Computo forense redes

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Definición

- Captura, registro y análisis de eventos de red con el objetivo de descubrir la fuente de ataques de seguridad u otros incidentes.
- De acuerdo a Simon Garfinkel, se cuenta con dis tipos de análsis forense de red
  - Catch-if-as-you-can System
  - Stop, look and listen

Catch-it-as-you-can System

- Todos los paquetes que pasan a través de un punto de tráfico son capturados y escritos en un medio de almacenamiento.
- El análisis de lleva a cabo posteriormente en forma de batch.
- Este tipo de enfoque requiere de grandes cantidades de espacio de almacenamiento, usualmente involucra un sistema RAID.

Lámina 3 Dr. Roberto Gómez Cárdenas

Stop, look and listen

- Cada paquete es analizado de forma rudimentaria en memoria y solo cierta información se almacena para un análisis futuro.
- Este enfoque requiere menos almacenamiento, pero puede requerir un procesador más rápido para no perder paquetes.

Lámina 4 Dr. Roberto Gómez Cárdenas

Forensia redes

- Se trata de monitoreo de redes, determinando si existe alguna anomalía (o actividades maliciosas) y determinar la naturaleza de los ataques si dio alguno.
- Aspectos importantes incluye captura de tráfico, preservación y análisis.
- Análisis involucra muchas actividades dependiendo de la naturaleza de la investigación y la evidencia presentada. Esto puede incluir:
  - Reensamblar paquetes
  - Extraer contenido de tráfico
  - Examinar flujo de tráfico
  - Inspeccionar encabezados de paquetes

Lámina 5 Dr. Roberto Gómez Cárdenas

Forensia redes puede responder las siguiente preguntas

- ¿En qué momento una IP en particular exitosamente comprometió el sistema?
- ¿Cuál es la duración de una sesión http?
- ¿Qué protocolo de red se usó en un ataque?
- ¿Cuál es el atributo principal de una conexión ftp?
- ¿Cuál es el atributo principal de la baja exitosa de un archivo?

Lámina 6 Dr. Roberto Gómez Cárdenas

¿Porqué forensia en redes?

- Tamper resistant especialmente si se lleva a cabo en un modo de tipo bridge/tap.
- No produce ningún impacto en el end-point.
- No provoca ningún impacto en plataformas.
- Trabaja a través de diferentes sistemas operativos.
- Capaz de derivar información que a través de un análisis forense de un host.

Lámina 7 Dr. Roberto Gómez Cárdenas

Ventajas de forensia en redes

- Recuperación evidencia
  - Un atacante subió un backdoor a un servidor.
  - Borró el backdoor.
  - Se puede recuperar la herramienta a partir de la captura del paquete.
  - Un empleado disgustado sube un documento confidencial a un servidor.
  - Es posible recuperar el documento, y tener evidencia para denunciar.
- Podemos conocer exactamente que es transferido y con quien se comunica el atacante aún si este ha borrado la evidencia de un servidor comprometido.

Lámina 8 Dr. Roberto Gómez Cárdenas

Proceso

- Captura
  - El proceso de capturar paquetes que viajan en un medio.
- Registro
  - El proceso de escribir paquetes capturados en dispositivos de almacenamientos.
- Análisis
  - El proceso de analizar paquetes.
- Objetivos
  - Descubrir la naturaleza de la instrusión.
  - Complementar forensia de host

Lámina 9 Dr. Roberto Gómez Cárdenas

Técnicas tradicionales de análisis de forense de redes

- Los pasos comunes son
  - Mensaje de alerta de un IDS
  - Analizar y examinar el evento de alarma.
  - Examinar el paquete (análisis del encabezado del protocolo)
  - Determinar el evento (intrusión, virus, escaneo, etc).
  - Escalar el evento.

Lámina 10 Dr. Roberto Gómez Cárdenas

Técnicas emergentes

- Otros enfoques al análisis forense de redes
  - Reporte de alerta de otras fuentes
  - Determinar la ocurrencia del evento
  - Reconstrucción de la sesión
  - Examinar el paquete (encabezado protocolo y análisis carga).
  - Escalar el evento.
- La carga juega un papel principal en *malicious traffic mining!*

Lámina 11 Dr. Roberto Gómez Cárdenas

Propósito forensia redes

- Los propósitos principales son
  - Descubrir actividades maliciosas
  - Reconstrucción de una sesión de datos.
  - Reconstruir eventos pasaos de redes.
  - Extraer evidencia.
  - Analizar tráfico cifrado u oculto.

