Sniffers

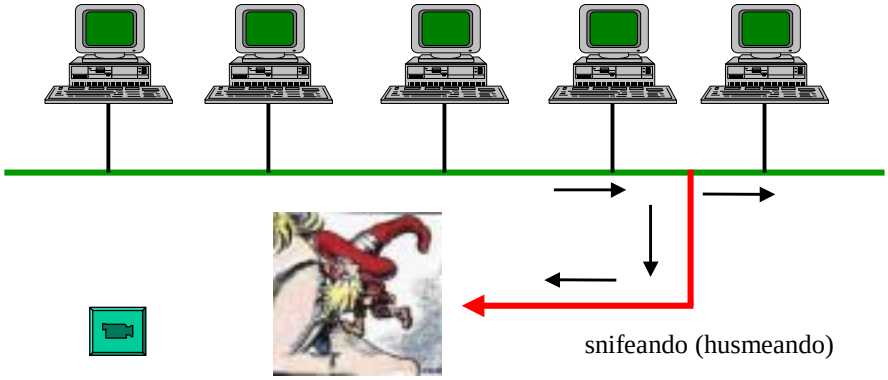
Roberto Gómez Cárdenas
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez

Sniffers y Analizadores

- Un sniffer es un proceso que "olfatea" el tráfico que se genera en la red *a nivel de enlace*;
  - puede leer toda la información que circule por el tramo de red en el que se encuentre.
  - se pueden capturar claves de acceso, datos que se transmiten, numeros de secuencia, etc...
- Un analizador de protocolos es un sniffer al que se le ha añadido funcionalidad suficiente como para entender y traducir los protocolos que se están hablando en la red.
  - debe tener suficiente funcionalidad como para entender las tramas de nivel de enlace, y los paquetes que transporten.
- Diferencia:
  - normalmente la diferencia entre un sniffer y un analizador de protocolos, es que el segundo está a la venta en las tiendas y no muestra claves de acceso.

Sniffers

¿Cómo se comunican dos computadoras en una red local?



snifeando (husmeando)

computadora en modo promiscuo

Lámina 3 Roberto Gómez Cárdenas

Lectura a nivel enlace

- El sniffer se dedica a leer TRAMAS de red.
- Los datos que obtendremos de él serán tramas que transportarán paquetes (IP, IPX, etc...).
- En estos paquetes se incluyen los datos de capas superiores
  - entre ellos los de la capa de aplicación (posiblemente claves de acceso).
- Para efectos prácticos en este presentación se hablará de *paquetes.*

Lámina 4 Roberto Gómez Cárdenas

Lista sniffers para Windows

- Ethereal
- WinDump
- Network Associates Sniffer (for Windows)
- WinNT Server (Network Monitor)
- BlackICE Pro
- CiAll
- EtherPeek
- Intellimax LanExplorer
- Triticom LANdecoder32
- SpyNet/PeepNet
- Analyzer: a public domain protocol analyzer

Lámina 5 Roberto Gómez Cárdenas

Lista Sniffers para Macintosh

- EtherPeek
  - http://www.aggroup.com/
  - EtherPeek has been around for years in a Macintosh version and has also ported their software to Windows.

Lámina 6 Roberto Gómez Cárdenas

Lista Sniffers para Unix

- esniff.c (phrack 45)
- tcpdump
- Linsniffer
- Linuxsniffer.
- Hunt
- Sniffit
- netXray
- Ethereal
- snoop
- snort
- trinux
- karpski
- SuperSniffer v1.3
- esniff
- exdump

Lámina 7 Roberto Gómez Cárdenas

Lista snifferes DOS

- Sniffer(r) Network Analyzer
  - http://www.nai.com
- The Gobbler and Beholder
  - http://nmrc.org/files/msdos/gobbler.zip
- Klos PacketView
  - http://www.klos.com

Lámina 8 Roberto Gómez Cárdenas

El sniffer ethereal

http://www.ethereal.com

Lámina 9 Roberto Gómez Cárdenas

Ethereal

- Ethereal es un analizador de tráfico de red, o "sniffer", para sistemas operativos Unix y sistemas basados en Unix, así como sistemas Windows
- Utiliza:
  - GTK+, una libreria que provee una interface de usuario grafica,
  - libpcap,una libreria para filtrar y capturar paquetes,
- Posee la posibilidad de ver la reconstruccion del fluido de una sesión TCP.
- Autor: Gerald Combs (julio 1998 - version 0.2.0.)

Lámina 10 Roberto Gómez Cárdenas

Plataformas

- AIX
- Tru64 Unix (formalmente Digital Unix)
- Debian GNU/Linux
- Red Hat Linux
- FreeBSD
- NetBSD
- OpenBSD
- HP/UX
- Sparc / Solaris 8
- Windows 2000, Windows NT y Windows Me/98/95

Lámina 11 Roberto Gómez Cárdenas

Versión y download

- Posible obtenerlo de
  - http://www.ethereal.com
- Requisitos
  - GTK+, el GIMP Tool Kit y Glin
  - libpcap (www.tcpdump.org)
- Unix
  - rpm, paquetes debian. .tar.gz
- Windows
  - winpcap (www.polito.it)

Lámina 12 Roberto Gómez Cárdenas

Características

- Datos pueden ser capturados del cable de una conexión viva, o leídos de un archivo capturado.
- Necesario tener máximos privilegios para usarlo
- Puede leer archivos de datos de diferentes paquetes de captura de datos
  - tcpdump (libpcap), NAI's Sniffer™ (compressed and uncompressed), Sniffer™ Pro, NetXray™, Sun snoop and atmsnoop, Shomiti/Finisar Surveyor, AIX's iptrace, Microsoft's Network Monitor, Novell's LANalyzer, RADCOM's WAN/LAN Analyzer, etc

Lámina 13 Roberto Gómez Cárdenas

Más características

- Datos pueden ser capturados de Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM, e interfaces tipo loopback
  - no todos los tipos son soportados en todas las plataformas
- Datos pueden verse a través de un GUI o de una terminal en texto plano.
- La salida puede ser guardada o impresa como texto plano o Postcript
- Toda, o parte, de la captura puede ser almacenada en disco.
- Se cuenta con una guía del usuario en html

Lámina 14 Roberto Gómez Cárdenas

Principales ventanas ethereal

- Panel alto (list pane)
  - "summary" de cada paquete capturado
  - eligiendo en esta ventana se despliega las otras dos
- Panel de en medio (tree view)
  - despliega paquete seleccionado en el panel superior pero en más detalle
- Panel bajo (data view)
  - despliega datos del paquete seleccionado en el panel alto, y "highligths" el campo seleccionado en el panel de enmedio

Lámina 15 Roberto Gómez Cárdenas

Los tres paneles de ethereal

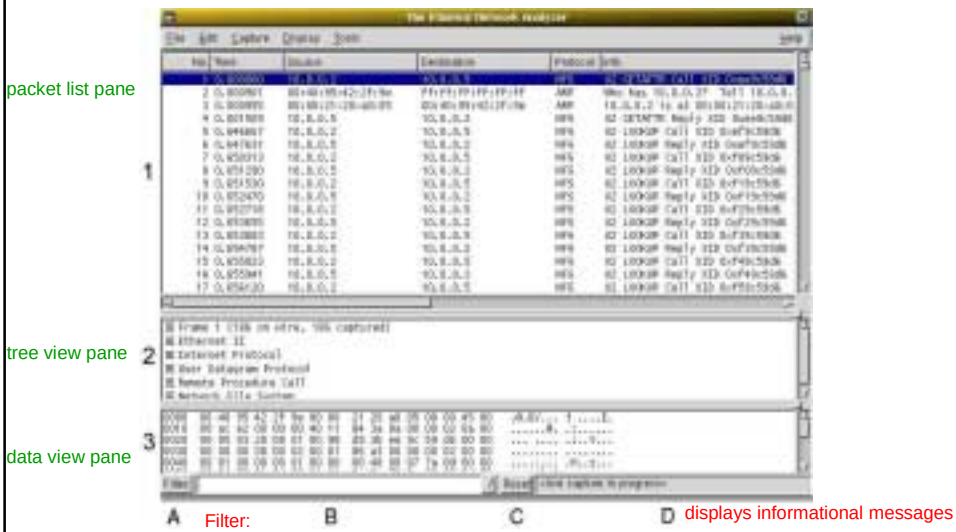


Lámina 16 Roberto Gómez Cárdenas

Los menús principales de ethereal

- File
  - abrir, guardar archivos de captura, imprimir archivos captura, etc.
- Edit
  - encontrar un frame, ir a un frame, marcar uno o más frames, asignar preferencias, crear filtro y activar/desactivar disección protocolos
- Capture
  - empezar/terminar captura de paquetes
- Display
  - desplegar plugins, seguir un stream TCP, obtener un resumen de los paqueres capturados, desplegar estadísticas de protocolos, colorear frames
- Help
  - ayuda básica de ethereal

Lámina 17 Roberto Gómez Cárdenas

Lanzando ethereal

- Dos métodos para capturar paquetes con ethereal
  - En la línea de comandos teclear

    # ethereal –i eth0 -k
  - Arrancar ethereal y seleccionar Start... del menú de captura
    - se despliega menú de preferencias de captura

