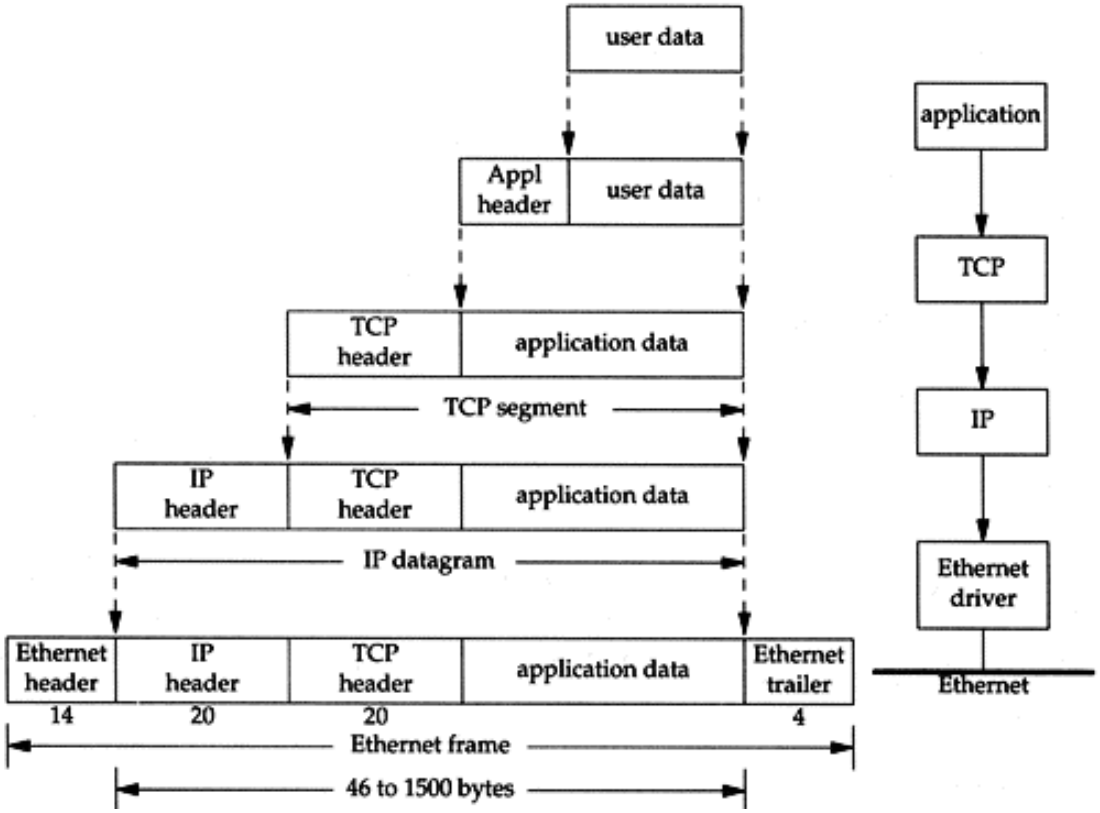
Técnica de las Escuchas/Interceptaciones Telemáticas

Corrado Federici

Tenerife, 16 mayo 2012

Prerrequisitos: los principales niveles OSI

La comunicación entre dos ordenadores se divide en fragmentos de tamaño variable (llamados Frame o datagrammi o paquetes)



