



TEMARIO CURSO SEGURIDAD LINUX

Objetivo: Concientizar al alumno de la importancia de la seguridad en la administración de sistemas, pudiendo implementar un sistema completo de seguridad.

Dirigido a alumnos con conocimientos en sistemas operativos Linux y Unix y conocimientos básicos de redes.

La duración del curso es de 24 horas y se dictará en la Universidad Tecnológica Nacional Sede Facultad Regional Buenos Aires o en su defecto en sus oficinas si cuenta con la infraestructura adecuada.

Se brindará material de apoyo y certificación de la

 **Secretaría de Cultura y Extensión Universitaria - UTN - FRBA**



Los cursos ofrecidos están preparados para que aquellos alumnos que deseen rendir la certificación del LPI (Linux Professional Institute) lo puedan hacer.

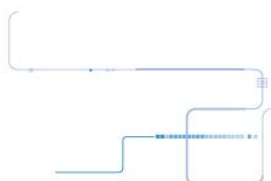
Temario:

1. INTRODUCCION

- 1.1 Introducción a la seguridad de redes
- 1.2 Linux como servidor de Internet
- 1.3 Seguridad en Linux
- 1.4 Vulnerabilidades comunes
- 1.5 Permisos y usuarios
- 1.6 Patch management
- 1.7 Netfilter Firewall Framework
- 1.8 Intrusion Detection
- 1.9 VPN

2. SEGURIDAD BASICA

- 2.1 Requisitos mínimos de seguridad
- 2.2 Contraseñas
- 2.3 Políticas de usuarios y grupos
- 2.4 Permisos de archivos básicos y extendidos





- 2.5 Posix ACLs
- 2.6 Encriptación de filesystems y archivos
- 2.7 Integridad de archivos
- 2.8 Extended Inet Daemon
- 2.9 TcpWrappers
- 2.10 Monitoreo de red y parámetros
- 2.11 Sniffer y monitoreo de paquetes
- 2.12 Scanner de puertos y fingerprinting
- 2.13 Scanner de vulnerabilidades

3. SEGURIDAD DE SERVICIOS

- 3.1 Web, Apache+CGI+SSL
- 3.2 OpenSSL y generación de certificados
- 3.3 Sendmail y Postfix
- 3.4 FTP
- 3.5 Samba
- 3.6 SSH
- 3.7 Túneles SSL

4. FIREWALL

- 4.1 Introducción a Netfilter
- 4.2 Configuración de Firewall vía iptables
- 4.3 Statefull Firewall
- 4.4 Firewalls complejos: DMZ

5. INTRUSION DETECTION

- 5.1 Introducción a los IDS
- 5.2 Snort IDS
- 5.3 Configuración de Snort
- 5.4 Ejemplos reales

