SISTEMAS UNI
Tecnologías de la Información

UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

LINUX
SEGURIDAD EN REDES Y FIREWALLS

Duración 24 horas.

8 Sesiones.

Dirigido a:

- Estudiantes
- Profesionales
- Público en general.

CURSO LIBRE

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".

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.

REQUERIMIENTOS:

- Conocimientos previos sobre Protoculos y configuración TCP / IP.

WWW.SISTEMASUNI.EDU.PE
SISUNI.INFO@UNI.EDU.PE
CENTRAL: 200-9060
DIRECTO: 481 - 1070 ANEXO 5231

SISTEMAS UNI
Tecnologías de la Información

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

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 rewall, Defensa de la red perimetral. Puertos y servicios.
- De nición de la POLITICA de SEGURIDAD, Preparando el servidor y sus componentes.

Sesión 2

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.

WWW.SISTEMASUNI.EDU.PE
SISUNI.INFO@UNI.EDU.PE
CENTRAL: 200-9060
DIRECTO: 481 - 1070 ANEXO 5231

CONTENIDO:

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 rewall. 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.

SISTEMAS UNI
Tecnologías de la Información

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

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 Prácticas	Nota Final:
$PP=\frac{(PR1 + Pr2 + Pr3 + PR4) - Menor\ (PR)}{3}$	$NF = (PP + EF) / 2$

WWW.SISTEMASUNI.EDU.PE
SISUNI.INFO@UNI.EDU.PE
CENTRAL: 200-9060
DIRECTO: 481 - 1070 ANEXO 5231