LINUX SEGURIDAD EN REDES Y FIREWALL

Duración: 24 hrs.

Código: LNFIW

Curso:

Descripción del curso

El curso de Linux avanzado le permitirá elevar la disponibilidad de los servidores basados en Linux a los niveles de servicios de Red externos. Además de administrar los servicios de Red de manera controlada, aprenderá su teoría de utilización y las bondades de sus protocolos, las mismas que serán volcadas en ejemplos y análisis de opciones para su posterior decisión sobre el servicio de Red a implementar.

Objetivos:

El Participante al finalizar el curso será capaz de:

Desarrollarse en el campo de la seguridad perimetral de las redes LAN. Implementar seguridad a nivel de capa de RED con NETFILTER. Implementar PROXYS a nivel de capa de Red y capa de Aplicación. Implementar un "Firewall Antivirus".

Dirigido a:

- Estudiantes.
- Ingenieros de Sistemas.
- Técnicos de Sistemas.
- Administradores de Red.
- Jefes de Sistema o Soporte.
- Profesionales de carreras afines o personas con interés en temas informáticos, redes y sistemas.

REQUISITOS MÍNIMOS

- Configuración de redes basadas en TCP/IP.
- Conocimientos del protocolo TCP/IP y su funcionamiento.
- Implementar servicios TCP/IP en LINUX/Windows (Web, Correo, etc).
- Haber llevado los cursos Linux Administración y Linux Servicios Internet o tener.

CONTENIDO

Sesión 1

Introducción a la protección perimetral de la red

- Implementación y disposición del Firewall en una LAN.
- Disposiciones generales para la instalación de LINUX.
- Consideraciones para instalar el firewall, Defensa de la red perimetral. Puertos y servicios.
- Definición de la POLITICA de SEGURIDAD, Preparando el servidor y sus componentes.

Sesión 2

Implementación de las reglas de filtrado y políticas de seguridad

- Componente NETFILTER del núcleo de Linux.
- Política ACCEPT versus Política DROP: seguridad perimetral.
- Traducción de Direcciones de Red. "NATEO" de puertos específicos.
- NAT de origen y NAT de destino (SNAT/DNAT).
- Diagrama de flujo de análisis de las reglas de NETFILTER.
- Script de implementación de reglas de filtrado y NAT.

Sesión 3

Control de la navegación HTTP y HTTPS: Proxy Squid

- Control de Navegación WWW: Servidor Proxy SQUID.
- Como trabaja el servidor SQUID, Herramientas: Listas de Control de Acceso (ACL).
- Pruebas del servidor SQUID en el firewall. Control de Ancho de Banda con SQUID.
- MONITOREO con SARG.

Sesión 4

Protocolo SSH

- Introducción. Ssh, Sftp, Scp, Openssh. Paquetes a instalar. Archivos de configuración.
- Seguridad con Openssh.

CONTENIDO

Sesión 5

Protocolo HTTPS

- Servicio HTTPS Apache. Algoritmos de cifrado.
- OpenSSL, Mod_SSL.
- Apache con extensiones SSL.
- Apache SSL.
- UTF8 y codificación de documentos.
- Generando clave y certificado.
- Archivos de configuración, Seguridad con openssh.

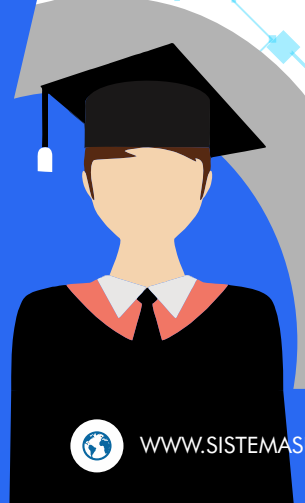
Sesión 6

Cliente OpenVPN

- OpenVPN – Introducción.
- Características Principales.
- Modos de funcionamiento, Autenticación.
- Implementación de un cliente OpenVPN.
- Configuración de clientes Windows. Monitoreo con IpTraf.

EVALUACIÓN

La evaluación de cursos será totalmente práctica. Se realizarán entre 4 y 5 prácticas de las cuales se eliminará la nota más baja y se obtendrá un promedio (PP). Durante la última sesión se realizará un examen final (EF), el cual se promediará con la nota de prácticas y de esta manera se tendrá la calificación final.



PROMEDIO DE PRACTICAS

$$PP=\frac{(PR1 + Pr2 + Pr3 + PR4) - Menor\ (PR)}{3}$$

Nota Final:

$$NF = (PP + EF) / 2$$