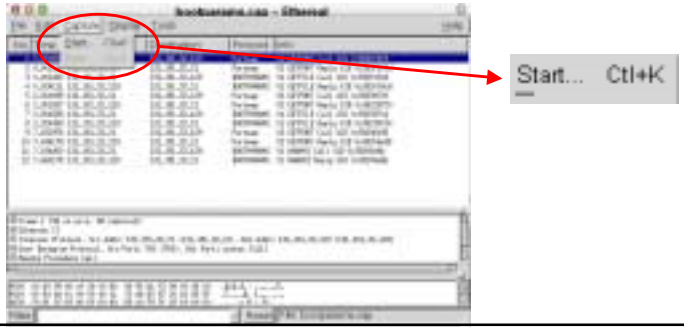
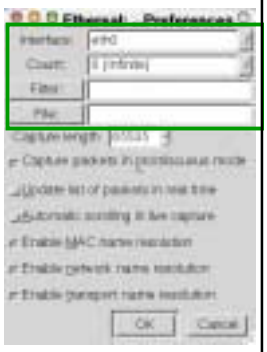


Lámina 18 Roberto Gómez Cárdenas

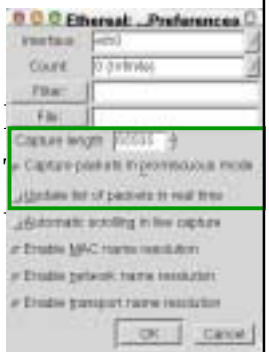
El cuadro de dialogo de captura (1/4)



- Interface especifica la interfaz de captura
  - solo se puede capturar en una interfaz
  - en algunas sistemas no es posible usar interfaces tipo loopback
  - misma función que la opción –i <interface>
- Count número de paquetes a capturar
  - numero por default: 0, que significa que no pare de capturar
- Filter especificar un filtro de captura
- File nombre archivo donde se va a almacenar los paquetes capturados

Lámina 19 Roberto Gómez Cárdenas

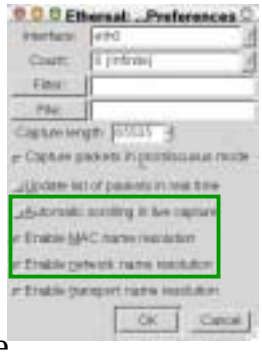
El cuadro de dialogo de captura (2/4)



- Capture length máxima cantidad de datos a capturar en cada paquete (snaplen)
  - default: 65535
  - al menos la MTU de la interfaz usada
- promiscous interfaz en modo promiscuo
  - si no es especificada solo se capturan paquetes que salen o llegan a ala computadora (no todos los paquetes que pasen por ahí)
- update actualizar el panel de paquetes en tiempo real
  - en caso contrario no se despliega ningún paquete hasta que se detenga la captura

Lámina 20 Roberto Gómez Cárdenas

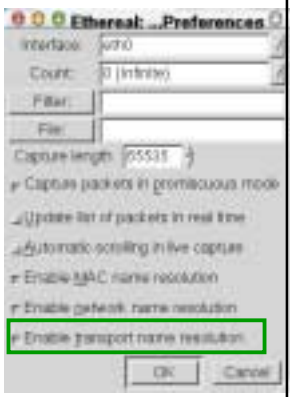
El cuadro de dialogo de captura (3/4)



- automatic ... ethereal scroll el panel de paquetes conforme llegan nuevos
  - siempre se ve el último paquete
  - en caso contrario se añaden paquetes nuevos al final de la lista pero no se lleva a cabo ningún scroll
- enable MAC traducción de los primeros tres bytes de la dirección MAC en nombre del fabricante (IETF)
- enable Network traducción direcciones IP en nombre dominio DNS

Lámina 21 Roberto Gómez Cárdenas

El cuadro de dialogo de captura (4/4)



- enable transport traducción de número de puertos en protocolos

Lámina 22 Roberto Gómez Cárdenas

Filtrados de paquetes

- Dos tipos de filtros
  - a nivel captura
  - a nivel despliegue

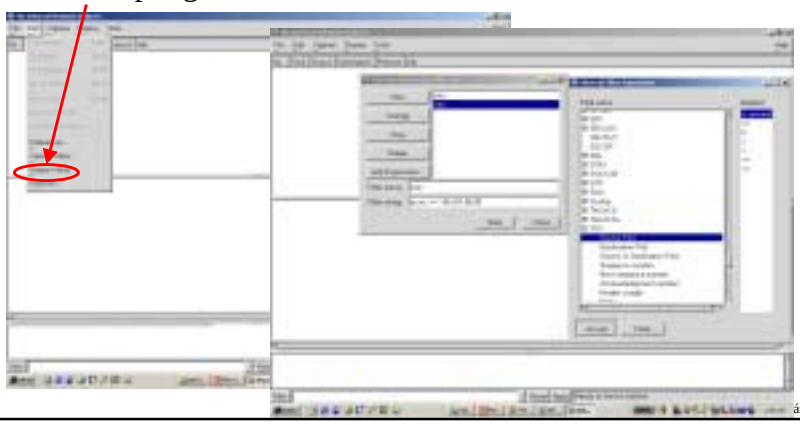


Lámina 23 ...árdenas

Filtrando paquetes en la captura

- Ethereal utiliza lenguaje libpcap para definir sus filtros.
  - mayor información man page de tcpdump
- Filtro se define en el campo filter de las preferencias del cuadro diálogo captura
- Un filtro esta formado por una serie de expresiones primitivas conectadas por conjunciones:

  [not] primitiva [and | or [not] primitiva ...]

- Ejemplos

  tcp port 23 and host 10.0.0.5

  tcp port 23 and not host 10.0.0.5

Lámina 24 Roberto Gómez Cárdenas

Lista de primitivas (1/3)

- [src| dst] host <host>
  - filtra un host, por IP o por nombre
  - opciones src, dst especifica tráfico entrada o salida
- ether [src | dst] host <ehost>
  - filtro de direcciones ethernet
- gateway host <host>
  - filtrar paquetes que usan host como gateway
  - dirección ethernet fuente o destino es host pero no la dirección fuente ni la destino es host
- less | greater <length>
  - filtra paquetes de longitud menor o igual a un determinado valor
  - paquetes que son mayores o iguales a un determinado valor

Lámina 25 Roberto Gómez Cárdenas

Lista de primitivas (2/3)

- [src | dst] net <net> [{mak <mask>} | {len<len>}]
  - filtrar en número de red
  - opciones src, dst especifica tráfico entrada o salida
  - posible especificar netmask de la red
- [tcp | udp] [src | dst] port <port>
  - fltrar en números de puerto TCP y UDP
  - opciones src, dst especifica tráfico entrada o salida
  - opciones tcp, udp especifica paquetes TCP o UDP
  - tcp, udp debe aparecer antes que src, dst
- ip | ether proto <protocol>
  - filtrar a nivel IP o ethernet

Lámina 26 Roberto Gómez Cárdenas

Lista de primitivas (3/3)

- ether | ip broadcast | multicast
  - filtrar broadcast o multicast tipo Ethernet o IP
- <expr> relop <expr>
  - creación de expresiones complejas de filtros que seleccionen bytes o rangos de bytes en paquetes
  - mayor información: man tcpdump

Lámina 27 Roberto Gómez Cárdenas

Examinando paquetes capturados

- Posible ver los paquetes capturados.
- Paquetes capturados en tiempo real
- Ver paquetes en ventanas separadas
- Existe un menú que puede activarse cuando se selecciona un paquete
- Otros menús
  - edición
  - despliegue

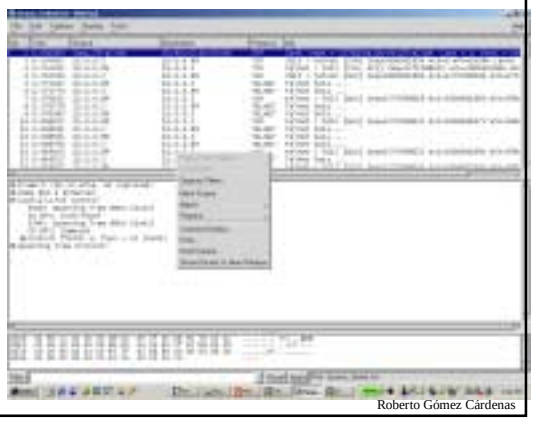


Lámina 28 Roberto Gómez Cárdenas

Menú de edición

- Find Frame buscar frame a través de un filtro.
- Go to Frame permite ir a un frame a través de un número
- Mark Frame marca el frame seleccionado
- Mark all frames marca todos los frames
- Unmark all frames desmarca todos los frames
- Preferences asignar preferencias para diferentes parámetros que controla ethereal
- Capture files crear y editar filtros
- Protocols activar/desactivar disección de protocolos

Lámina 29 Roberto Gómez Cárdenas

Menú de despliegue

- Options controla forma desplegar información acerca de paquetes
- Match Selected seleccionar paquetes que tienen un campo seleccionado en panel árbol
- Colorize Display colorear paquetes
- Collapse All retrae los subárboles menú árbol
- Expand All expande los subárboles menú árbol
- Show packet... despliega paquetes seleccionados en una ventana aparte
- User Specified ... decodificar algunos paquetes como un protocolo en particular

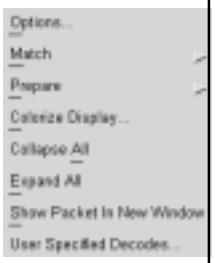


Lámina 30 Roberto Gómez Cárdenas

Disección de paquetes

- Ethereal realiza una disección de los paquetes
- Los protocolos que entiende los disecta de tal forma que se puede apreciar el payload y el encabezado