Lámina 12 Dr. Roberto Gómez Cárdenas

Imagen general

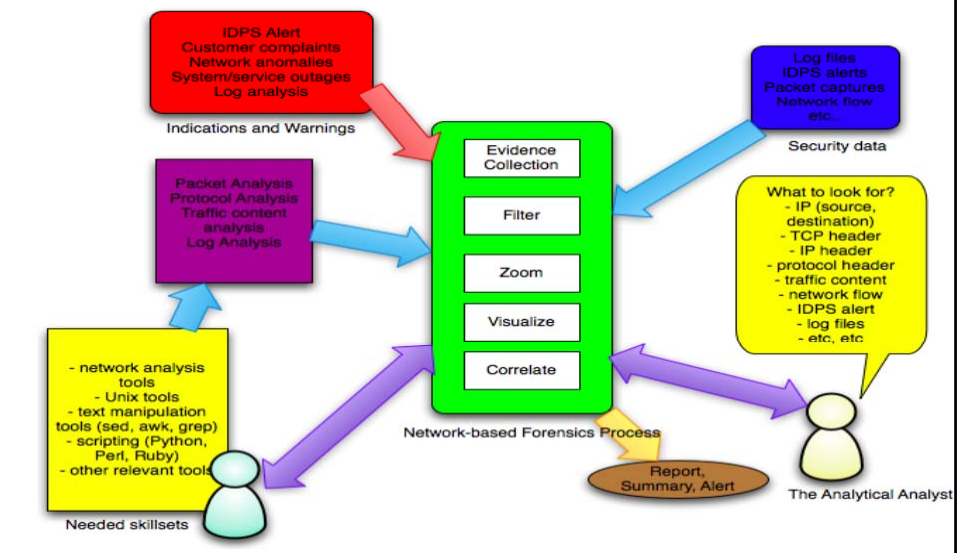


Lámina 13 Dr. Roberto Gómez Cárdenas

Adquisición

- Llevar a cabo una copia forense de la evidencia digital adquirida en la escena.
- Copia forense
  - Cadena de evidencia
  - Firmas digitales
  - Controles de acceso
- Copia completa
  - Puede ser difícil debido a la velocidad de las redes.
  - Puede ir más allá del alance de la garantía o de la autoridad, cuidado.
  - Consideraciones de privacidad.

Lámina 14 Dr. Roberto Gómez Cárdenas

Consideraciones arquitectura

- Tomar en cuanta
  - Muchos datos
    - Difícil manejar los volúmenes obtenidos.
    - Constraints de privacidad y legales.
    - ¿Qué tipos de datos?
  - Pocos datos
    - Puede faltar información crítica.
    - Evidencia
  - Nivel de acceso
    - ¿Cómo obtener datos en redes fuera del control de la organización?

Lámina 15 Dr. Roberto Gómez Cárdenas

Ejemplo arquitectura

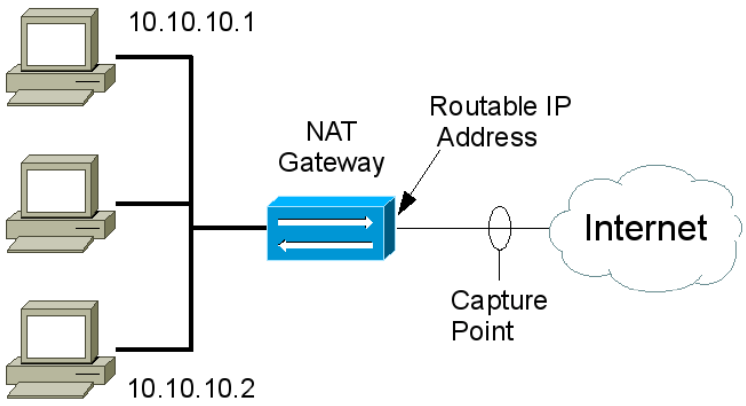


Lámina 16 Dr. Roberto Gómez Cárdenas

Adquisición básica

- Recopilar todo el tráfico visto en la interfaz de red.
- Herramienta más popular: tcpdump
  - Usa libpcap
  - Es un wrapper alrededor de la facilidad de captura del núcleo.
  - Varios núcleos unix puede hacer packet matching en el núcleo.

```
tcpdump -i eth0 -s0 -w output.pcap port 80
```

Lámina 17 Dr. Roberto Gómez Cárdenas

¿Donde capturar?