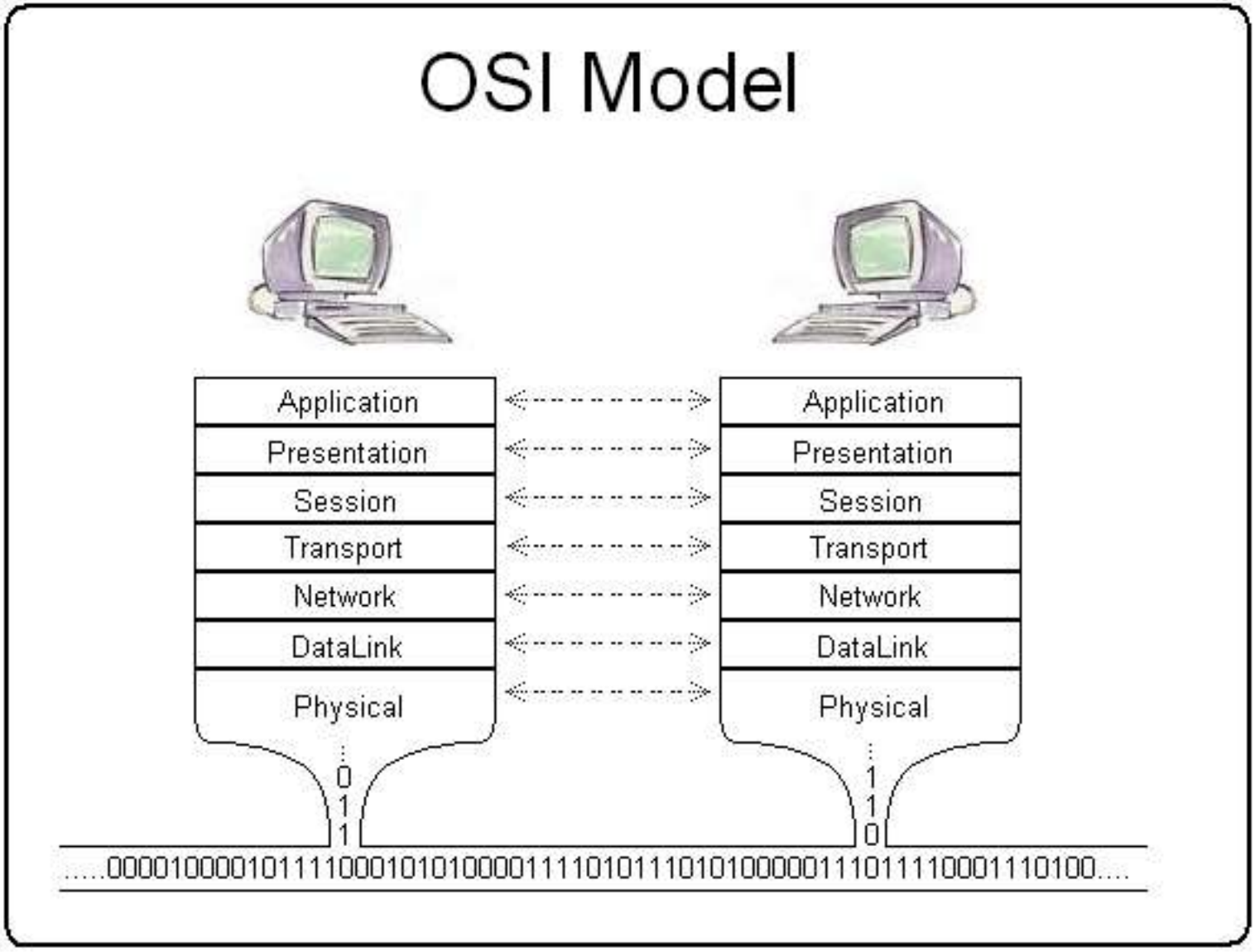
Nivel aplicativo (VII):
Chat, voip, mail, ...

Nivel transporte (IV):
Puertos: 80, 25, 110, 443,...

