Departamento de Seguridad Informática MINSAP

Febrero 2018

Volumen 1, nº 1

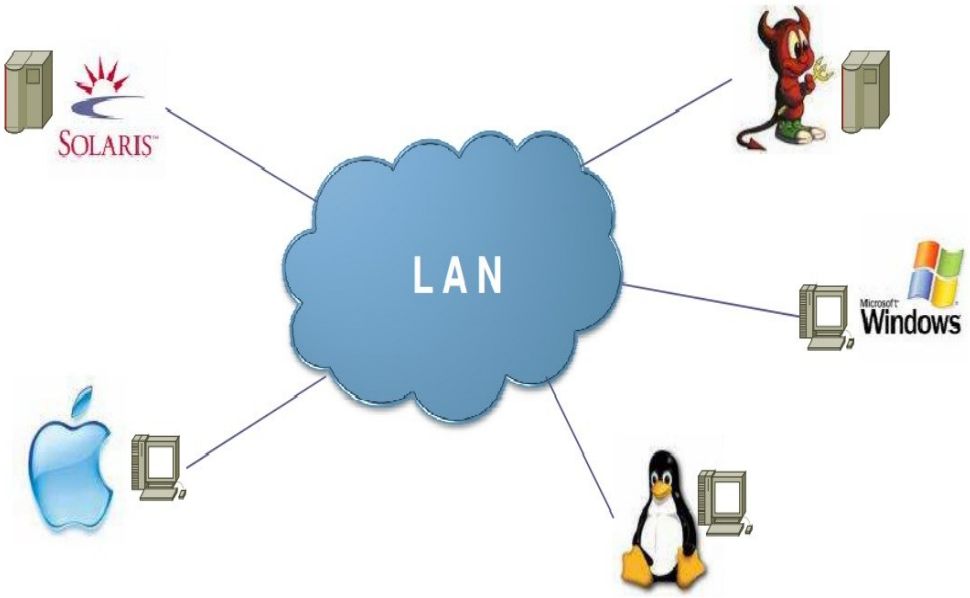
Boletín de Seguridad Informática

Contenido:

Curso de Redes-Parte 2

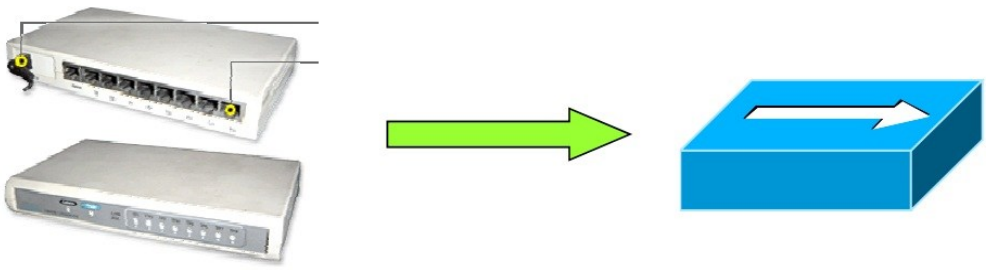
Componentes básicos de una red LAN

• Computadores (Hosts): Son quienes inician y procesan la información proveniente de sus pares.



• Hub (Concentrador):

