

INCIDENCIAS EN REDES LOCALES

TIPOS DE INCIDENCIAS

Incidenencias físicas

Incidenencias lógicas *

Fallos de: Tarjetas de red, Cables, Dispositivos de interconexión

Ataques de seguridad, software espía, correo spam

* Importancia medidas prevención: Antivirus actualizados, uso cortafuegos, acceso equipos protegidos por contraseñas,...

VER Ad-Aware en Herramientas de Diagnóstico - Aplicaciones

MONITORIZACIÓN DE REDES

Herramientas disponibles

Comprobadores de red: Continuidad de cables y otros parámetros

Monitores de red (s.o.): Mapas de actividad (carga) de la red

Analizadores de red: Rastreo tráfico (arg. y prot.) de la red

Windows: Monitor de rendimientos de Windows:

Ctrl+ALT+Sup; Administrador de tareas -

- Rendimiento - Monitor de Recursos

Linux (Ubuntu): Menú del Sistema - Administración -

- Monitor del sistema - Monitor de Rendimiento

Programas: Wireshark (antes Ethereal)

Redes inalámbricas: Aircrack-ng, ERW,

NetStumbler, Kismet, Aircrack-ng.

Protocolos SNMP

En un entorno SNMP (capa Aplicación OSI) unos programas monitorizan el tráfico de la red y recopilan datos estadísticos en bases de datos (MIB) que son analizadas periódicamente.

Programas que usan el protocolo SNMP:

OpenView de HP, SysUpTime para Windows y Linux.

Logs del sistema

Fichero en el que se registra lo que sucede en un determinado sistema durante un intervalo de tiempo específico. Son generados por el s.o. y otras aplicaciones: Datos monitorización de red, tráfico de paquetes, colisiones, fallos, etc que pueden ser analizados por el administrador de la red.

Windows: Inicio - Panel de Control - Herramientas Administrativas -

- Visor de Eventos

Linux: Entorno gráfico: KSystemLog

Los logs se guardan en el directorio /var/log

HERRAMIENTAS DE DIAGNÓSTICO

Aplicaciones

Chequear estado de un equipo y limpiarlo

Ad-Ware: Programa anti-espía (spyware, adware, troyanos, etc.)

Linux: Backtrack: Seguridad redes generales e inalámbricas.

WifiWay: Seguridad redes inalámbricas, bluetooth, radio.

WifiSlax: Seguridad redes inalámbricas y generales

Windows

Herramientas de red: Propiedades de red - Panel de Control - Centro de redes y Recursos Compartidos

Comandos de Consola (cmd)

Net: Diagnóstico funcionamiento red, y acceso a recursos compartidos. Variantes:

Net Send, Start, Stop, Share, View, Sessions, Time*/SET, User, Localgroup

Netstat: Muestra conexiones activas en el equipo. Variantes:

Netstat -a, -e, -n, -o, -p, -s

Comandos de red (y variantes)

Ipconfig /all, /renew, /release, /registerdns, /flushdns

Ping, -t, -a, -l, -n, -i, TTL, -r, -v

Tracert, -d, -h

Route PRINT, ADD, DEL, CHANGE

Linux

Herramientas de red:

Menú Administración

Herramientas de red

Monitor del sistema (se encuentra el Monitor de Rendimiento)

Comandos: En Ubuntu

Menú Aplicaciones - Accesorios - Terminal, se pueden utilizar:

Ipconfig: Configuración de red del adaptador, y su modificación.

Ip: Consulta configuración TCP/IP, y encaminamiento, permite ciertas modificaciones

Route: Consultar y establecer parámetros de enrutamiento.

Ping: Conexión/Conectividad entre equipos.

Netstat: Consultar puertos abiertos o a la escucha.