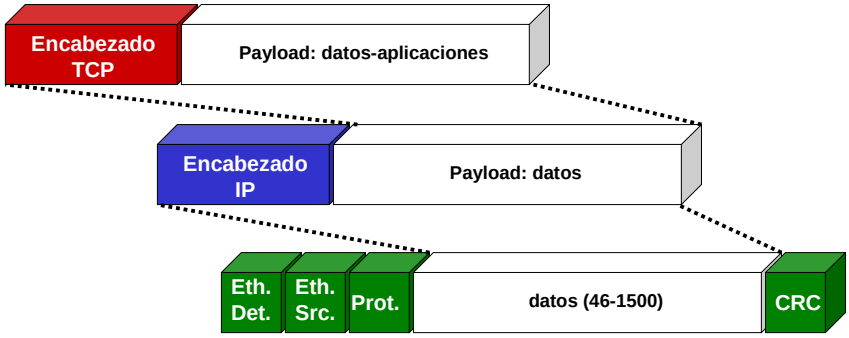


Lámina 31 Roberto Gómez Cárdenas

Encabezado protocolo IP

0	3	7	15	18	23	31
número versión	longitud	tipo de servicio	longitud del paquete			
identificación				DF	MF	offset del fragmento
tiempo de vida		transporte	checksum del encabezado			
dirección fuente						
dirección destino						
opciones						relleno

Lámina 32 Roberto Gómez Cárdenas

Encabezado TCP

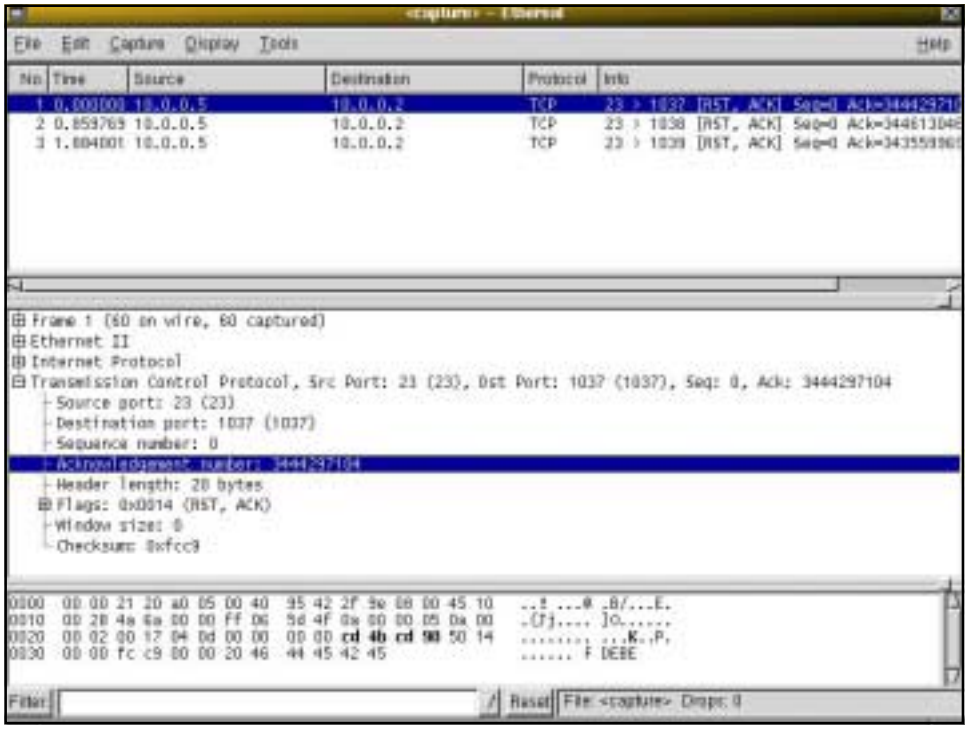
0	3	9	15	18	23	31
puerto fuente					puerto destino	
número de secuencia						
número de acknowledgement						
offset de datos	reservado	URG	ACK	PSH	RST	SYN	FIN	tamaño de la ventana
checksum					apuntador urgente	
opciones					relleno	

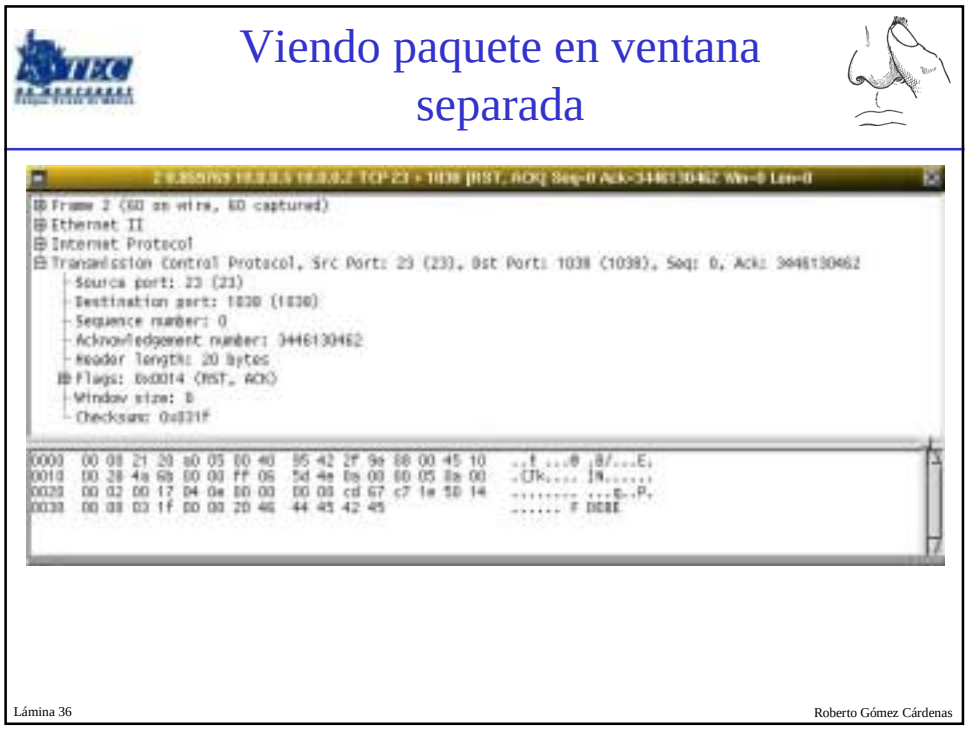
Lámina 33 Roberto Gómez Cárdenas

Encabezado Protocolo UDP

0	15	31
número puerto fuente	número puerto destino	
longitud	checksum	

Lámina 34 Roberto Gómez Cárdenas


File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 0.000000 10.0.0.5 10.0.0.2 TCP 23 > 1037 [RST, ACK] Seq=0 Ack=3444297104
2 0.859769 10.0.0.5 10.0.0.2 TCP 23 > 1038 [RST, ACK] Seq=0 Ack=3446130462
3 1.804001 10.0.0.5 10.0.0.2 TCP 23 > 1039 [RST, ACK] Seq=0 Ack=3435593961
Frame 1 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 1037 (1037), Seq: 0, Ack: 3444297104
Source port: 23 (23)
Destination port: 1037 (1037)
Sequence number: 0
Acknowledgement number: 3444297104
Header length: 20 bytes
Flags: 0x0014 (RST, ACK)
Window size: 0
Checksum: 0xfcc9
0000 00 00 21 20 a0 05 00 40 95 42 2f 9e 08 00 45 10 ..! ...@ .B/...E.
0010 00 28 4a 6a 00 00 ff 06 5d 4f 0a 00 00 05 0a 00 .(Jj....]O......
0020 00 02 00 17 04 0d 00 00 00 00 cd 4b cd 90 50 14 ....K..P.
0030 00 00 fc c9 00 00 20 46 44 45 42 45 ...... F DEBE
Filter:
Reset
File: <capture> Drops: 0


Viendo paquete en ventana separada
Frame 2 (60 on wire, 60 captured)
Ethernet II
Internet Protocol
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 1038 (1038), Seq: 0, Ack: 3446130462
Source port: 23 (23)
Destination port: 1038 (1038)
Sequence number: 0
Acknowledgement number: 3446130462
Header length: 20 bytes
Flags: 0x0014 (RST, ACK)
Window size: 0
Checksum: 0x031f
0000 00 00 21 20 a0 05 00 40 95 42 2f 9e 08 00 45 10 ..! ...@ .B/...E.
0010 00 28 4a 6b 00 00 ff 06 5d 4e 0a 00 00 05 0a 00 .(Jk....]N......
0020 00 02 00 17 04 0e 00 00 00 00 cd 67 c7 1e 50 14 ....g..P.
0030 00 00 03 1f 00 00 20 46 44 45 42 45 ...... F DEBE
Lámina 36
Roberto Gómez Cárdenas

Dos opciones interesantes

- Colorear paquetes
  - colorear paquetes que cumple con reglas de un filtro
  - opción: Colorize Display
    - menú de Despliegue
    - menú que surge cuando se selecciona un paquete
- Seguimiento de una sesión TCP
  - permite reconstruir una sesión tcp
  - opción: Follow TCP Streams
    - menú campo del panel del árbol de tres vistas
    - menú que surge cuando se selecciona un paquete