- Hub
  - Facil de adquirir información
  - Son muy ineficientes.
- Switch
  - Posible habilitar spanning en alguno de los puertos.

Lámina 18 Dr. Roberto Gómez Cárdenas

Swithches manipulados

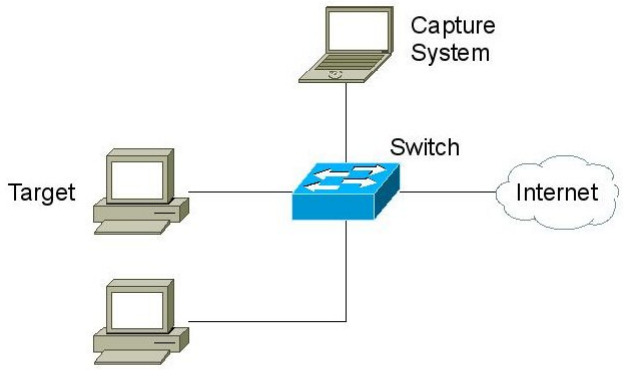


Lámina 19 Dr. Roberto Gómez Cárdenas

Dispositivo de adquisición dedicado

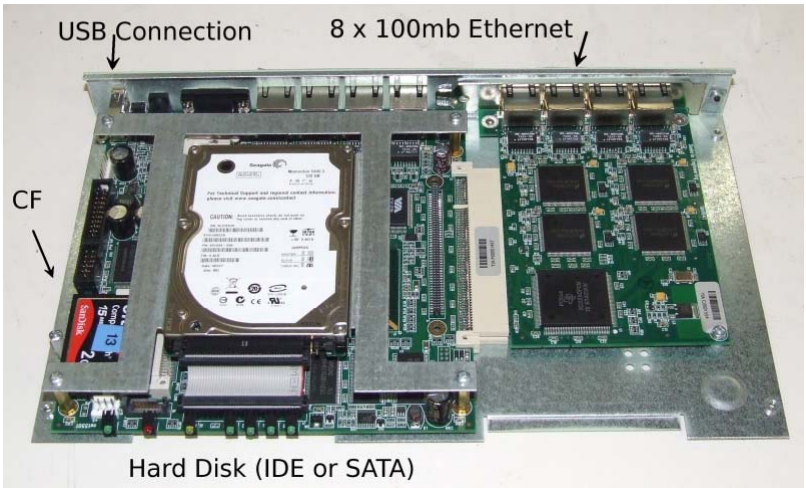


Lámina 20 Dr. Roberto Gómez Cárdenas

Análisis

- Protocolos de redes se encuentran en niveles.
- Se leen paquetes de izquierda a derecha, con los protocolos de bajo nivel en primer lugar.

Etherne t	IP	TC P	HTTP	HTML

- El proceso de dividir cada paquete de red en diferentes protocolos se conoce como disección de paquetes.
- Existen varias herramientas para llevar a cabo lo anterior.

Lámina 21 Dr. Roberto Gómez Cárdenas

Disección de paquetes

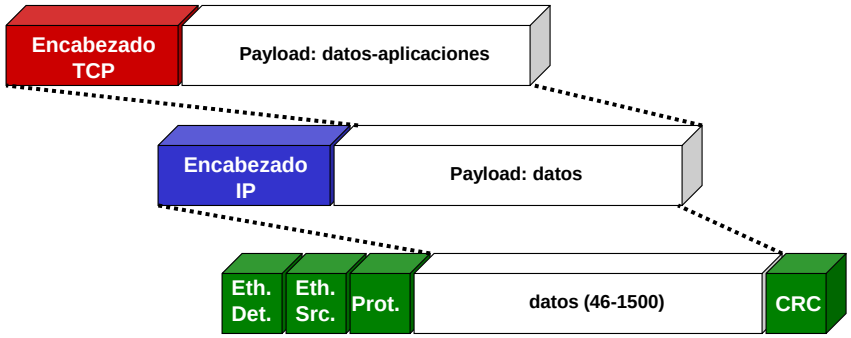


Lámina 22 Dr. Roberto Gómez Cárdenas

Características herramientas

- Asegurad integridad datos.
- Disectores de protocolos.
- Enfasis en herramientas que permiten reconstruir una sesión de forma automática.
- Derivar información de alto nivel acerca de un evento de red a partir de paquetes de datos.
- Ser capaz de extraer archivos o contenido útil de un paquete capturado.
- Se capaz de reproducir como telnet, ftp e IRC,
- El uso de las herramientas depende de las necesidades.