Nivel red (III):
Direcciones IP: 137.204.111.18

Nivel conexión de datos (II):
Direcciones MAC 14-DA-E9-AF-39-CE

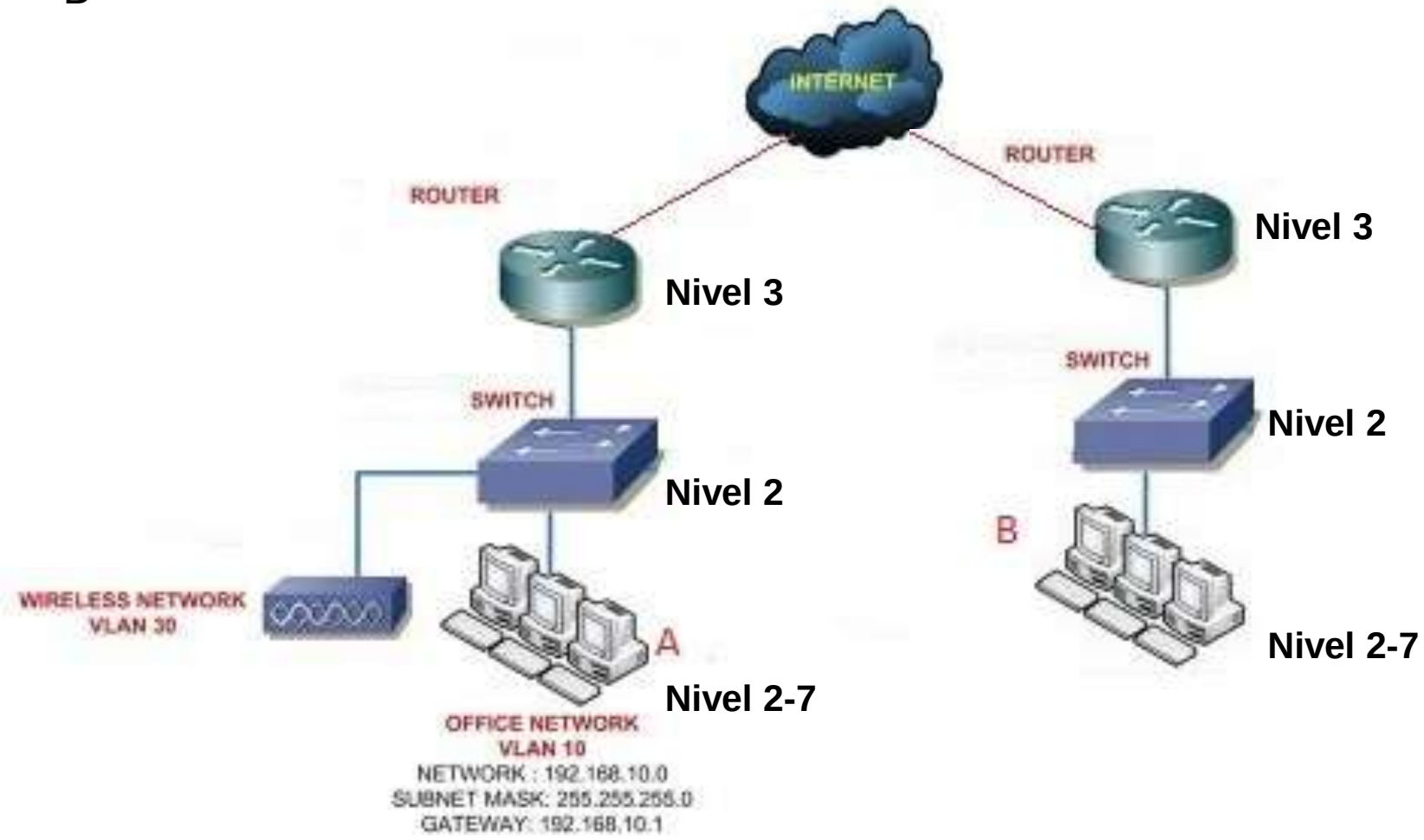
Prerrequisitos: comunicación entre dos peer



en.wikipedia.org

Prerrequisitos: comunicación entre dos peer

Es identificada por un par de números (dirección, puerta) llamada Socket Socket A (131.204.151.6,1025) ←→ (92.16.11.151,80) Socket B



Definición y Tipos

- Prevista en el art. 266 bis LECriminal
- Regulada en el art. 267 LECriminal: autorizadas por el juez de instrucción a petición del Ministerio fiscal por un máximo de 15 días (renovables)
- Consiste en averiguar el contenido de la comunicación efectuada entre sistemas informáticos o telemáticos mediante cualquier tipo de enlace (con cable o sin hilos)
- Se materializa en el uso de equipos informáticos (las llamadas ondas) específicos o genéricos (tras modificaciones),incluso de propiedad privada

Definición y Tipos

- Colocando y configurando acertadamente las sondas se realizan escuchas:

- Con un objetivo **individual o múltiple**: cuando se captura todo el tráfico relativo a uno o varios ordenadores, mediante una operación de filtro de **bajo y medio nivel** (nivel II,III,IV)

- **Aplicación** (llamada paramétrica): cuando se captura todo el tráfico relativo a un conjunto de ordenadores, mediante una operación de filtro de **alto nivel** (nivel 7)

Wiretapping (WT)

- En las redes de cable WT significa conectar una sonda en algún punto de una red para capturar el tráfico de datos de manera totalmente pasiva
- El plazo recuerda a la era de la telefonía analógica, cuando era posible escuchar una conversación mediante su interconexión en paralelo a la línea
- La misma actividad puede realizarse de forma legal o de manera abusiva teniendo, por tanto, nombres diferentes:

Operador	Actividad	Autorizada por
Amministrador de red	Sniffing	Propietario
Fuerzas del orden	Lawful Interception (LI)	Disposición judicial
Agente ilegal	Eavesdropping	Ninguna

¿Para qué sirve el WT en una red?