Lámina 37 Roberto Gómez Cárdenas

Pasos colorear paquetes

- Elegir opción Colorize Display
- Se tiene que definir un filtro y asociarle un color
  - opción new de la ventana generada
  - proporcionar un nombre al filtro
  - después hay que definir el filtro
- Opciones definir filtro
  - a través de un cuadro de diálogo (botón Add Expression)
  - introducir expresión directamente

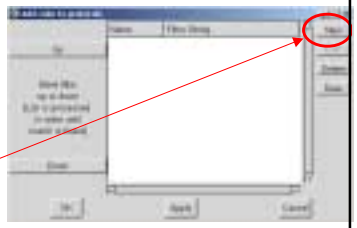


Lámina 38 Roberto Gómez Cárdenas

Pasos colorear paquetes

- Asociando un color
  - a través de los cuadros de dialogo respectivo elegir colores foreground (caracteres) y del background (el fondo)
- Terminando
  - opcion ok del cuadro Chose Color
  - opción ok del cuadro Edit Color Filter
  - Add Color Protocols

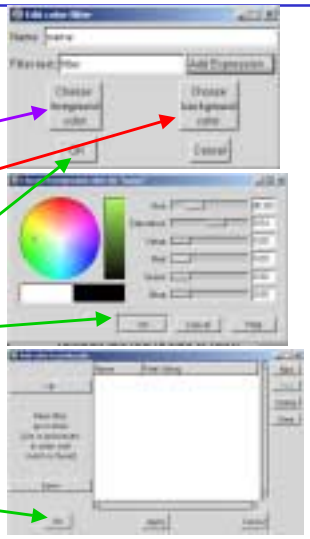
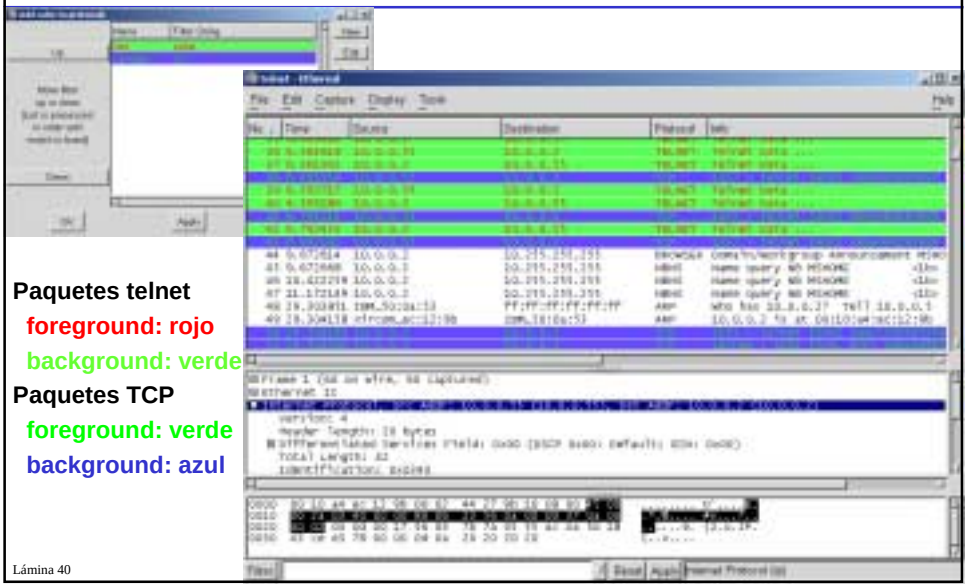


Lámina 39 Roberto Gómez Cárdenas

Ejemplo de coloreo



Paquetes telnet
foreground: rojo
background: verde
Paquetes TCP
foreground: verde
background: azul

Lámina 40

Siguiendo TCP streams

- Solo se puede dar seguimiento a protocolos orientados conexión
- Seleccionar paquete que forma parte de la sesión TCP a dar seguimiento.
- Seleccionar opción Follow TCP Stream del menú

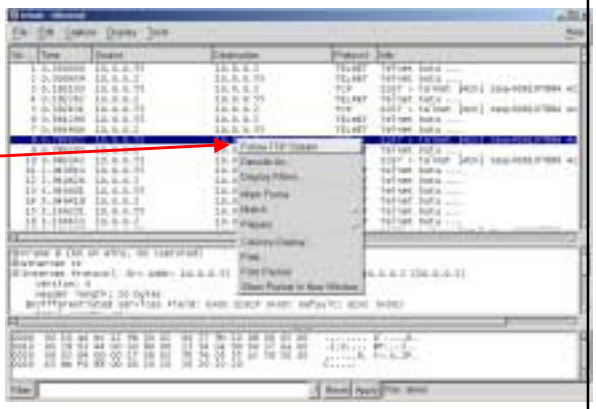


Lámina 41 Roberto Gómez Cárdenas

Formatos despliegue disponibles

- ASCII
  - datos de cada lado en ASCII, pero alternados
  - caracteres no imprimibles no se despliegan
- EBCDIC
  - for the big-iron freaks out there
- HEX Dump
  - ver todos los datos, pero no se ve en ASCII

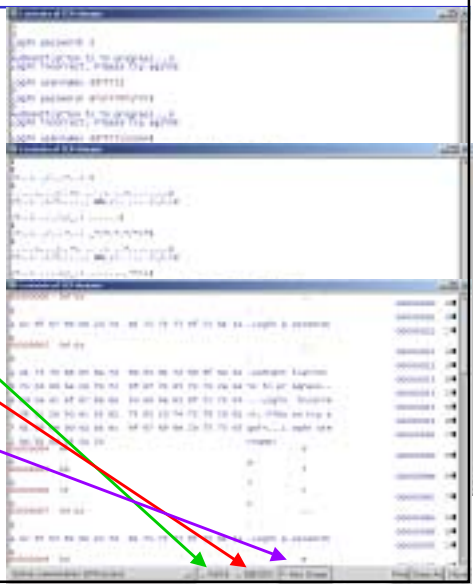


Lámina 42

Limitantes Ethereal (y otros sniffers)

- Es lento para la lectura
- Redes switcheadas
- Redes encriptadas
- Redes de alta velocidad

Lámina 43 Roberto Gómez Cárdenas

Introducción a los sniffers activos

conceptos de base

Lámina 44 Roberto Gómez Cárdenas

Tipos de sniffers

- Pasivos
  - sniffers no realizan actividad alguna
  - solo capturan paquetes
- Activos
  - sniffers intentan apoderarse de las sesiones
  - uso de técnicas para lograr lo anterior
    - spoofing
    - envenenamiento de la tabla de arp

Lámina 45 Roberto Gómez Cárdenas

Spoofing

- Spoofing es la creación de paquetes de comunicación TCP/IP usando una dirección IP de alguien más.
- Lo anterior permite entrar en un sistema haciéndose pasar por un usuario autorizado.
- Una vez dentro del sistema, el atacante puede servirse de éste como plataforma para introducirse en otro y así sucesivamente.

Lámina 46 Roberto Gómez Cárdenas

Un ejemplo de Spoofing

- Un ejemplo es hacer un telnet al puerto 25 y enviar correos a nombre de otra persona.
  - una variante es modificar los parametros del manejador de correos.
- Además, cualquiera, con un poco más de conocimientos, puede escoger cualquier dirección IP.

Lámina 47 Roberto Gómez Cárdenas

1er ejemplo spoofing: ataque ARP

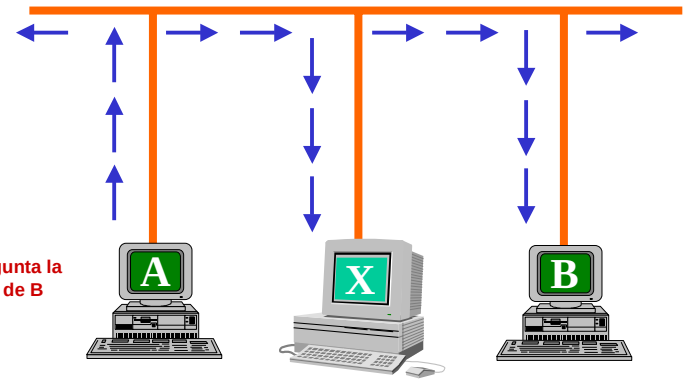
- Consiste en hacerse pasar por una máquina que no es.
- Aprovecha el principio de funcionamiento del protocolo ARP.
- Sólo es útil es redes/máquinas que utilizan este protocolo (locales).

