Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Tcpdump, ethereal y snort
Herramientas para conocer tu red

Hugo Francisco González Robledo
Centro de Telecomunicaciones
Instituto Tecnológico de San Luis Potosi
hugo.gonzalez@itslp.edu.mx
http://ardilla.zapto.org
Mayo 2005

CICOL 2005

Analizadores de Protocolos

Hugo Francisco González Robledo
Centro de Telecomunicaciones
Instituto Tecnológico de San Luis Potosi
hugo.gonzalez@itslp.edu.mx
http://ardilla.zapto.org
Mayo 2005

CICOL 2005

Agenda

- La importancia de conocer tu red
- Repaso del protocolo TCP/IP
- Introducción al Análisis de protocolos
- Sniffers
- Tcpdump
- Ethereal
- Snort

La importancia de conocer tu red

- Para administradores de red ...
  - Detección de fallas
  - Detección de anomalias
  - Detección de vulnerabilidades
- Para usuarios avanzados ...
  - Depuración de protocolos
  - Depuración de aplicaciones
- Para “intrusos” ...
  - ¡¿?!

Un forma adecuada para solucionar problemas de red involucra los siguientes 7 pasos:

- Reconocer los síntomas.
- Definir el problema.
- Analizar el problema.
- Aislar el problema.
- Identificar y probar la causa del problema.
- Solucionar el problema.
- Verificar que el problema ha sido resuelto.

Repaso de TCP/IP

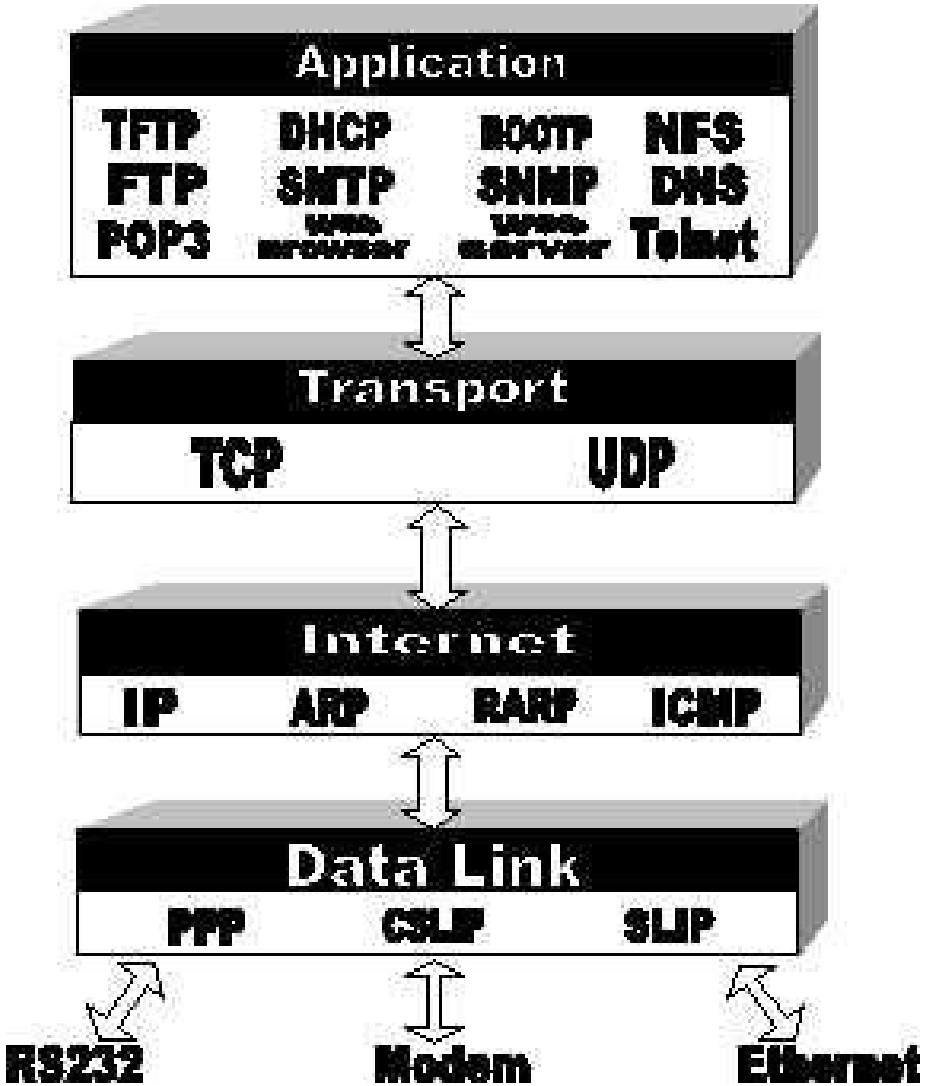
- Los protocolos que comunican al mundo.
- Existen 2 versiones:
  - IPv4
  - IPv6
- La más usada es IPv4, pero los analizadores ya están listos para identificar y ver IPv6 .

