DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

TECNICO ESPECIALISTA EN SEGURIDAD INFORMATICA.

- **Modalidad:** MIXTO. (PRESENCIAL Y DISTANCIA)
- **Duración:** 300 HORAS DISTANCIA Y 30 HORAS PRESENCIALES TOTALES, DIVIDIDAS EN TRES GRUPOS DE 100 HORAS DISTANCIA Y 10 HORAS PRESENCIALES C/ UNO.
- **Formación Presencial:** 10 horas por cada curso, 2.5 horas c/ semana, a determinar por el cliente.
- **Contenido AAFF:**

TÉCNICO ESPECIALISTA EN SEGURIDAD INFORMÁTICA
A SEGURIDAD, SPAM, SPYWARE Y VIRUS

1 Virus: ataque de programas maliciosos
¿Qué es un virus informático?
Virus: Tantos tipos como lloriqueos en un jardín de infancia
¿Quién crea un virus informático?
¡Qué no hacer!
¡Cuando atacan los virus!
Ahora que tengo su atención...
Revisión del antivirus: tácticas de 10 minutos
Refuerce su ordenador: una fuerte defensa contra virus en pocashoras
Sin gusanos en mi Apple
¿Tiene un virus en su Pocket?
Resumen
2 Spyware: invasión de anunciantes, piratasy oportunistas
¿Qué es el spyware?
¿Qué hace el spyware y por qué es tan malo?
¿Cómo se introduce un programa spyware en mi ordenador?
Tipos de spyware: snoops, adware, cookies...
¿Quién está en peligro?
¿Cómo sé si tengo spyware?
Defiéndase contra el spyware
Prohíba el paso a los espías: cree una fuerte defensa en una tarde
Resumen
3 Hacker: hay un hombre en mi máquina
¿Qué es un hacker?
¿Quiénes son los hacker?
¿Qué daño pueden hacer los hacker?
Objetivos de un ataque hack
Motivación de un hacker: pienso luego practico el hacking
Herramientas de los entendidos: ¿me pasarías un caballode Troya?
Firewall: Prohíba el paso a los hacker
Firewall de software: programas que detienen a los hacker
Cómo detectar el ataque de un hacker
Cómo arreglar el ataque de un hacker
Cierre las escotillas con tácticas de 10 minutos
Sepárese del mundo con una pared: instale un firewall mejor en una tarde

DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

Resumen
4 Ladrones de identidad y phishers: proteja su buennombre y su cuenta bancaria
¿Qué es un robo de identidad?
¿Qué es el phishing?
¿Cómo funciona el phishing?
¿Qué es el pharming?
¿Qué daño puede hacer el phishing?
¿Quién está en peligro? ¡Todos!
Tácticas de 10 minutos para no ser estafado
Proteja su identidad en una tarde
Resumen
5 Spam: correo no deseado
¿Qué es el spam?
¿Por qué sigue llegando spam?
¿Por qué nadie detiene a los spammers?
¿Cómo consiguen los spammers mi dirección de correo electrónico?
Daños que puede provocar el spam
Tácticas de 10 minutos para reducir el spam
Termine con más spam en una tarde
Resumen
6 Snoop en redes inalámbricas: selle su red Wi-Fi
¿Qué es una red inalámbrica particular?
¿Qué daño puede hacer un snoop de red inalámbrica?
¿Quiénes son los snooper?
¡Su red Wi-Fi está llena de agujeros!
Primera línea de defensa: proteja su red Wi-Fi
Detectar la visita de un snoop inalámbrico
¡Estoy siendo atacado! Qué hacer si descubre un snoop de red inalámbrica
Conseguir seguridad inalámbrica: tácticas rápidas y algunasque pueden llevarle más tiempo
Resumen
7 Privacidad violada: cubra sus huellas y su reputación
¿Por qué es importante su privacidad?
¿Qué deja tras de sí en un ordenador?
¿Quiénes son los snoop de su privacidad?
Consecuencias de ser cogido
Tácticas de emergencia
Oculte su rastro en 10 minutos
Cubra su rastro en una tarde
Borre los reproductores multimedia
Resumen
8 Preparemos Windows a prueba de bombas
Si Windows XP fuera un dique, usted sería un pequeño holandés
Resumen
9 Empezar desde el principio: borrar un disco duroy restaurarlo completamente
Encienda la mecha y aléjese
Comencemos

DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

Paso 1: Descargue los drivers y el software que necesite para la instalación
Paso 2: Hacer copia de seguridad
Paso 3: Ponga el enchufe en la red
Paso 4: Borre Windows
Paso 5: Instale Windows de nuevo
Paso 6: Instale los drivers o controladores
Paso 7: Instale protección contra malware
Paso 8a: Instale Service Pack 2 de Windows XP (desde un CD)
Paso 8b: Instale SP2 desde Internet
Paso 9: Configurar sus configuraciones de seguridad
Paso 10: Instale Firefox
Paso 11: Configure su red de conexiones

Paso 12: Actualice Windows con los últimos parches de seguridad
Paso 13: Actualice todos sus programas de seguridad y ficherosde firmas de seguridad
Paso 14: Active Windows
Paso 15: Re-instale sus programas
Paso 16: Otras cosas que puede hacer
Resumen
10 Mantenimiento continuo: rechace futuras amenazas
Observe usted mismo: mantenga su ordenador seguro
Rutinas diarias: pasear al perro, dar de comer a los niñosy proteger su ordenador
Rutinas semanales: cómo estar aburrido una mañana de sábado
Rutinas mensuales: limpiar el garaje, recortar el seto y actualizar Windows
Báñese una vez al año si lo necesita y reformatee y reinstale
Resumen
11 Eligiendo software: gangas, acuerdos y softwareinútiles
Nada en la vida es gratis, excepto el software
Weirdware: cuando no es payware o freeware
¿Por qué debería pagar por mi caja de herramientas de seguridad?
Eligiendo el software de seguridad correcto
Resumen
12 Herramientas del negocio: productos de seguridadque debería tener
Qué software de seguridad es bueno para usted.
Programas antivirus
Anti-Spyware
Firewalls
Anti-spam
Resumen

DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

TÉCNICO ESPECIALISTA EN SEGURIDAD INFORMÁTICA
B PROTECCIÓN DEL PC Y SEGURIDAD EN INTERNET

Introducción

1 Seguridad básica de Windows

Introducción
¿Por qué tiene que estar protegido?
¿Por qué está en peligro?
Resumen

2 Contraseñas

Introducción
El poder de las contraseñas
Descodificar contraseñas
Almacenar las contraseñas
Una contraseña superpoderosa
Resumen

3 Virus, gusanos y otros malware

Introducción
Términos malware
La historia de los malware
Resumen

4 Parches

Introducción
Terminología de parches
¿Por qué debería poner parches?
¿Cómo sé a qué le tengo que poner parches?
Resumen

5 Seguridad del perímetro

Introducción
De fosos y puentes a firewall y filtros
Firewall
Detección y prevención de intrusos
Resumen

6 Seguridad en el correo electrónico

Introducción
La evolución del correo electrónico
La seguridad del correo electrónico preocupa
Resumen

7 Privacidad y seguridad navegando por la Web

Introducción
La revolucionaria World Wide Web
La seguridad de la Web preocupa
Resumen

8 Seguridad en redes inalámbricas

Introducción
Lo esencial de las redes inalámbricas
Medidas básicas de seguridad en redes inalámbricas
Medidas de seguridad adicionales en los hotspot
Resumen

