

AR421 - Análisis de Protocolos y Diagnóstico de Redes TCP/IP utilizando WireShark.

Sin lugar a dudas, las redes de datos TCP/IP están jugando un rol crítico en los negocios de las empresas actuales. Una buena salud de la red es un factor crítico de éxito de toda empresa moderna. Este curso presencial, que es dictado por un instructor con una reconocida trayectoria de más de 15 años en Internetworking, está orientado a detectar y corregir las falencias de rendimiento y seguridad que su red puede presentar..

El curso se concentra en la instalación y operación del software libre denominado Ethereal/Wireshark, y en cómo una aplicación como ésta, nos permite realizar un acabado análisis de protocolos y un diagnóstico adecuado de nuestra red TCP/IP. Se revisan tanto aspectos de rendimiento como aspectos de seguridad.

Al realizar el curso, el alumno estará capacitado para instalar y operar el analizador de protocolos Ethereal/Wireshark para realizar diagnósticos adecuados en su red y tomar las medidas correctivas correspondientes.

Objetivos:

Una vez finalizado este curso, el alumno podrá:

- Obtener e Instalar el software libre denominado Ethereal/Wireshark.
- Operar este software para determinar el estado de salud de su Red TCP/IP.
- Detectar y corregir eventuales anomalías que su red pueda presentar.
- Realizar capturas de trafico para su posterior análisis.
- Aplicar filtros de captura y despliegue al utilizar el analizador de protocolos.
- Determinar datos estadísticos y parámetros de operación normales de su red (Baseline)
- Visualizar cada paquete capturado en forma decodificada o en su despliegue hexadecimal / ASCII.
- Determinar los parámetros normales y anormales de los principales encabezados de la familia de protocolos TCP/IP
- Establecer los tiempos de respuesta de diversas aplicaciones.
- Determinar los riesgos de seguridad a los que eventualmente esta sometida su Red TCP/IP.

Contenido del curso:

1. Modelo OSI
2. Protocolos TCP/IP principales y estructuras de los encabezados
3. Dispositivos de Interconexión
4. Tecnologías Ethernet
5. Introducción a los analizadores de protocolo
6. Obtención e Instalación de Ethereal/Wireshark
7. Captura de tráfico
8. Definición de Filtros
9. Datos estadísticos
10. Baselining
11. Detección y corrección de fallas en : ARP, ICMP, IP, UDP, TCP, DNS, FTP, HTTP, DCHP
12. Información Experta
13. Tiempos de respuesta, RTT
14. Trabajo con archivos de captura
15. Documentación y análisis de una aplicación
16. Seguridad
17. Estudios de casos

Metodología

El curso se realizará en base a exposición del relator, demostraciones en vivo, laboratorios en vivo y estudios de caso.

Materiales

Los participantes recibirán los siguientes materiales:

Manual del alumno CD con software y documentación
Libro: Wireshark Network Analysis, de Laura Chappell



Audiencia:

Este curso está dirigido a:

- Administradores de redes TCP/IP
- Profesionales del área técnica responsables por la administración, configuración y soporte de redes corporativas TCP/IP
- Profesionales del área técnica interesados en conocer a fondo las características de TCP/IP, sus vulnerabilidades y anomalías
- Desarrolladores de aplicaciones que utilizan TCP/IP como plataforma
- Profesionales del área de auditoría de Seguridad y Redes de Datos

Requisitos:

Para un beneficio óptimo del curso AR421, debiera tener los siguientes conocimientos previos.

- Asistencia al curso DC800 - Comunicaciones e Internetworking o conocimientos equivalentes
- Asistencia al curso DC513 - TCP/IP Conectividad Multiplataforma o conocimientos equivalentes
- Modelo OSI
- Protocolos TCP/IP
- Direccionamiento IP
- Lectura Avanzada de Inglés Técnico.

Información General

Duración: 40 Horas

Valor: 48 UF

Consultas e Inscripciones

Mesa Central : (56-2) 334-5755

Fax : (56-2) 334-5847

Relator:

Ricardo Segal Kirberg

Ingeniero Civil Electricista de Universidad de Chile



Ha ocupado diversos cargos en empresas del área de informática, destacando: Gerente de Ingeniería y Desarrollo, Gerente Técnico y Gerente de Proyectos de Computerland y Gerente General de Computadores Personales Ltda. Ha participado, durante los últimos veinte años, en importantes proyectos de redes de área local, comunicaciones, e-learning y ASP. Ha sido profesor y expositor en diversos cursos y seminarios sobre temas tales como Perspectivas y tendencias de la Computación Personal, Redes de Área Local, Comunicaciones y Conectividad, Routers y Switches Cisco. En los últimos años ha participado en Congresos Mundiales de e-Learning, como relator de cursos en la modalidad blended e-learning y ha actuado como Consultor Senior en diversos proyectos de e-learning. Es profesor certificado Novell, Microsoft y Cisco. Ha realizado diversas asesorías a empresas chilenas en las áreas de Internetworking y uso estratégico de las Tecnologías de la Información.

Ha sido Director de la Asociación Chilena de Empresas de Tecnología de la Información (ACTI A.G.) y Presidente de la ACE, entidad que agrupa a empresas de e-Learning en ACTI.

Actualmente se desempeña como Socio y Consultor de LABC.