Lámina 48 Roberto Gómez Cárdenas

Protocolo ARP
(funcionamiento normal)

Tabla arp de máquina A:
I_A: dirección lógica A, F_A dirección física A
se desconoce la dirección física de B (F_B)

1	I_A	I_B
	F_A	?



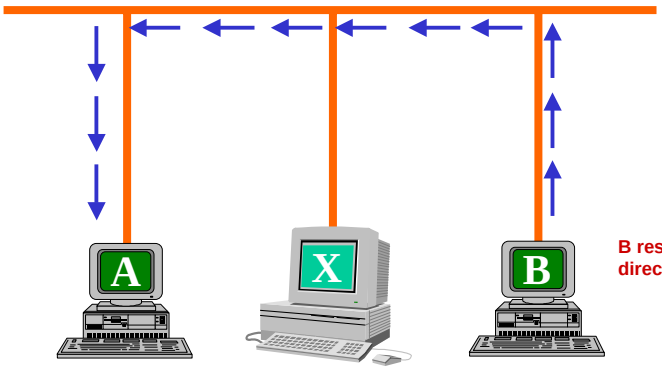
Máquina A pregunta la dirección física de B

Lámina 49 Roberto Gómez Cárdenas

Protocolo ARP
(funcionamiento normal)

A actualiza su tabla arp

2	I_A	I_B
	F_A	F_B



B responde con su dirección física (F_B)

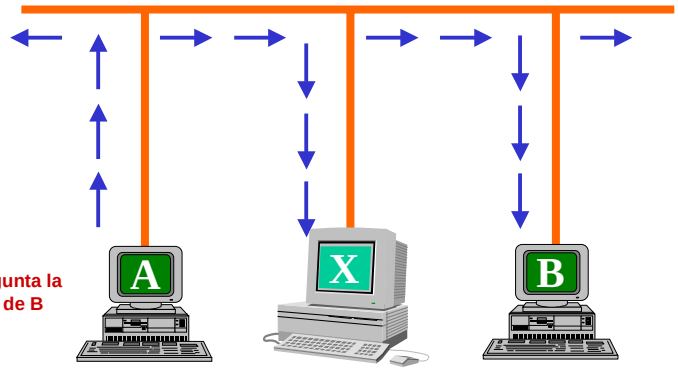
Lámina 50 Roberto Gómez Cárdenas

Ataque ARP

(máquina A solicita direccón de B)

Tabla arp de máquina A:

1	I_A	I_B
	F_A	?



Máquina A pregunta la dirección física de B

Máquina Intrusa

Lámina 51 Roberto Gómez Cárdenas

Las tablas ARP de las máquinas

A
Tabla ARP

I_B	F_x

Tabla ARP máquina A

Para A:
dirección física de B es F_X

B
Tabla ARP

I_A	F_A

Tabla ARP máquina B

Para B:
dirección física de A es F_A

Lámina 52 Roberto Gómez Cárdenas

Ataque ARP

Máquina intrusa (X) le notifica a B que ella es A

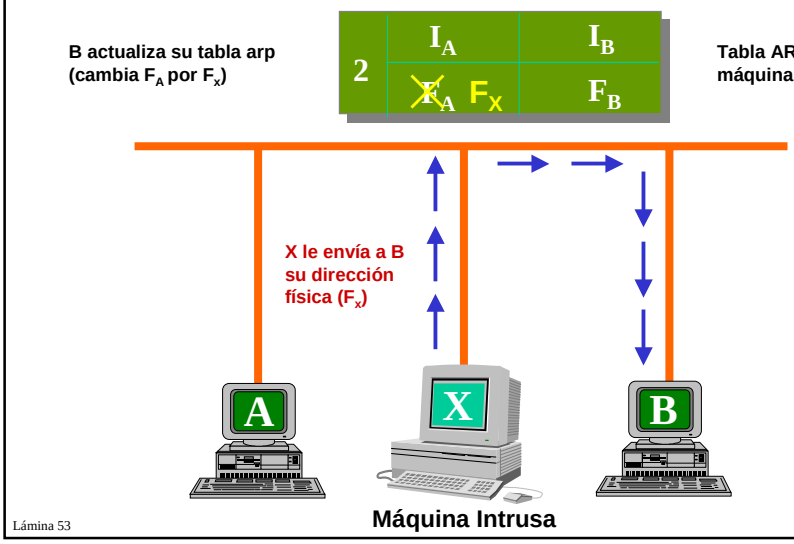
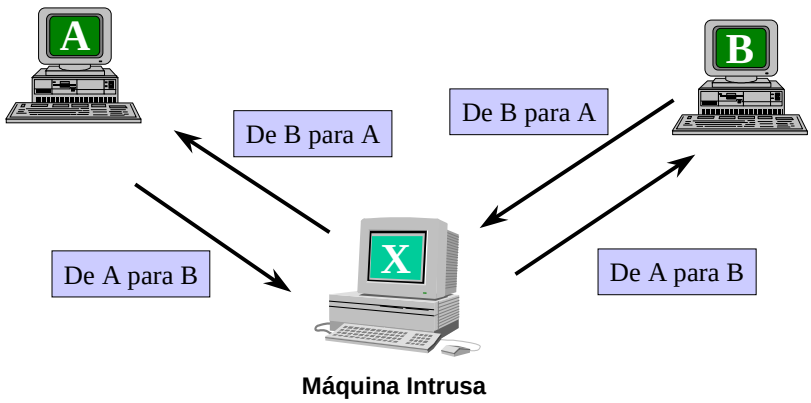


Lámina 53 Roberto Gómez Cárdenas

Finalmente



Toda la información entre A y B pasa por X

Lámina 54 Roberto Gómez Cárdenas

Protocolo ICMP (Internet Control Message Protocol)

- Permite a ruteadores y servidores reportar errores o información de control sobre la red.
- Reporta errores como:
  - Expiración del TTL
  - Congestión
  - Dirección IP destino no alcanzable, etc.
- Viaja encapsulado en el área de datos de un datagrama IP.

Lámina 55 Roberto Gómez Cárdenas

Mensajes ICMP más comunes

Tipo	Descripción
0	Echo reply
3	Destination Unreachable
4	Source Quench
5	Redirect (Cambio de Ruta)
8	Echo request
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply

Lámina 56 Roberto Gómez Cárdenas

Mensaje ICMP Cambio de Ruta

Utilizado por un ruteador para indicarle a una máquina en su segmento que utilice una nueva ruta para determinados destinos.

Lámina 57 Roberto Gómez Cárdenas

Mensaje ICMP Cambio de Ruta

(funcionamiento normal)

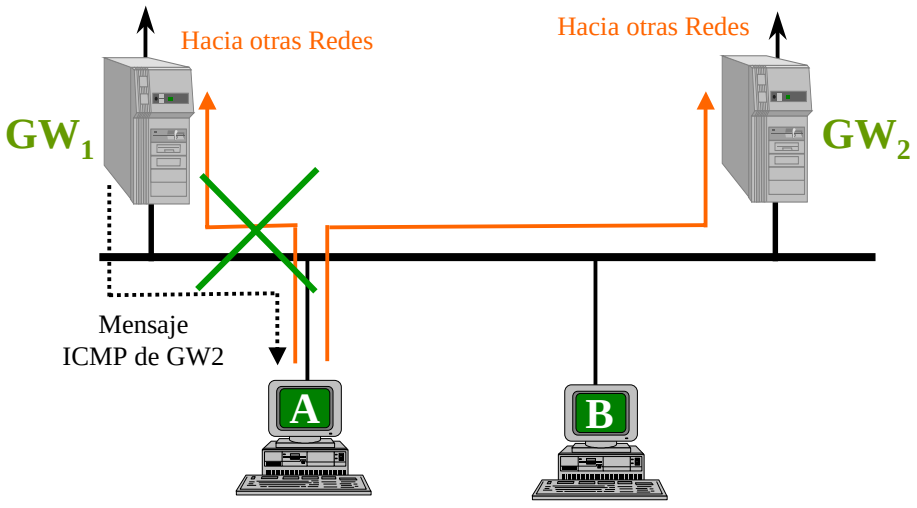
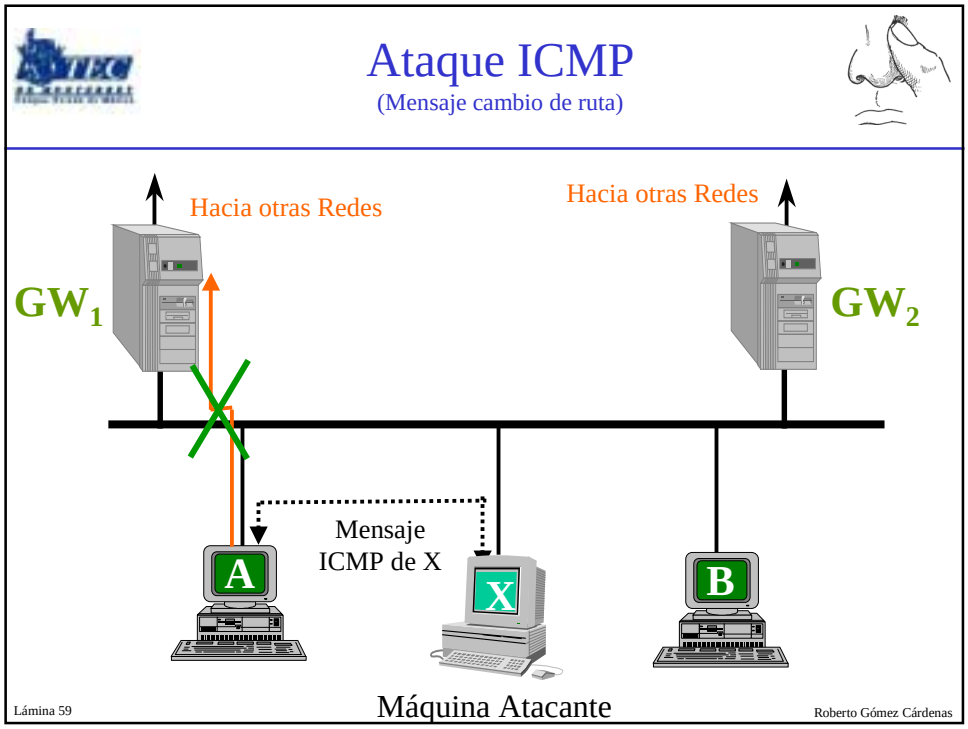
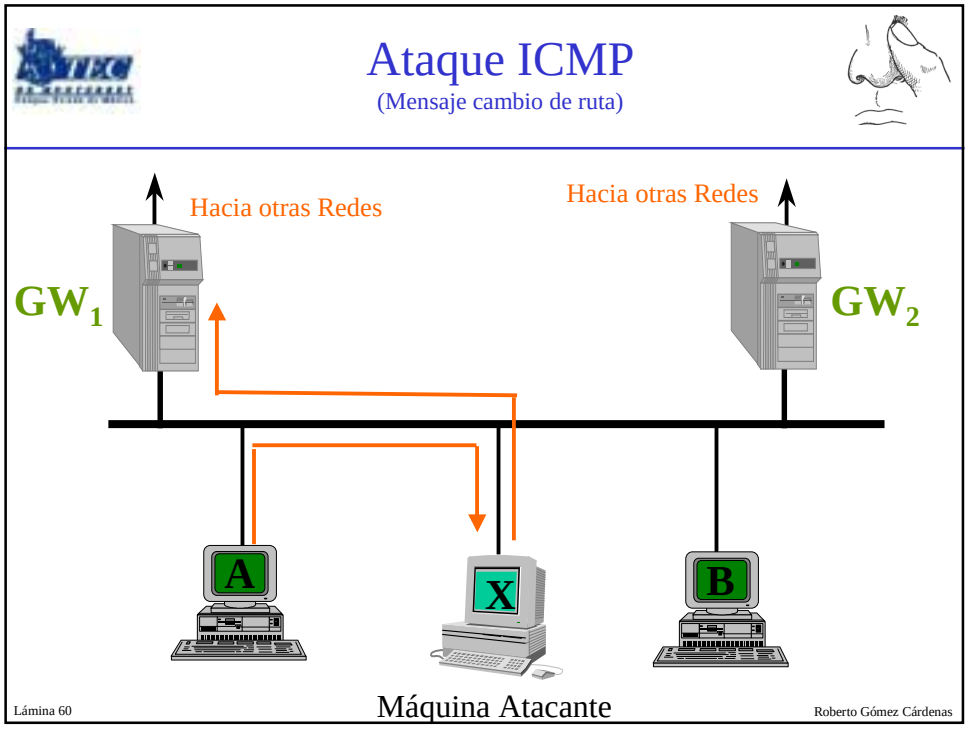


