

MONITOREO DE LA *SEGURIDAD* EN REDES EN SISTEMAS LINUX



Algunas veces aprender una nueva capacidad a través del aprendizaje de una totalmente diferente, puede ser la clave para llegar a aprender ambas sin notarlo.

Esta es la aproximación que hemos tomado para enseñar y combinar en un mismo curso, dos temas sumamente interesantes y actuales, Linux un sistema operativo de software libre y herramientas que nos sirven para monitorizar la seguridad de redes. Quizás esta es la oportunidad que has estado esperando para adentrarte en ambos mundos.

Objetivo: Al finalizar el curso, el alumno tendrá el conocimiento y las herramientas necesarias para llevar a cabo la administración básica de un sistema Linux en la modalidad de servidor, así como también, dominara las herramientas de seguridad que le permitan llevar a cabo la recolección, análisis y notificación de indicadores y advertencias para detectar intrusiones y responder a ellas.

Orientado a: Profesionales de carreras afines a Ingeniería en Sistemas, Licenciado en Informática, etc. que deseen dar su primer paso firme hacia la administración de sistemas Linux con un enfoque en particular en las herramientas de monitoreo de la seguridad en redes.

Prerrequisitos: Haber cursado o tener conocimiento del tema de sistemas operativos y conceptos básicos de redes, en específico de redes TCP/IP.

Duración: 20 hrs

Horario: Cuatro (4) Sábados en un horario de 9 a.m. a 2 p.m.

Temario:

- Instalación y Particionamiento del Disco Duro
- Instalación y Configuración de GRUB
- Instalación de aplicaciones desde código fuente
 - configure
 - make
 - make install
- Administración de Paquetes
 - Usando apt

BIOGRAFÍA DEL INSTRUCTOR:

Miguel Guirao (a.k.a. Chicolinux) comenzó su carrera profesional en el 2000, en una compañía que comercializaba productos y servicios de Control de Asistencia e Identificación, donde él era responsable de los productos, hardware y software, y servicios de la marca DATACARD. Posteriormente, salto a la arena de las telecomunicaciones para trabajar dentro de la subsidiaría más grande del grupo América Móvil, Telcel, en donde actualmente se desempeña como Analista de Sistemas de Información en el Depto. de Informática Regional. Puesto en el que lleva más de 5 años.



Se adentro en el mundo de la Seguridad de la Información cuando cursaba la Maestría en Gestión de Tecnologías. Desde entonces, ha enfocada todas sus energías en mejorar su carrera profesional en este campo.

Aparte de su trabajo en Telcel, se desempeña como profesor por honorarios en la Universidad Anahuac Mayab en donde enseña en

- Usando rpm
- Trabajando en la línea de comandos
 - bash
 - echo
 - env
 - exec
 - export
 - bash history
- Procesamiento de flujos de texto usando filtros
 - *cat*
 - *cut*
 - *expand*
 - *fmt*
 - *head*
 - *hexdump*
 - *join*
 - *nl*
 - *paste*
 - *pr*
 - *sed*
 - *sort*
 - *split*
 - *tac*
 - *tail*
 - *tr*
 - *unexpand*
 - *uniq*
 - *wc*
- *Administración de Archivos*
- *Usando flujos, pipes y redireccionamientos*
- *Crear, monitorear y matar procesos*
- *Modificar las prioridades de los procesos*
- *Buscar archivos de texto usando expresiones regulares*
- *Uso básico del editor vi*
- *Control del montaje y desmontaje de sistemas de archivos*
- *Uso de los permisos de archivos*
- *Gestión de la propiedad de archivos*
- *Crear y modificar enlaces duros y simbólicos*
- *Buscando archivos del sistema*
-
- ¿Que es la Monitorización de la Seguridad de Redes?
 - Indicaciones y Advertencias
 - Recolección, Análisis y Notificación
 - Principios de Seguridad: Detección
 - Principios de Seguridad: Limitaciones

la Escuela de Ingeniería en Sistemas en las áreas de Seguridad de la Información, Redes, Desarrollo Web y de Aplicaciones para dispositivos móviles.

También es fundador y coordinador del Grupo de Usuarios de Software Libre más antiguo del área, grupo que fundo cuando estaba en la universidad. Igualmente fundo FUTURA – Soluciones Libres, una empresa inicial en la rama de soluciones de TI y capacitación que se enfoca en otorgar soluciones de TI basadas en el uso y aplicación de soluciones de software libre.

Si, ocasionalmente dispone de tiempo libre, y cuando lo tiene, le gusta leer novelas, viajar a lugares interesantes, o simplemente tener un tiempo de hacking en su pequeño laboratorio en casa. Siempre hay un libro de tecnologías en su mochila y corre tres distribuciones de Linux diferentes en su laptop sólo por diversión.

- Consideraciones de Despliegue
 - Modelos de Amenaza y Zonas de Monitorización
 - ◆ El Perímetro
 - ◆ La Zona Desmilitarizada
 - ◆ La Zona Inalámbrica
 - ◆ La Intranet
 - Acceso al Trafico de Cada Zona
 - ◆ Concentradores
 - ◆ Puertos SPAN
 - ◆ Taps
 - ◆ Dispositivos en linea
 - Monitorización sin Hilos
 - Arquitectura del Sensor
 - Administración de Sensores
- Datos de Contenido Completo
 - LIBPCAP
 - TCPDUMP
 - Ethereal
- Datos de Sesión
 - Fprobe
 - Ng_netflow
 - ...
- Datos Estadísticos
 - lpcad
 - lfstat
 - Bmon
 - Trafshow
 - Tttt
 - Tcpcstat
 - Ntop
- Herramientas para atacar la monitorización de Seguridad en Redes
 - Packit
 - IP Sorcery
 - Fragroute
 - LFT
 - Xprobe2

Entregables: Al inicio del curso el alumno recibirá un LiveCD de una distribución de Linux que incluye las herramientas que serán cubiertas en clase. Así mismo se entrega la documentación pertinente de acuerdo al curso.