Lámina 23 Dr. Roberto Gómez Cárdenas

Herramientas

- Xplico
- NetworkMiner
- Pyags(Network Forensics Module)
- Bro-IDS
- Tcpxtract
- Tcpow
- Chaosreader
- Wireshark
- Foremost
- ClamAV - anti virus

Lámina 24 Dr. Roberto Gómez Cárdenas

Xplico

- Es todo un marco de análisis forense de redes
- Ofrece identificación de puertos independiente.
- Reconstrucción de la sesión tcp para extraer datos/contenidos de un archivo pcap.
- Salida a una base de datos (sqlite/mysql)
- Mapa de geolocalización.
- Muchas cosas más

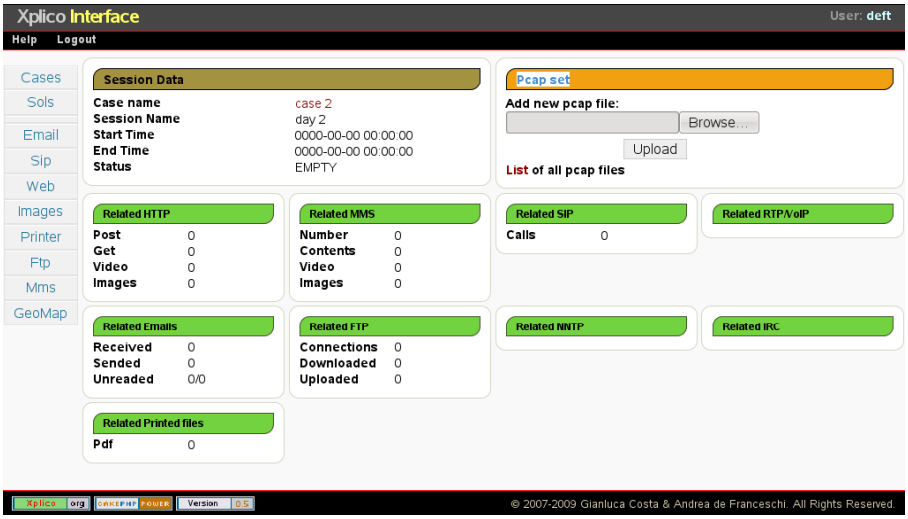
Lámina 25 Dr. Roberto Gómez Cárdenas

Ejemplos

- xplico -m rltm -i eth0
  - Corre en tiempo real escuchando en la interfaz eth0
- xplico -m rltm -i eth0
  - Corre para decodificar archivo de captura de paquete
- xplico -m pcap -d /tmp/pcap-directory
  - Corre para decodificar archivo de captura en el directorio

Lámina 26 Dr. Roberto Gómez Cárdenas

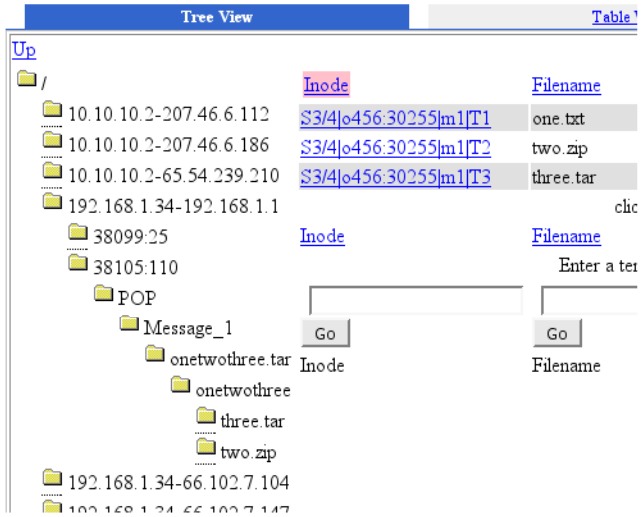
Ejemplo GUI



Pyflag – Modulo Analisis Forense

- Proporciona correlación con bitácoras y forensia de sistema de archivos y memoria.
- Ofrece análisis de información de alto nivel.
- Usar scanner de protocolos para reconstruir el flujo de tráfico para diferentes protocolos.
- Indexa datos pcap.
  - Util para gigabits de datos.
  - Búsqueda de paquetes indexados es más rápido.