Lámina 58 Roberto Gómez Cárdenas


Ataque ICMP
(Mensaje cambio de ruta)
Hacia otras Redes
Hacia otras Redes
GW1
GW2
Mensaje
ICMP de X
A
X
B
Lámina 59
Máquina Atacante
Roberto Gómez Cárdenas


Ataque ICMP
(Mensaje cambio de ruta)
Hacia otras Redes
Hacia otras Redes
GW1
GW2
A
X
B
Lámina 60
Máquina Atacante
Roberto Gómez Cárdenas

Ejemplo sniffers activos: ettercap

ettercap

Lámina 61 Roberto Gómez Cárdenas

Presentando ettercap

Kiddie: A friend of mine told me that it is possible to sniff on a LAN... so I bought a switch ;)
NaGoR: mmhhh....
Kiddie: Now my LAN is SECURE ! you can't sniff my packets... ah ah ah
NaGoR: are you sure ? look at ettercap doing its work...
Kiddie: Oh my god... it sniffs all my traffic !!
I will use only ciphered connections on my LAN, so ettercap can't sniff them ! ah ah ah
NaGoR: mmhhh....
Kiddie: Now I'm using SSH. My LAN is SECURE !
NaGoR: are you sure ? look at ettercap doing its work...
Kiddie: shit !! grrrr...

"a false sense of security, is worse than insecurity" -- Steve Gibson
hey folks... wake up ! the net is NOT secure !!
ettercap demonstrates that now is the time to encourage research on internet protocols to make them more secure.

Lámina 62 Roberto Gómez Cárdenas

ettercap

- Similar a dsniff aunque no soporta tantos protocolos
- Puede spoofear el arp en ambos lado de la sesión para lograr un sniffing tipo full-duplex
- Permite inserción de comandos en sesiones TCP persistentes
- Presenta una interfaz de menu
- Autores:
  - Alberto Ornaghi (ALoR) <alor@users.sourceforge.net>
  - Marco Valleri (NaGA) <crwm@freemail.it>

Lámina 63 Roberto Gómez Cárdenas

Plataformas soportadas

- Linux 2.0.x
- Linux 2.2.x
- Linux 2.4.x
- FreeBSD 4.x
- OpenBSD 2.[789] 3.0
- NetBSD 1.5
- Mac OS X (darwin 1.3 1.4 5.1)
- Windows 9x/NT/2000/XP
- Solaris 2.x

Lámina 64 Roberto Gómez Cárdenas

Requerimientos

- No requiere de ninguna biblioteca como libpcap, libnet o libnids, tampoco es necesario ncurses, pero es altamente recomendable instalarlo.
- Si es necesario que soporte SSH1 y/p HTTPS, ettercap requiere las bibliotecas de OpenSSL
- Para Win32:
  - requiere Windows NT/2000/XP.
  - winpcap versión 2.3 o mayor
  - cygwin de http://cygwin.com/setup.exe

Lámina 65 Roberto Gómez Cárdenas

Características ettercap

- Sniffer/interceptor/logger multipropósito sólo para redes LAN switcheadas
- Soporta disección pasiva y activa de varios protocolos (aún los encriptados)
  - incluye varias características para análisis de redes y hosts.
- No hace criptoanálisis en los criptogramas.

Lámina 66 Roberto Gómez Cárdenas

Modos operación

- El sniffer tiene cuatro modos de operación
  - Basado en IP, paquetes filtrados en fuente y destino IP
  - Basado en MAC, paquetes filtrados en base a direcciones MAC, útil para sniffear conexiones a través del gateway
  - Basado en ARP, útil para envenenar el arp para sniffear en una lan switcheado entre dos hosts (full-duplex)
  - Basado en ARP público, usa envenamiento de arp para sniffear una lan switcheada de un host víctima al resto de los hosts (half-duplex)

Lámina 67 Roberto Gómez Cárdenas

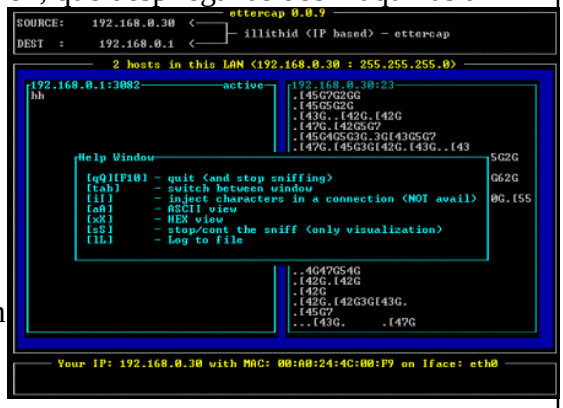
Usando ettercap

- Dos interfaces disponibles
  - Interfaz ncurses
  - Línea de comandos

Lámina 68 Roberto Gómez Cárdenas

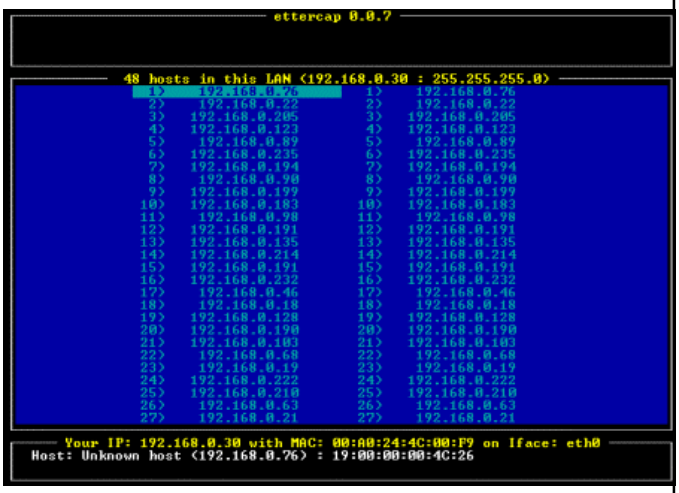
La interfaz ncurses

- Ventana principal dividida en tres subsecciones:
  - **alta:** diagrama de conexión, que despliega las dos máquinas a sniffear o a conectar o sobre las que se va a operar
  - **media:** lista de los host conocidos en la LAN (unidos hub o switch)
  - **baja:** ventana de status, proporciona información adicional acerca de los objetos actualmente seleccionados, status actual y otros hints importantes.



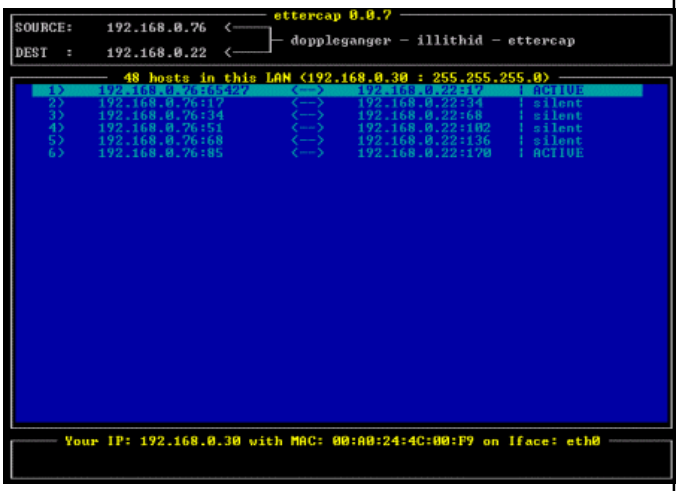
Lista hosts disponibles

- Lo primero que se obtiene es la lista de hosts de la LAN
- Se puede seleccionar con flechas y teclas de tabulador los dos hosts a monitorear, y después seleccionar el método apropiado (IP, MAC or ARP based sniffing).