9 Spyware y adware

DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

Introducción
¿Qué es adware?
¿Qué es spyware?
Deshacerse de los spyware
Resumen
10 Proteger su ordenador
Introducción
Mantenimiento general de su PC
Parches y actualizaciones
Centro de seguridad de Windows Vista
Resumen
11 Cuando golpea el desastre
Introducción
Comprobar sus registros de eventos
Permitir las auditorías de seguridad
Revisar los registros del firewall
Escanear su ordenador
Restaurar su sistema
Comenzar desde cero
Restaurar sus datos
Recurrir a los profesionales
Resumen
12 Alternativas Microsoft: Dentrodel escritorio Linux
Introducción
Entornos de escritorio comunes
El sistema X Window y los gestores de ventanas
Clientes de correo electrónico y gestores de información personal
Navegadores Web
Suites de aplicaciones ofimáticas
Ejecutar aplicaciones Windows en Linux
Resumen
TÉCNICO ESPECIALISTA EN SEGURIDAD INFORMÁTICA
C SEGURIDAD EN LINUX
Presentar los casos de negocio para software de código abierto
Introducción
Los costes de usar soluciones de seguridad libres
Los beneficios de usar soluciones libres de seguridad
"Vender" una solución gratis
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Fortalecer el sistema operativo
Introducción
Actualizar el sistema operativo
Manejar los asuntos de mantenimiento
Deshabilitar manualmente los servicios y puertos innecesarios
Cerrar puertos
Fortalecer el sistema con Bastille
Manejar sus archivos de registro

DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

Usar optimizadores de registro
Seguridad mejorada en Linux
Asegurar Novell SUSE Linux
Novell AppArmor
Sistema de prevención de intrusión al host
Herramientas de pruebas de Linux
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Enumeración y escaneo de su red
Introducción
Escanear
Enumeración
¿Cómo funciona el escaneo?
Herramientas de código abierto
Resumen
Preguntas frecuentes
Presentar la detección de intrusión y Snort
Introducción
¿Cómo funciona un IDS?
¿Dónde encaja Snort?
Requisitos del sistema para Snort
Explorar las características de Snort
Usar Snort en su red
Consideraciones de seguridad con Snort
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Instalar y configurar Snort y sus componentes adicionales
Colocar su NIDS
Configurar Snort en Linux
Otros componentes adicionales de Snort
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Uso avanzado de Snort
Introducción
Monitorizar la red
Configurar vinculación de canales en Linux
Conjunto de reglas de Snort
Plug-ins
Plug-ins del preprocesador
Plug-ins de detección
Plug-ins de salida
Snort en línea
Resolver requisitos específicos de seguridad
Resumen
Soluciones por la vía rápida
Preguntas frecuentes

DESARROLLO CURRICULAR DE LA ACCIÓN FORMATIVA

Análisis de red, solución de problemas, y sniffer de paquetes
Introducción
¿Qué es el análisis de red y sniffer?
¿Quién usa analizadores de red?
¿Cómo funciona?
Sniffing sin hilos
Disección de protocolo
Protección contra los sniffers
Análisis de red y Políticas
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Principios básicos de la criptografía y encriptación
Introducción
Algoritmos
Conceptos usados en criptografía
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Seguridad de perímetro, las DMZ, Acceso remoto y las VPN
Introducción
Tipos de cortafuegos
Arquitecturas de cortafuegos
Implementar cortafuegos
Proporcionar acceso remoto seguro
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Host Bastion Linux
Introducción
Instalación del sistema
Eliminar componentes opcionales
Pasos adicionales
Control de acceso a los recursos
Auditar el acceso a los recursos
Administración remota
Configuraciones de host bastión
Soporte y mantenimiento del host bastión
Lista de comprobaciones del host bastión Linux
Resumen
Soluciones por la vía rápida
Preguntas frecuentes
Fortalecer el servidor Web Apache
Entender las vulnerabilidades comunes dentro del servidor Web Apache
Parches y seguridad del sistema operativo
Fortalecer la aplicación Apache
Monitorizar el servidor para un funcionamiento seguro