Ejemplo salida



Ejemplo sesión MSN Chat

Prox	Time Stamp	Packet	Sender Nick	Text
	2005-08-08 16:40:09	436	(Target)	hello
	2005-08-08 16:40:22	445	user022714@hotmail.com	hi there buddy
	2005-08-08 16:40:27	449	(Target)	whats up man?
	2005-08-08 16:40:39	460	user022714@hotmail.com	im getting a new plan ready
	2005-08-08 16:40:48	468	(Target)	really? what are u planning?
	2005-08-08 16:41:24	486	user022714@hotmail.com	we can hit that bank on the corner across my house
	2005-08-08 16:41:34	494	(Target)	we are gonna need some serious firepower for that

Image description: A chat session using MSN messanger. Note the packet link allowing direct access to the exact packet which contained the message.

Up
/
Frame 164 (72 bytes on wire, 72 bytes captured)
Ethernet II, Src: 00:11:50:63:6b:32 (00:11:50:63:6b:32), Dst: 00:50:bf:79:fc:8e (00:5
Internet Protocol, Src: 192.168.1.34 (192.168.1.34), Dst: 192.168.1.1 (192.168.1.
Transmission Control Protocol, Src Port: 38105 (38105), Dst Port: 110 (110), Seq:
Post Office Protocol
Request: True

Tcpxtract

- Herramienta que permite la extracción de archivos de tráfico de red en base a firmas de archivos.
- Usa una técnica conocida como data carving (extraer archivos basado en encabezados y footers).
- Fácil escribir firmas archivos.
- Puede ser usado
- http://tcpxtract.sourceforge.net/

Lámina 31 Dr. Roberto Gómez Cárdenas

Ejemplo corrida tcpxtract

```
tcpxtract -f malicious.pcap -c tcpxtract.conf -o
/nsm/tcpxtract
```

- El archivo tcpxtract.conf contiene firmas (basadas en metadatos del encabezado del archivo)
- Fácil de configurar y de añadir nuevas fimas
  - http://filext.com/index.php

Lámina 32 Dr. Roberto Gómez Cárdenas

Tcpflow

- Reconstruye diferentes flujos de TCP en archivos separado.
- Tráfico esta formado por diferentes sesiones, (HTTP. Bitorrent, Chat) la herramienta los extrae y los coloca en diferentes archivos.
- http://www.circlemud.org/ jelson/software/tcpow/
- Ejemplo

```
tcpflow -r malicious.pcap;
for i in `ls`; do file $i | awk 'print $1, $2' >
malicious.log; done
```

Lámina 33 Dr. Roberto Gómez Cárdenas

Chaosreader

- Herramienta completa de análisis forense de redes.
- Reconstruye sesiones completas de telnet, ftp, IRC, de paquetes capturados.
- Capaz de repetir la sesión, como una sesión telnet.
- Genera reporte HTML al leer archivos de captura
- http://www.brendangregg.com/chaosreader.html
- Ejemplo uso:

```
chaosreader malicious.pcap
```

Lámina 34 Dr. Roberto Gómez Cárdenas

Ejemplo reporte

Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

Image Report - Click here for a report on captured images.
GET/POST Report (Empty) - Click here for a report on HTTP GETs and POSTs.
HTTP Proxy Log - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