Estado conexiones entre hosts

- Después de seleccionar un método, la interfaz muestra todas las conexiones entre los dos hosts
- Se puede elegir la conexión que se desea sniffear
- Cada conexión tiene un atributo (activo o silencio) que indica si existe alguna actividad en esta conexión.



Snifeando la conexión

- La interfaz de snifeo muestra tanto el puerto fuente como destino.
- Es posible registrar los datos sniffeados, examinarlo en modo ascii o hexadecimal, inyectar caracteres en una conexión telnet y mucho más

Los menús de ayuda

- Presionando la tecla 'h' en cada pantalla se despliega ayuda en línea.

Lámina 73

Otras opciones

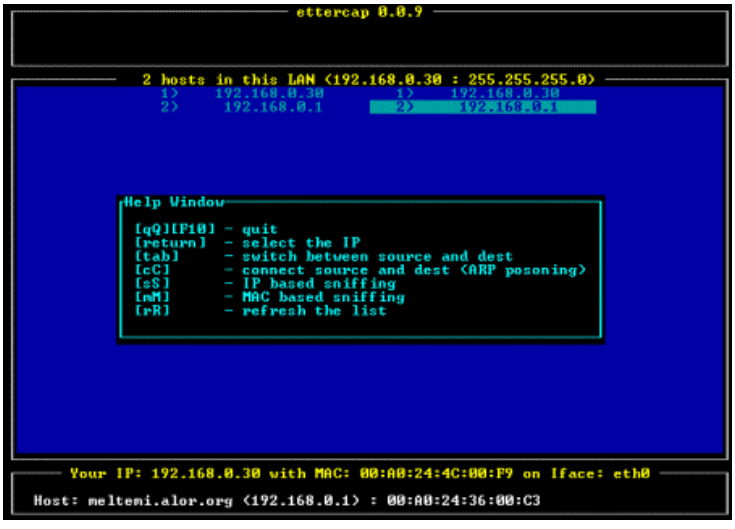


Lámina 74 Roberto Gómez Cárdenas

Trabajando fuera de línea

- Si es necesario analizar un archivo con información capturada por tcpdump o ethereal en formato libpcap, es posible usar el plugin Sprite
- Posible usarlo para reconstruir las listas de conexión, el proceso de recolecta de passwords, o la huella pasiva del sistema operativo.
- Especificar el archivo con la opción -T usar ettercap como si se estuviera snifiando en la red
- Para guardar un archivo tcpdump para un análisis posterior hay que usar la opción -Y

Lámina 75 Roberto Gómez Cárdenas

Examinando paquetes en hexadecimal en modo simple (sin ncurses)

```
0020: 6500 401f 0a8a 006c 0000 008a 003a 0000  e.@....l.....:..
0030: 006c 0046 0000 0000 007b 0000 0000 fdff  .l.F.....{......
0040: 0100 0100 0000 0000 0000 6c00 0000 0000  ..........l.....
0050: 0000 8077 0cfd 499d c001 0038 b07f 199e  ...w..I....8....
0060: c001 8077 0cfd 499d c001 8077 0cfd 499d  ...w..I....w..I.
0070: c001 e71a 0000 0000 0000 e71a 0000 0000  ................
0080: 0000 0000 0000 0c00 0000 0000 0b00 0000  ................
0090: 434f 4e46 497e 3456 2e49 4e00 0000 0000  CONFI~4V.IN.....
00a0: 0000 0000 0000 0000 636f 6e66 6967 7572  ........configur
00b0: 652e 696e 0000                           e.in..

192.168.0.1:3012 -> 192.168.0.30:139 | seq 9ca3f387 ack 203916 | flags AP |

0000: 0000 006d ff53 4d42 3200 0000 0018 0700  ...m.SMB2.......
0010: 0000 0000 0000 0000 0000 0000 0300 4005  ..............@.
0020: 6500 801f 0f29 0000 000a 0000 4000 0000  e....)......@...
0030: 0000 0000 0000 0029 0044 0000 0000 0001  .......).D......
0040: 0001 002c 0000 0000 1600 5605 0700 0401  .........V......
0050: 0000 0000 5c74 6f6f 6c73 5c65 7474 6572  ....\tools\etter
0060: 6361 705c 636f 6e66 6967 7572 652e 696e  cap\configure.in
0070: 00                                       .

192.168.0.30:139 -> 192.168.0.1:3012 | seq 203916 ack 9ca3f3f8 | flags AP |

0000: 0000 00b2 ff53 4d42 3200 0000 0088 4100  .....SMB2.....A.
0010: 0000 0000 0000 0000 0000 0000 0300 4005  ..............@.
0020: 6500 801f 0a8a 006c 0000 008a 003a 0000  e......l.....:..
0030: 006c 0046 0000 0000 007b 0000 0000 fdff  .l.F.....{......
0040: 0100 0100 0000 0000 0000 6c00 0000 0000  ..........l.....
0050: 0000 8077 0cfd 499d c001 0038 b07f 199e  ...w..I....8....
0060: c001 8077 0cfd 499d c001 8077 0cfd 499d  ...w..I....w..I.
0070: c001 e71a 0000 0000 0000 e71a 0000 0000  ................
0080: 0000 0000 0000 0c00 0000 0000 0b00 0000  ................
0090: 434f 4e46 497e 3456 2e49 4e00 0000 0000  CONFI~4V.IN.....
00a0: 0000 0000 0000 0000 636f 6e66 6967 7572  ........configur
00b0: 652e 696e 0000                           e.in..

192.168.0.1:3012 -> 192.168.0.30:139 | seq 9ca3f3f8 ack 2039cc | flags A |
```

Lámina 76 nas

¿Cómo funciona todo?

- La lista de hosts
- Sniffing basado en IP
- Sniffing basado en MAC
- Sniffing basado en ARP
- Envenamiento de ARP
- ARP público
- ARP público inteligente
- Inyección de caracteres

Lámina 77 Roberto Gómez Cárdenas

La lista de hosts

- Cuando empieza hace una lista de todos los hosts en la LAN.
- Envía un ARP REQUEST a cada IP en la LAN
  - revisando la IP actual y el netmask
  - posible capturar los ARP REPLIES y hacer la lista de los hosts que están respondiendo en la LAN
- Con este método también los hosts Windows responden
- Precaución con netmask = 255.255.0.0
  - ettercap enviará 255*255 = 65025 mensajes tipo arp request
  - tomará más de un minuto construir la lista

Lámina 78 Roberto Gómez Cárdenas

Sniffing basado en IP

- El viejo estilo de sniffeo
- La interfaz de red se pone en modo promiscuo y recupera todos los paquetes que coinciden con el filtro IP
- Si se usa interfaz ncurses
  - el filtro es construido en base a IP fuente/destino y puerto fuente/destino en ambas direcciones de la conexión
- En modo comando de línea
  - posible crear un filtro IP personalizado
  - se puede especificar solo la fuente, solo el destino o ambos; cada uno con o sin un puerto asociado

Lámina 79 Roberto Gómez Cárdenas

Mac based Sniffing

- Pone interfaz en modo promiscuo y captura los paquetes que contenga el filtro con la dirección mac
- El filtro se construye dando las IPs de los dos hosts
  - ettercap busca en la lista de hosts y asocia la dirección mac al filtro
- Ejemplos
  - asumiendo que vodka es el gateway a inernet

    ettercap –N –m ron vodka
  - lo cual regresa todas las conexiones que ron tiene con hosts remotos

Lámina 80 Roberto Gómez Cárdenas

Arp based sniffing

- No pone la interfaz en modo promiscuo.
- No es necesario, los paquetes llegan a la máquina.
  - el switch reenvia los paquetes a la máquina
- Como funciona
  - ettecarp “envenena” el caché del arp de dos hosts, identificandose como otro host
  - una vez que el caché fue envenenado, los hosts empiezan a comunicarse, pero sus paquetes se envían a la máquina “interceptora”
  - esta máquina almacena estos paquetes y los enviara a la máquina destino

Lámina 81 Roberto Gómez Cárdenas

Caracteresiticas arp sniffing

- La conexión es transparente para las víctimas
  - no saben que están siendo “snifeados”
  - la única forma de descubrir lo que esta pasando es ver los cachés arp de las máquinas y verificar si hay dos hosts con la misma dirección MAC