- A que parte le debo poner más atención.

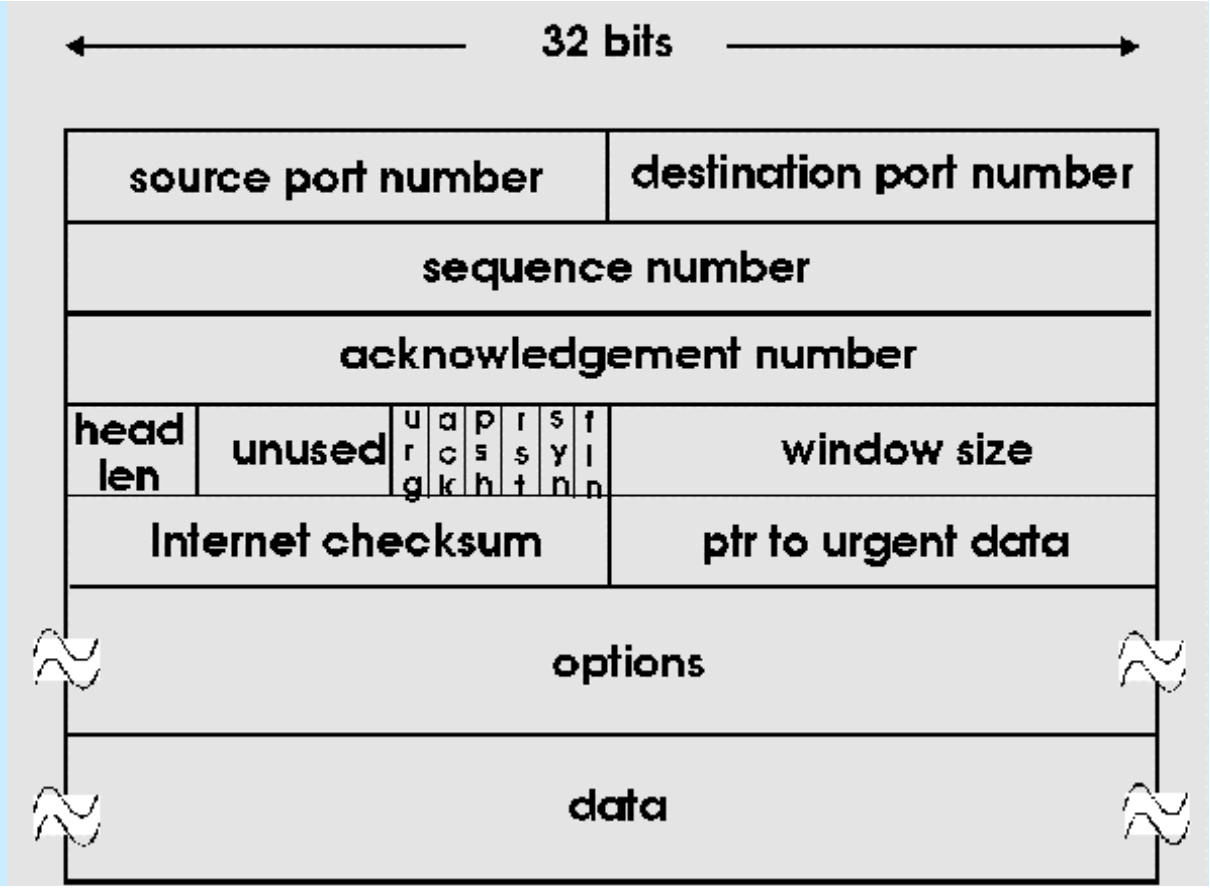
OSI vs TCP/IP

Application (X.400, FTAM, VT)	Applications SMTP, TELNET, FTP
Presentation	
Session	
Transport	Transport (Transmission Control Protocol)
Network	Internet (Internet Protocol)
Data Link	Network Interface
Physical	Hardware

TCP/IP


Application
TFTP
DHCP
BOOTP
NFS
FTP
SMTP
SNMP
DNS
POP3
Web browser
Web server
Telnet
Transport
TCP
UDP
Internet
IP
ARP
RARP
ICMP
Data Link
PPP
CSLIP
SLIP
RS232
Modem
Ethernet

TCP


32 bits
source port number
destination port number
sequence number
acknowledgement number
head len
unused
urg
ack
psh
rst
syn
fin
window size
Internet checksum
ptr to urgent data
options
data

Introducción al análisis de Protocolos

- COSAS que me gustaría identificar
  - Segmentos de red.
  - Gateway
  - Servidores DNS
  - Servidores de Correo
  - Servidores Web.
  - Ataques
  - Funcionamiento sospechoso

Introducción al análisis de Protocolos

- COSAS que debo saber
  - Fundamentos de redes
  - Protocolos
  - Herramientas
  - ?

Puntos a considerar

- La topologia de la red es importante para analisis de protocolos.
- El funcionamiento de Ethernet.
  - Repite
  - Si no es para la maquina, la descarta
- Los sniffers usan modo promiscuo

Hubs

- Son repetidores, lo que entra a un puerto, va redirigido a todos los demas.
-

Switchs

- Son “más” inteligentes, forman “caminos” entre los puertos.

Tcpdump

- Tcpdump es un sniffer o husmeador de red.
- Captura la información que pasa sobre el cable.
- La información te la da en formato “crudo”.
- Puedes guardar la información tal y como pasa por la red.
- Tiene filtros.