- **Análisis de las prestaciones:** congestión, cuellos de botella, detección de tarjetas de red defectuosas...
- **Detección de intrusiones:** ataques a los sistemas de información internos o externos, profiling de actividades de Spyware & malware …
- **Forensics en tiempo real**: recogida de indicios de otras actividades post mortem (recogida de log por los dispositivos de red)
- **Localización e identificación del hablante:** si los indicios de red son genuinos…

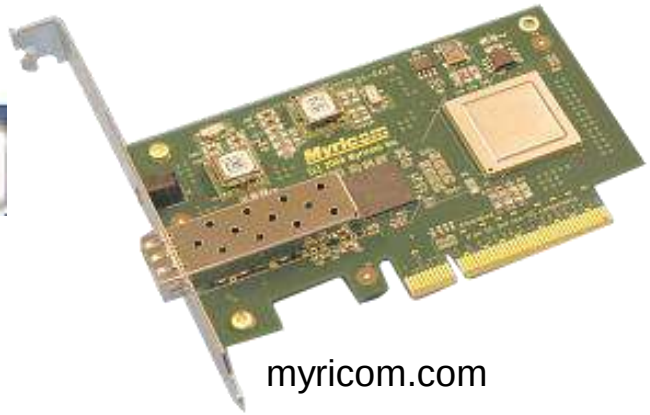
Elementos conceptuales de una LI: Sonda

La sonda es un dispositivo de primera línea pues viene expuesta a un tráfico de red, incluso muy elevado, y por tanto debe cumplir con funciones básicas:

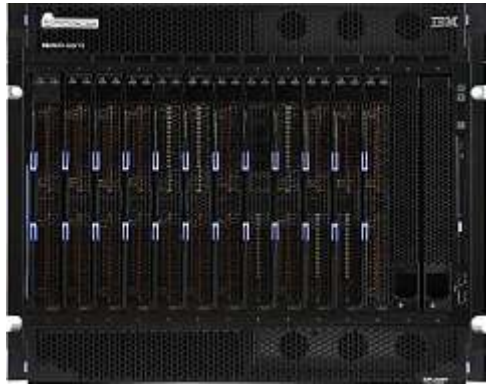
- Captura de los paquetes de datos
- Filtro opcional a nivel 2,3,4 o 7 en Hw (directamente sobre la tarjeta de red) o en Sw (a nivel de driver del SO)
- Memoria temporal (RAM/disco) y envío a otros elementos de red para un nuevo análisis

Son dispositivos específicos o bien COTS que utilizan SO optimizados para el objetivo(normalmente, Linux o FreeBSD)