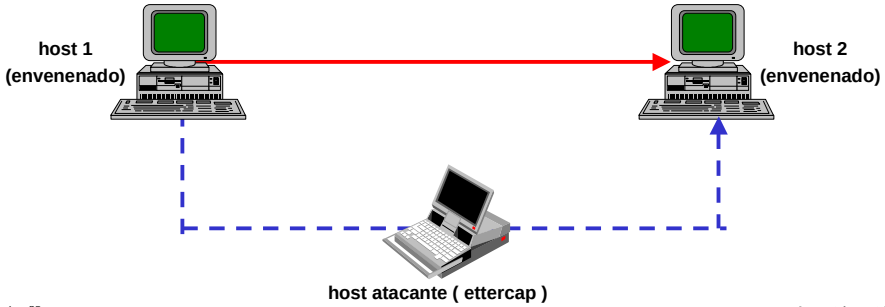


Lámina 82 Roberto Gómez Cárdenas

Envenenando el caché de arp

- Protocolo arp tiene una inseguridad intrínseca.
- Para reducir tráfico en cable, creará una entrada en la caché del arp, aún cuando no fue solicitado.
- Cada *arp-reply* que viaja en el cable será insertado en la tabla de arp.
- Ataque:
  - se enván arp-reply a los dos host a sniffear
  - en este mensaje se indica que la dirección mac del segundo host es la del atacante
  - el host enviara paquetes que deben ir al primer host a la máquina atacante
  - lo mismo para el primer host pero en orden inverso

Lámina 83 Roberto Gómez Cárdenas

Ejemplos host envenenados

HOST 1:
mac: 01:01:01:01:01:01
ip: 192.168.0.1
HOST 2:
mac: 02:02:02:02:02:02
ip: 192.168.0.2

ATTACKER HOST:
mac: 03:03:03:03:03:03
ip: 192.168.0.3

se envían mensajes arp-reply a:

HOST 1 indicando que 192.168.0.2 esta en: 03:03:03:03:03:03
HOST 2 indicando que 192.168.0.1 esta en: 03:03:03:03:03:03

ahora se encuentran envenenados, y enviaran paquetes al host de ataque, este último enviará paquetes de la siguiente forma:

HOST 1 será reenviado a: 02:02:02:02:02:02
HOST 2 será reenviado a: 01:01:01:01:01:01

Lámina 84 Roberto Gómez Cárdenas

Algunas observaciones

- Linux Kernel 2.4.x

  Unsolicited ARP is not accepted by default.
  It is possible, that this option should be enabled for some devices (strip is candidate)

  – núcleos usan un sistema especial para prevenir mensajes arp-reply no solicitados
  – son los mensajes que ettercap envía
  – entonces??
  – en el mismo código se tiene

Lámina 85 Roberto Gómez Cárdenas

/usr/src/linux/net/ipV4/arp.c

```
/*  Process entry.  The idea here is we want to send a reply if it is a
 *  request for us or if it is a request for someone else that we hold
 *  a proxy for.  We want to add an entry to our cache if it is a reply
 *  to us or if it is a request for our address.
 *  (The assumption for this last is that if someone is requesting our
 *  address, they are probably intending to talk to us, so it saves time
 *  if we cache their address.  Their address is also probably not in
 *  our cache, since ours is not in their cache.)
 *
 *  Putting this another way, we only care about replies if they are to
 *  us, in which case we add them to the cache.  For requests, we care
 *  about those for us and those for our proxies.  We reply to both,
 *  and in the case of requests for us we add the requester to the arp
 *  cache.  */
```

Lámina 86 Roberto Gómez Cárdenas

¿Entonces?

- Si núcleo recibe REQUEST este almacena petición en caché
- ¿Que significa?
  - si ettercap debe enviar mensajes “spoofeados” del tipo REQUEST en lugar de REPLIES
- Versiones de ettercap 0.6.0 y más nuevos tienen este tipo de envenenamiento de ARP
  - alterna mensajes request y replies para envenenar ya que otros sistemas operativos no cuentan con esta características.
- Caso Solaris
  - no almacena un reply, si no se encuentra en el caché
  - solución enviar mensajes ICMP “spoofeados” ECHO_REQUEST al host

Lámina 87 Roberto Gómez Cárdenas

ARP Público

- Objetivo
  - capturar paquetes de un host victima hacia todos los otros en una lan switcheada
- se envía broadcast ARP replies con la IP de la victima y la mac de la máquina atacante
- Todos los hosts toman este reply y lo añaden a su caché, de tal forma que enviarán todos los paquetes de la víctima al atacante
- Problema
  - la víctima recibirá este reply y notará un conflicto IP (Win2K)
  - solución: SMART PUBLIC ARP

Lámina 88 Roberto Gómez Cárdenas

Smart Public Arp

- Los mensajes reply son enviados de forma selectiva a todos los hosts a excepción de la víctima
  - no existe conflictos IP
- Nota 1:
  - los host envenenados serán los de la lista
  - si no se desea envenenar a algún host se debe quitar de la lista
- Nota 2:
  - la lista es necesaria: no usar broadping startup (-b)
  - es imposible realizar smart arp sin la lista en modo silencio (z)
- Nota 3:
  - se envían mucho más mensajes de tipo reply a la LAN.

Lámina 89 Roberto Gómez Cárdenas

Inyección de caracteres

- Paquetes son enviados al atacante
  - este debe enviarlos al destino original
  - que pasa si se modifican los paquetes
- ¿Qué se puede hacer?
  - modificar, sumar, borrar el contenido de estos paquetes
- Necesario recalcular el checksum y susbtituirlo en el tráfico.
- También es posible insertar paquetes en la conexión
  - cuidar valor número de secuencia y ack y enviarlos al destino

Lámina 90 Roberto Gómez Cárdenas

Detección de sniffers

¿es posible?

Lámina 91 Roberto Gómez Cárdenas

Detección sniffers

- Sniffers son difíciles de detectar y combatir ya que son programas pasivos.
  - algunas veces imposible
- No generan bitacoras.
- Cuando se usan propiamente, no usan mucho disco ni memoria.
- Es posible localizarlos a nivel local
  - verificar que se esta ejecutando
- A nivel red, algunos pueden localizarse mediante herramientas

Lámina 92 Roberto Gómez Cárdenas

A nivel local

- Saber si alguna interfaz de red, de las computadoras de la red, se encuentra en modo promiscuo
  - a través comandos ifconfig y utilería ifstatus
- Comando ifconfig
  - responde con el status de todas las interfaces
  - ejemplo uso:

```
toto@cachafas:17>ifconfig
UP BROADCAST   RUNNIG PROMISC MULTICAST   MTU:1500  Metric:1
:
toto@cachafas:18>
```

Lámina 93 Roberto Gómez Cárdenas

A nivel local

- Utileria ifstatus
  - pequeño programa en Unix
  - verifica todas las interfaces de red en el sistema y reporta si alguna de ellas se encuentran en modo promiscuo.
  - también los detecta en host locales
  - un ejemplo de salida es:

```
WARNING: LINUX2.SAMSHACKER.NET  INTERFACE  eth0
IS IN PROMISCOUS MODE
```

Lámina 94 Roberto Gómez Cárdenas

Aprovechando errores implementación stack IP

- Posible detectar sniffers en algunos sistemas operativos
  - por ejemplo: Linux
- Aprovechar debilidad en la implementación del stack TCP/IP.
- Cuando se encuentra en modo promiscuo
  - responde a los paquetes TCP/IP que recibe con su dirección IP aún si la dirección MAC en dicho paquete esta mal
  - el comportamiento estándar es que los paquetes que contienen direcciones MAC erróneas no serán tomados en cuenta (i.e. no hay respuesta) ya que la interfaz de red los “tira”.

Lámina 95 Roberto Gómez Cárdenas

Aprovechandose de errores implementación stack IP

- ¿Cómo funciona?
  - se envian paquetes TCP/IP a todas las direcciones de la red, donde la dirección MAC contenga información errónea, la respuesta de dichas máquina seá un paquete RST
  - indicará que máquinas se encuentran en modo promiscuo.
- A pesar de que no se trata de un método perfecto puede ayudar a descubrir actividad sospechosa en una red.

Lámina 96 Roberto Gómez Cárdenas

Otras técnicas de detección

- DNS test
- Etherping TEST
- ARP TEST
- TEST ICMP Ping de Latencia

Lámina 97 Roberto Gómez Cárdenas

Otras opciones

- Hubs activos solo envían paquetes a un conjunto de máquinas previamente autorizadas
  - puede deshabilitar el sniffer ya que no recibirá paquetes que no sean enviados por a una máquina en específico.
  - Cisco, HP y 3COM cuentan con dichos hubs activos
- Switchear la red
  - ettercap
- Encripción de los canales de comunicación
  - PVNs: SSL, SSH, IPSec, L2TP, PPTP

Lámina 98 Roberto Gómez Cárdenas

Herramientas detección sniffers

- AntiSniff
  - la herramientas más fácil de detección de sniffers
  - http://www.l0pht.com/antisniff/
- CPM (Check Promiscuous Mode)
  - herramienta de Carnegie-Mellon que verifica si una máquina Unix se encuentra en modo promiscuo
  - ftp://coast.cs.purdue.edu/pub/tools/unix/cpm/
- neped
  - herramienta creada por The Apostols, que detecta sniffers corriendo en un segmento local
  - aprovecha error implementación de ARP en máquinas Linux
  - http://www.apostols.org/projectz/neped/

Lámina 99 Roberto Gómez Cárdenas

Herramientas detección sniffers

- sentinel
  - proyecto de implementación de las todas las técnicas de detección de promiscuidad
  - actualmente soporta 3 metodos de detección: DNS test, Etherping test y ARP test.
  - http://www.packetfactory.net/Projects/sentinel/
- cpm (Check Promiscuous Mode)
  - herramienta Unix para verificar el estatus promiscuo de adaptadores red
- los comandos/utilerías
  - ifconfig
  - ifstatus

Lámina 100 Roberto Gómez Cárdenas