1.	**Sun Nov 16 20:38:22 2003**	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• as_html
2.	**Sun Nov 16 20:38:22 2003**	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• as_html
3.	**Sun Nov 16 20:38:22 2003**	29 s	192.168.1.3:1367 <-> 192.77.84.99:80	web	374 bytes	• as_html
4.	**Sun Nov 16 20:38:24 2003**	22 s	192.168.1.3:1369 <-> 192.168.1.1:23	telnet	2047 bytes	• as_html • session_0004.telnet.replay 22 seconds
5.	**Sun Nov 16 20:38:28 2003**	21 s	192.168.1.3:1364 <-> 192.77.84.99:80	web	361 bytes	• as_html
6.	**Sun Nov 16 20:38:48 2003**	62 s	192.168.1.3:1370 <-> 192.77.84.99:80	web	13285 bytes	• as_html • session_0006.part_01.html 12610 bytes
7.	**Sun Nov 16 20:38:51 2003**	61 s	192.168.1.3:1371 <-> 192.77.84.99:80	web	951 bytes	• as_html • session_0007.part_01.gif 258 bytes
8.	**Sun Nov 16 20:38:51 2003**	61 s	192.168.1.3:1372 <-> 192.77.84.99:80	web	4136 bytes	• as_html • session_0008.part_01.jpeg 3448 bytes
9.	**Sun Nov 16 20:38:51 2003**	64 s	192.168.1.3:1373 <-> 192.77.84.99:80	web	19442 bytes	• as_html • session_0009.part_01.gif 18746 bytes
10.	**Sun Nov 16 20:39:02 2003**	16 s	192.168.1.3:1374 <-> 192.168.1.1:21	ftp	1091 bytes	• as_html

Lámina 35 Dr. Roberto Gómez Cárdenas

Wireshark

- Sniffer con capacidad de filtrado, muy flexible para analizar datos de sesiones y protocolos de aplicaciones.
- Puede ser usado para localizar fuentes sospechosas y direcciones destino.
- Capacidad de reconstruir una sesión TCP.
- Nueva versión permite reconstruir un stream UDP.

Lámina 36 Dr. Roberto Gómez Cárdenas

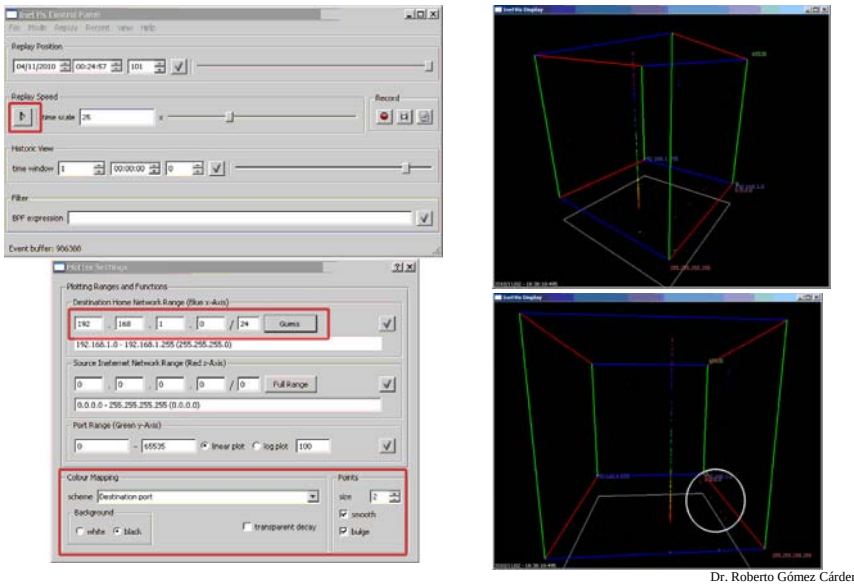
Tshark

- Wireshark en línea de comandos.
- Para capturas, análisis de red, etc en línea de comandos.
- Al usar las librerias pcap, su uso es similar a TCPDump y Windump.

InetVis

- Está basado en el concepto de Spinning Cube of Potencial Doom.
- Se trata de una herramienta de visualicación tridimensional del tráfico de red, que, además, puede visualizarse reproduciéndose a lo largo del tiempo.
- Su objetivo principal es el análisis de tráfico anómalo a través de una serie de patrones.
- Es multiplataforma y lo descargamos desde aquí:
  - Windows: inetvis/0.9.5/InetVis-0.9.5.1-w32.zip
  - Linux: inetvis/0.9.5/inetvis-0.9.5.1-linux.tar.gz
- Nota: La versión para linux porque usa librerias libmysqlclient ya obsoletas.