ipoque.com



myricom.com

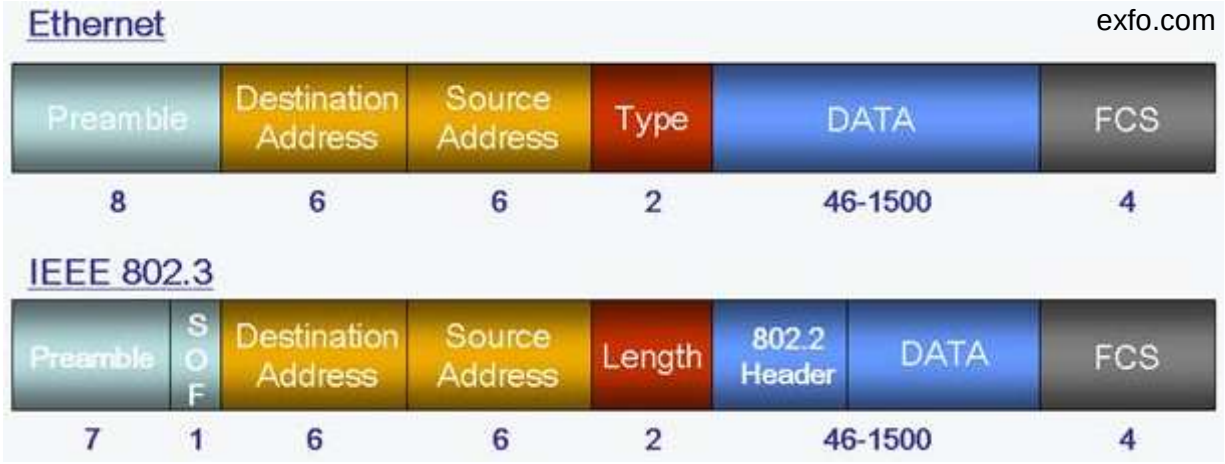


ibm.com

Elementos conceptuales de una LI: Repositorios y workstation

- Un repositorio backend (normalmente un database) contiene todos los paquetes completos capturados mediante hash
- Una aplicación de backend accede a los datos del repo:
  - ✓ Identifica las secciones y realiza controles de integridad
  - ✓ Descodifica los protocolos a todos los niveles (transforma los bit de manera comprensible para un ser humano)
  - ✓ Presenta los resultados de manera temporal y estructuralmente ordenados
  - ✓ Identifica ,autoriza y registra la actividad de los operadores (AAA)
- Por su ubicación en el trabajo, el operador accede a las aplicaciones y al análisis de los resultados mediante un navegador o un programa específico

¿Pero cómo es posible la captura?



Ethernet V2.0 MAC frame

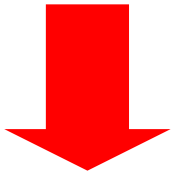
IEEE 802.3 frame

- Como se dijo, el tráfico de red está organizado en configuraciones de bits con una clara estructura
- Las tarjetas de red normalmente descartan los frames que no sean del tipo unicast o broadcast (FF-FF-FF-FF-FF-FF)
- Los software para la captura cambian este comportamiento e instruye a la tarjeta de red para reenviar todos los paquetes (modo "**promiscuo**")

Interacciones paramétricas

Escenario de ejemplo

- Las personas objeto de atención están localizadas en una posición desconocida de un área geográfica y acceden a servicios prestados por operadores exteriores
- En este caso, las únicas informaciones disponibles podrían encontrarse a nivel aplicativo



Patterns

Frases, direcciones e-mail, nombres de ficheros, nicknames…

Elementos de evaluación

Las sondas se sitúan en los puntos de agregación del tráfico de grandes áreas (en sentido ascendente o descendente de redes empresariales o incluso dorsales nacionales de tráfico)

Contras:

- ✓ Técnicamente muy díficil y costoso
- ✓ Ineficacia en presencia de conexiones codificadas
- ✓ Exigen una extrema especificidad de los pattern para evitar la recogida de datos irrelevantes

❑ **Pros**:

- ✓ A veces podría ser la única manera para obtener información en tiempos razonables para evitar las comisiones rogatorias
- ✓ Potencialmente útiles para identificar/localizar un target

Principio de funcionamiento

Dos modalidades para escuchas en redes IP distintas teniendo en cuenta el momento de la inspección:

- **Búsqueda "al vuelo" (on-the-fly seek)**:
  - ✓ Las sondas capturan los paquetes con filtro (opcional) a nivel 2, 3, 4 y buscan las palabras claves (inspección a nivel 7)
  - ✓ Los datos se colocan en la memoria rápida de la sonda (RAM) y se sobreescriben casi de inmediato
- **Memorización y búsqueda (store and seek)**:
  - ✓ Las sondas capturan los paquetes de datos con filtro (opcional) a nivel 2, 3 y 4 y los envían a los backend repository (memoria permanente)
  - ✓ La aplicación de backend busca las frases claves después de haber reconstruido las secciones (filtro nivel 7)

Comparaciones

Parámetro	On-the-fly seek	Store & seek
Costes	▪ Más contenidos: no requiere grandes aparatos de almacenamiento y de simplificación del tráfico (salvo en casos extremos)	Elevado: requiere veloces aparatos de almacenamiento y de simplificación del tráfico
Exhaustividad	Inferior: la sonda debe ser muy veloz y no puede hacer elaboraciones exhaustivas	▪ Superior: posibilidad de elaboraciones exhaustivas sobre datos cristalizados
Flexibilidad	Inferior: el tráfico, una vez inspecionado, se pierde para siempre	▪ Superior: puede variarse el set de frases claves también en un segundo momento
Garantías	▪ Superior si la calidad de las frases claves es óptima: no se corre ningún riesgo de conservar tráfico irrelevante (ni siquiera temporaneamente)	Inferior: hasta que el tráfico no se borra, pueden potencialmente ser conservados los contenidos del tráfico de los usarios de un área amplia

