Gestión de Logs y monitorización de la seguridad de red

Monitorización y análisis de trafico

- *Sistema de monitorización de trafico (NMS):* Supervisión de una red de comunicaciones activa con el fin de diagnosticar problemas y recopilar estadísticas para la administración y configuración detallada de la red.

Objetivos

- Identificación de servicios o servidores no oficiales
- Seguimiento de estadísticas de uso y trafico
- Solución de problemas de su red
- Investigar incidentes de red
- Investigar incidente de seguridad
- Mantener registros de usuarios para "gestión" de la responsabilidad

Herramientas básicas

- Ping: Saber si un servidor DNS esta activo o no
- Traceroute: Traza de saltos por los que pasan los paquetes IP de origen a destino

MRTG (Multi Router Traffic Grapher)

- Monitoriza la carga de trafico en los enlaces de red
- Genera paginas HTML con información visual en directo
- Usa SNMP
- Herramientas:
  - Linux-mrtg
  - cacti
    - Monitoriza, almacena y muestra estadísticas de red y servidor
    - Emplea RRDTool para representar graficamente
  - PRTG
  - munin
  - observium

SNMP

- Protocolo creado para el descubrimiento/Información de dispositivos de redes IP
- Recopilación y organizar información sobre los dispositivos gestionados en redes IP
- Se puede usar SNMP para cambiar el comportamiento del dispositivo gestionado