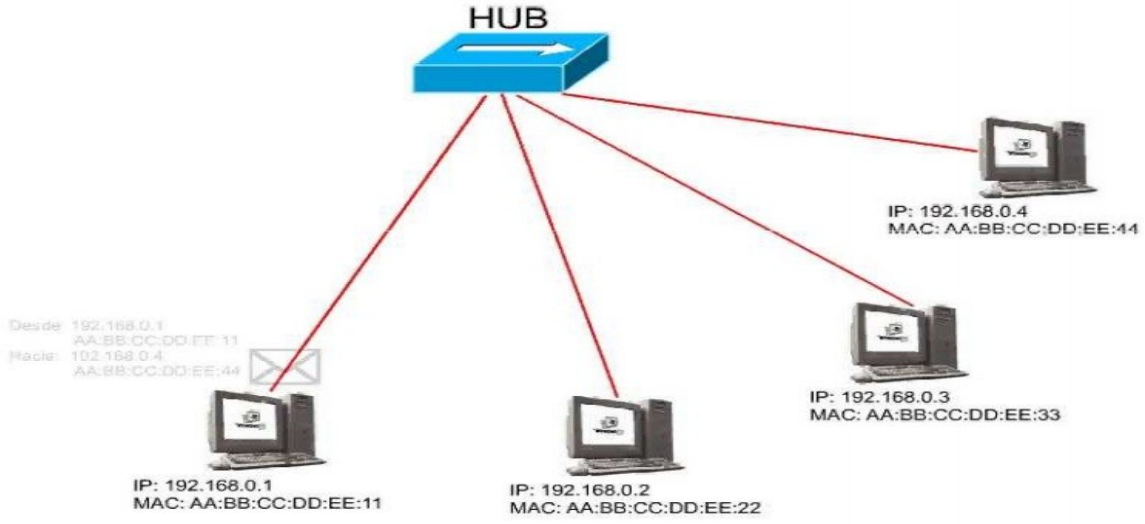
Permite conectar entre sí otros equipos y retransmite la información que recibe desde cualquiera de ellos a todos los demás.



Puntos de interés especial:

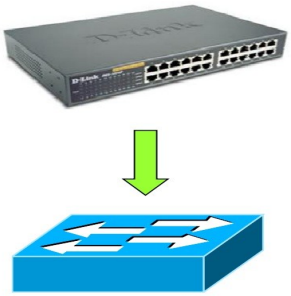
Otras herramientas como Snort, OSSIM así como multitud de IDS/IPS permiten alertar sobre algunos de los problemas y ataques expuestos en esta guía. No obstante, cuando se necesita analizar tráfico en profundidad o hay que auditar un entorno en el que el tiempo prima, dichas herramientas suelen carecer de la flexibilidad que nos ofrece un analizador de protocolos como Wireshark.

Funcionamiento de un HUB.

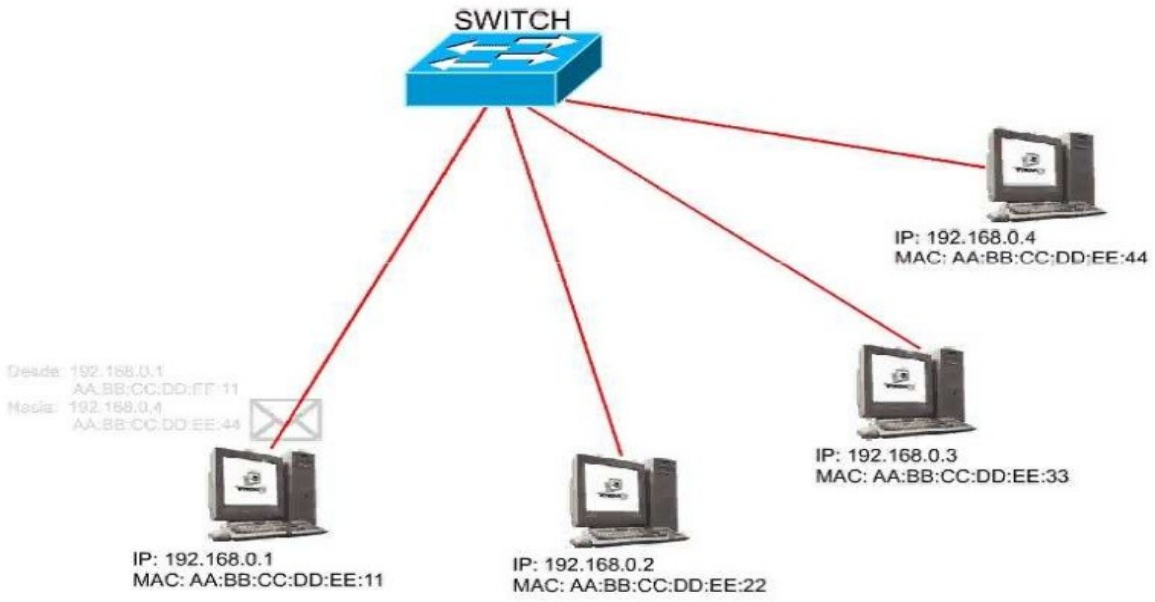


Componentes básicos de una red LAN

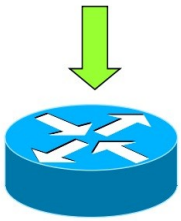
• Switch (Conmutador): Un switch entrega datos de acuerdo a la dirección de destino.