Ejemplo uso



Networkminer

- Reconstruir sesión red y archivos de un archivo de captura de paquetes.
- Host profiling y end point reporting.
- Herramienta windows
- Protocolos soportados: http, ftp, smb, etc.
- http://networkminer.sf.net/

Ejemplo NetworkMiner

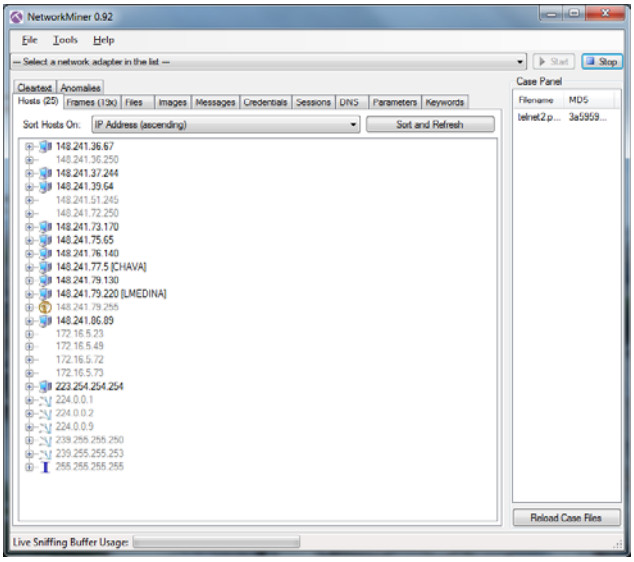


Lámina 41 Dr. Roberto Gómez Cárdenas

Búsqueda de strings en NetworkMiner

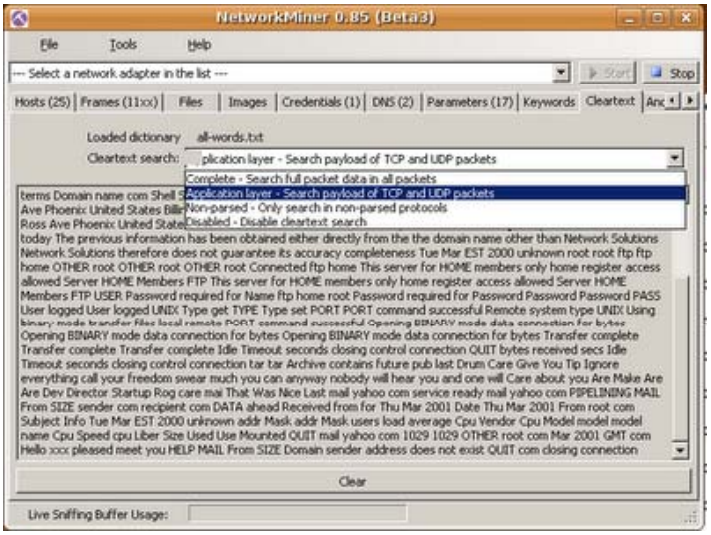


Lámina 42 Dr. Roberto Gómez Cárdenas

Foremost

- Capaz de extraer archivos basados en el encabezado, footer y estructura interna de una imagen dd y de archivos pcap.
- Utiliza una técnica conocida como carving.
- http://foremost.sourceforge.net/
- Uso:

```
foremost  -i archivo.pcap
```

  - los archivos extraídos se almacenan en un directorio de nombre output.

Lámina 43 Dr. Roberto Gómez Cárdenas

Foremost en acción

Lámina 44 Dr. Roberto Gómez Cárdenas

ClamAV

- Herramienta anti virus Open Source
- Soporta varios formatos de compresión
  - RAR, ZIP, UPX, etc.
- Detección de archivos maliciosos basados en firmas.
- Comprado por Sourcefire (desarrolladores de Snort) en agosto del 2007.
- Ejemplo

```
freshclam -datadir=/var/lib/clamav/
clamscan-d /var/db/clamav -r files dir/
```

Lámina 45 Dr. Roberto Gómez Cárdenas

Ejemplo salida

```
binary/iexplore.exe: Trojan.Poebot-32 FOUND
binary/dksfjhd.exe: Trojan.Proxy.Ranky-29 FOUND
binary/fgdkj.exe: OK
binary/ffkdl: OK
binary/kgjdfhg.exe: OK
binary/fkjhg.exe: OK
binary/uiwlkja.exe: Trojan.Proxy.Ranky-29 FOUND
binary/nude_pic.scr: OK
binary/bnxiu.exe: Trojan.Proxy.Ranky-29 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 60743
Engine version: devel-20060316
Scanned directories: 1
Scanned files: 9
Infected files: 4
Data scanned: 15.56 MB
Time: 7.448 sec (0 m 7 s)
```

Lámina 46 Dr. Roberto Gómez Cárdenas


Computo forense redes
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
Lámina 47
Dr. Roberto Gómez Cárdenas