- Puedes ver el contenido.
- Puedes ver la información remotamente.

Filtros tcpdump

- Ejemplos de filtros usando TCPdump
  - Host
  - Fuente
  - Destino
  - Protocolo
  - Banderas
- Filtros avanzados

Tcpdump

- Usando Tcpdump, parte interactiva

Ethereal

- Analizador de protocolos o sniffer de más nivel
- Una gran ventaja es la interface gráfica.
- Te permite dar seguimiento a conexiones.
- Puede ser en tiempo real ....
- Puedes leer lo que guardaste con tcpdump.
- Análisis de tráfico, protocolos usados
- Identificación de elementos de la red.

Divisiones de Ethereal

- Contiene 3 elementos principales
  - La parte de información general.
    - Numero de paquete
    - Hora
    - Fuente
    - Destino
    - Protocolo
    - Info general
  - Descripción detallada de los protocolos
  - Información “cruda” de la captura

Los filtros

- Los filtros de Ethereal son como los de tcpdump en el modo de captura, y aún más extensos en el modo de display.
  - Pueden capturar diferentes tipos de tráfico
  - Pueden capturar diferentes protocolos
  - Pueden capturar diferentes puertos
  - Pueden capturar diferentes fuentes, destinos
    - Ejemplos de filtros

Ethereal

- Ejemplo interactivo

Snort

- Snort es más complejo.
- Puede funcionar como sniffer (parecido a tcpdump)
- O como escaner de red
- O como detector de intrusos
- O como sistema de prevención de intrusos

Snort

- Ejemplos de Snort

Conclusiones

- El tráfico se puede capturar por etapas, para ir analizando que pasa en la red.
- Conocer el estado de la red, permite identificar problemas, y posibles malos usos.
- También agujeros de seguridad y fallas de diseño.

Preguntas y Respuestas