Funcionamiento de un switch

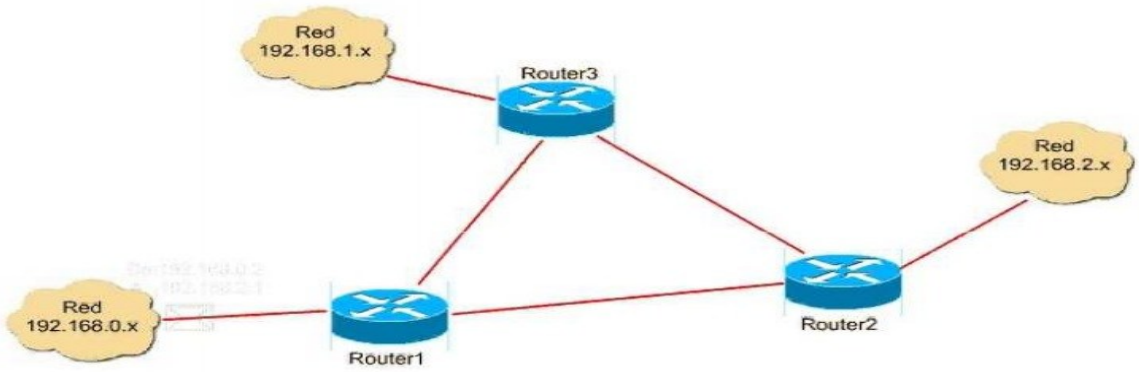


Componentes básicos de una red LAN



- Router (Enrutador): Interconecta trozos o redes enteras. Toma redes enteras. Toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red.

Funcionamiento de un router



Dirección IP (Internet Protocol)

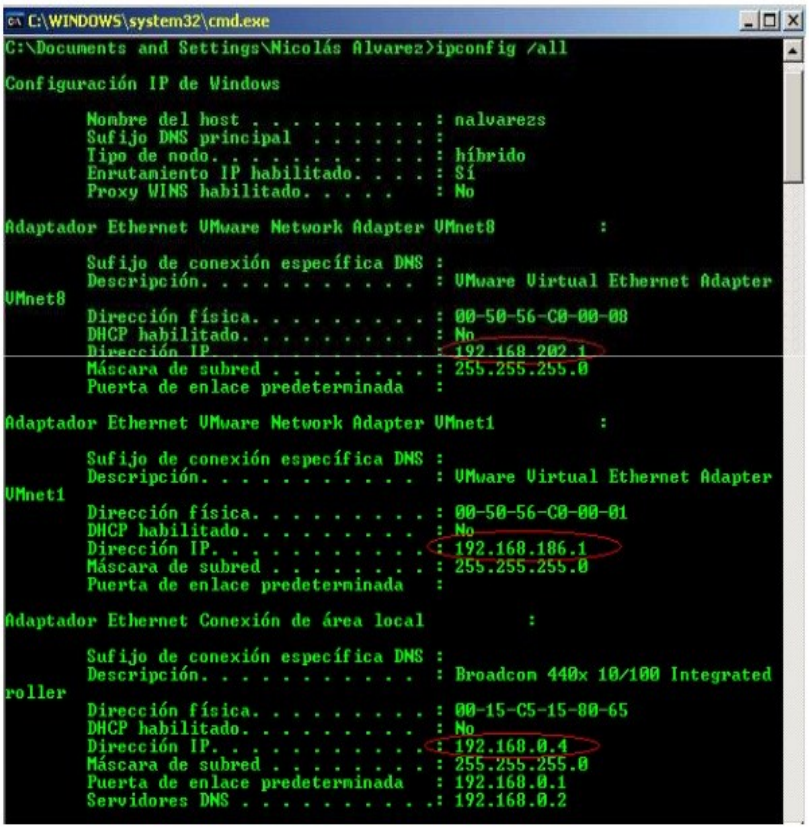
• Es un número que identifica a una interfaz de un dispositivo dentro de una red que de una red que utilice el protocolo IP(Internet Protocol).

