema 4.2: Iptables y Netfilter

Tema 4.3: Proxys en Linux

Tema 4.4: IPCop: instalación y configuración

