ANÁLISIS DE PROTOCOLOS MEDIANTE WIRESHARK

Duración: 3 días, 21 horas

Este curso presenta las funcionalidades de la herramienta WireShark pero haciendo foco en el funcionamiento de las aplicaciones en red para entender los problemas que pueden presentar los protocolos de la pila TCP/IP y hacer análisis de rendimiento.

Por tanto, es un curso de protocolos IP analizados mediante aplicación WireShark

Guión del Curso

- Herramienta Wireshark, presentación.
- Implementaciones de la aplicación wireshark en entornos de prueba, profesional (appliances) e integrados en dispositivos de red.
- Conjunto de herramientas adicionales a Wireshark para análisis de tráfico en la red.
- Capturas de tráfico. Generación de tráfico espejo. Limitaciones HW
- Cabeceras. Esta parte es esencial, porque Wireshark nos presenta disección de cabeceras que habremos de analizar para entender los flujos de tráfico de usuario o/y control.

    1. Cabeceras de capa OSI 2:
        - Trama ethernet Comercial V2
        - Trama ethernet IEEE 802.2 y variantes
        - Etiquetado de VLANs IEEE 802.1q/p
        - Spanning-Tree
        - Protocolos de descubrimiento: IEEE LLDP, …
    2. Cabeceras de capa OSI 3:
        - IP
        - ARP
        - IP-ICMP
        - IPv6

3. Cabeceras de capa OSI 4:

    - TCP --> A esta cabecera se le dedica mayor extensión de tiempo para presentar el análisis de control de congestión (tres modos) y del uso del buffer de la ventana deslizante.
    - UDP
    - IPSec
    - SSL
    - Routing

- Cabeceras de capas superiores de OSI: Sólo se presentan algunos ejemplos como https, ftp, smtp, dns, … porque es un campo casi infinito por la multitud de aplicaciones.

- Elección de puntos de captura para Wireshark

- Uso avanzado de Wireshark: Filtros y presentación de tramas

- Estadísticas: Métricas y curvas

- Medidas de latencia

- Identificación y análisis de flujos: Estudio de concordancia de estos flujos con los parámetros de configuración de QoS.

Ejemplos de capturas reales

Laboratorios:

Lab 1: Conocer el estado actual de la Red IP
Lab 2: Obtener y analizar datos de la Red TCP/IP. Herramientas de análisis
Lab 3: Capturas en Switches y Routers. SPAN y RSPAN, RMON
Lab 4: Entorno de interface y configuración de Wireshark
Lab 5: Análisis de tráfico con Wireshark
Lab 6: Análisis de Spanning Tree, VLANs, Trunks, VTP
Lab 7: Análisis de Protocolos de Routing
Lab 8: Aplicaciones: DHCP, DNS, FTP, TFTP, SMTP, SNMP, Syslog,
Lab 9: Aplicaciones www: http y https (con y sin Proxy)
Lab 10: Métricas de wireshark, curvas y análisis de latencia
Lab 11: Análisis y gestión de entornos Multicast. Protocolo IGMP y PIM