Ejemplo:

200.104.172.117

192.168.0.1

127.0.0.1



ANÁLISIS DE TRÁFICO CON WIRESHARK

1. ANÁLISIS DE TRÁFICO

Seguramente todo administrador de redes ha tenido que enfrentarse alguna vez a una pérdida del rendimiento de la red que gestiona. En ese caso sabrá que no siempre es sencillo, por falta de tiempo y recursos o por desconocimiento de las herramientas apropiadas, tener claros los motivos por los que esto ha sucedido. En ocasiones, incluso se ha podido llegar a perder la conectividad o bien ciertos equipos han podido desconectarse sin motivo aparente.

En la mayoría de ocasiones, las causas de estos problemas tienen un origen no premeditado y se deben a una mala configuración de la red como puede ser tormentas broadcast, spanning-tree mal configurado, enlaces redundantes, etc. Pero, en otras ocasiones, puede tratarse de ataques inducidos por terceros que pretenden dejar fuera de servicio un servidor web mediante un ataque DoS, husmear tráfico mediante un envenenamiento ARP o simplemente infectar los equipos con código malicioso para que formen parte de una red zombi o botnet.

En cualquier caso, conocer el origen del incidente es el primer paso para poder tomar las contramedidas necesarias y conseguir una correcta protección. En este punto , los analizadores de tráfico pueden resultar de gran utilidad para detectar, analizar y correlacionar tráfico identificando las amenazas de red para, posteriormente, limitar su impacto. Con tal propósito, existen en el mercado dispositivos avanzados como el appliance MARS (Monitoring, Analysis and Response System) de Cisco o IDS/IPS basados en hardware de diversos fabricantes. Pero estas soluciones no siempre están al alcance de todas las empresas ya que su coste puede que no cumpla un principio básico de proporcionalidad (el gasto es superior al beneficio obtenido) y, por lo tanto, no se justifique su adquisición.

Por ello, y para cubrir las necesidades de entidades con infraestructuras tecnológicas más modestas, INTECO-CERT presenta esta «Guía de análisis de tráfico con Wireshark». Tiene por objeto sensibilizar a administradores y técnicos de las ventajas de auditar la red con un analizador de tráfico, principalmente utilizando la herramienta libre Wireshark. Además, ofrece ejemplos prácticos de ataques en redes de área local bastante conocidos y que actualmente siguen siendo uno de los mayores enemigos en los entornos corporativos.El presente documento está dividido en una serie de apartados que tratan diversos ataques reales llevados a cabo en redes de área local, como son ARP Spoof, DHCPFlooding, DNS Spoof, DDoS Attacks, VLAN Hopping, etc. En ellos se emplea Wireshark como herramienta principal de apoyo para ayudar a detectar, o al menos acotar en gran medida, los problemas generados por dichos ataques. Asimismo, se proponen diversas acciones de mitigación para cada uno de los casos expuestos.

2. ¿POR QUÉ WIRESHARK?

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix.

Conocido originalmente como Ethereal, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red. Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente (versión 1.4.3); y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark "entiende" la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico.

De forma similar a Tcpdump, Wireshark incluye una versión en línea de comandos, denominada Tshark, aunque el presente documento se centrará únicamente en su versión gráfica. Es importante indicar también que las funcionalidades utilizadas en el presente informe solo representan una pequeña parte de todo el potencial que puede ofrecernos Wireshark, y cuyo objetivo principal es servir de guía orientativa para cualquier administrador que necesite detectar, analizar o solucionar anomalías de red. Pueden existir situaciones en las que Wireshark no sea capaz de interpretar ciertos protocolos debido a la falta de documentación o estandarización de los mismos, en cuyo caso la ingeniería inversa será la mejor forma de abordar la situación. Otras herramientas como Snort, OSSIM así como multitud de IDS/IPS permiten alertar sobre algunos de los problemas y ataques expuestos en esta guía. No obstante, cuando se necesita analizar tráfico en profundidad o hay que auditar un entorno en el que el tiempo prima, dichas herramientas suelen carecer de la flexibilidad que nos ofrece un analizador de protocolos como Wireshark.