UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS

LINUX
SEGURIDAD EN REDES Y FIREWALLS

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.

• Conocimientos Previos

Conocimientos previos sobre Protoculos y configuración TCP / IP.

• El participante al final del curso sera 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, Profesionales y Publico en General

Duración del curso
24
HORAS.

Evaluación

Será totalmentepráctica. Se realizarán entre 4 o 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:

PP=(PR1 + PR2 + PR3 + PR4 - MENOR (PR)

NOTA FINAL:

NF= PP + EF

Modalidad Online

Requiere una PC con las siguientes caracteristicas:

- Procesador - 1GHZ o más rapido / en un chip (SOC).
- RAM - 1GB para 32 Bits o 2GB para 64.
- Espacio Libre 16GB - SO de 32 bits / 32GB - SO de 64 bits.
- Una tarjeta gráfica - DirectX 9, posterior o controlador WDDM 1.0.
- Pantalla - 800x 600 resolución.
- Conexión a internet estable.

Conéctate a nuestras diferentes Plataformas Digitales:

Telf.: 200 - 9060 Opción 1
E-mail: sisuni.info@uni.edu.pe

www.sistemasuni.edu.pe

“Aumenta tus conocimientos, desarrolla nuevas habilidades y construye hoy tu futuro”.

CLASE #01

- 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.
- Denición de la POLITICA de SEGURIDAD, Preparando el servidor y sus componentes.
- 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 NA.

CLASE #02

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

CLASE #03

- 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

CLASE #04

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