Soluciones técnicas

- Las soluciones comerciales disponibles (Ipoque, Qosmos,Verint, ..) no siempre constituyen un eficaz compromiso entre costes y prestaciones

- Existen, por tanto, alternativas de bajo coste que tienen un uso práctico sobre el terreno

Blueye Layer 7 Sniffer

Main features at glance

- Pcap compatible keyword driven sniffer
- Operates in real time on high traffic links (wired or wireless) or on off-line captures
- Rebuilds complete tcp sessions (e.g. phishing emails) or just captures interesting fram
- Fully configurable with simple text files
- Deployable in a distributed scenario, with many front end probes and a central backend (MySQL powered)
- Email alerts on relevant events
- Available for Windows 2000/XP/2003/Vista and Linux platforms
- Open source project under GPL2 license

www.blueye.it

Blueye Layer 7 Sniffer

- Proyecto de seguridad nacido en 2005 para afrontar el problema "de la aguja en un pajar"

- Criterio: "identificar con rapidez aquello que es potencialmente últil en el interior de un flujo telemático, pero de la manera más completa posible"

- Es una solución táctica o estratégica para detectar relevar pautas «interesantes» presentes en el tráfico de datos de redes por cable o sin ellos

Blueye Layer 7 Sniffer

- Blueye es una suite de aplicaciones Open Source que operan juntas para identificar las sesiones TCP que transportan patrones que han sido definidao por el usuario
- El protocolo final es un fichero de formato estándard (que se puede ver con Wireshark) que contiene todos los paquetes de la sesión desde el inicio hasta el final, garantizándose una correcta secuencia y sin duplicados
- Si no se especifican los patrones, Blueye se comporta como un sniffer normal que captura y guarda todos los paquetes en el disco fijo

Blueye Layer 7 Sniffer

- Reconstruye las sesiones TCP “al vuelo”, es decir, trabajando solo en RAM (ejemplo: e-mail, páginas web...) y escribe en el disco solo aquello que es interesante
- Los patrones pueden ser especificados en formato ASCII o en bruto
- Configurable con simples ficheros de texto
- El control de los paquetes se puede hacer sobre el tráfico en tiempo real así como en capturas ya realizadas por otros

Blueye Layer 7 Sniffer

- Reconstruye las sesiones TCP “al vuelo”, es decir, trabajando solo en RAM (ejemplo: e-mail, páginas web...) y escribe en el disco solo aquello que es interesante
- Los patrones pueden ser especificados en formato ASCII o en bruto
- Configurable con simples ficheros de texto
- El control de los paquetes se puede hacer sobre el tráfico en tiempo real así como en capturas ya realizadas por otros

Microespías informáticos

Presupuestos

- Son “agentes” software extremadamente sofisticados que se instalan en el ordenador sujeto a investigación
- Permiten capturar y enviar a un centro de escucha todos los contenidos que se han intercambiado mediante la conexión a Internet del sujeto investigado
- Se trata del único medio posible cuando la interceptación telemática del canal de transmisión es imposible (Skype y otros)

Funciones de captura

- Audio de micrófono y auriculares
- Teclas pulsadas (key-logger)
- Captura de pantalla
- Movimientos del ratón
- Fotografías mediante la Webcam
- Tráfico de red
- Achivos existentes en el ordenador (documentos, imágenes, audio, video, ...)

Funciones de ocultación

- Ausente de la lista de los procesos activos
- Ausente de la lista de las conexiones activas (netstat –a en símbolo del sistema)
- Cifrado y firma de las comunicaciones frente a una estación de recepción de internet
- Desactivación con una orden (en remoto) o por un tiempo determinado (pej. porque termina el periodo autorizado por el decreto)
- Memorización temporal y transmisión concomitante con otros programas

Gracias por vuestro tiempo

Corrado Federici

corrado.federici@unibo.it