CURSO DE PRÁCTICA OPERATIVA EN INVESTIGACIÓN

MÓDULO 5

INTERNET, DOCUMENTACIÓN Y BASES DE DATOS

HERRAMIENTAS DE INVESTIGACIÓN

Y

SEGURIDAD EN INTERNET

Daniel Fernández
dfernandez@isecauditors.com

Xavier Carbonell
xcarbonell@isecauditors.com

4 de Julio de 2003

Índice

- Introducción
- Intrusiones y ataques
- Métodos de defensa
- Técnicas de detección
- Localización y Preservación de la evidencia digital
- Casos de Investigación

¿Qué es un cibercrimen/ciberdelito?

- Cibercrimen o ciberdelito es aquel acto delictivo que emplea Internet de dos posibles formas:
  - Como una vía más para cometer el delito:
    - Estafa a través de correo electrónico
    - Apuestas, juego, ventas, etc. ilegales
    - Distribución de pornografía infantil
    - Piratería de propiedad intelectual
    - Espionaje industrial
    - etc.
  - Como objetivo sin el cual no existiría el delito:
    - Intrusión en sistemas o redes
    - Ataques de DoS a sistemas de información
    - etc.

Categorías de ciberdelito

- La UE definió los ciberdelitos en el Convenio sobre la Ciberdelincuencia (23.XI.2001):
  - Delitos contra la confidencialidad, integridad, disponibilidad de los datos y sistemas informático.
    - Acceso ilícito
    - Interceptación Ilícita
    - Interferencia en los datos
    - Interferencia en el sistema
    - Abuso de los dispositivos
  - Delitos informáticos:
    - Falsificación informática
    - Fraude informático
  - Delitos relacionados con el contenido:
    - Delitos relacionados con la pornografía infantil
  - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Actores de un cibercrimen

- El mito del cibercriminal lo define así:
  - Muy inteligente, fanático de los ordenadores pero no integrado socialmente.
  - Adolescentes varones no violentos.
  - No cometen delitos en el mundo real.
  - etc, etc, etc.....
- La realidad es que el perfil del cibercriminal cada vez es más amplio: +600 Millones de usuarios de Internet no son fáciles de clasificar .
- Las razones del cibercriminal encajan en estas:
  - Por diversión o reto
  - Provecho monetario
  - Venganza
  - Motivaciones políticas o ideológicas
  - Motivaciones sexuales

Índice

- Diferencias entre Intrusiones y Ataques
- Tipos de ataques
    - Directos
    - Distribuidos
- Ataques automáticos
- Actividades de ataque
- Hacking para todos

Intrusiones vs. Ataques

- El ataque precede a la intrusión.
- Es posible realizar un ataque sin entrar en una máquina o sistema.
- Los ataques acostumbran a tener una duración menor que las intrusiones, y normalmente no se altera el sistema atacado, mientras que en las intrusiones si.
- La recuperación de los sistemas frente a un ataque es siempre mucho más rápida.
- Una intrusión puede implicar fugas de información, mientras que un ataque no.
- Un ejemplo de un ataque podría ser un ataque de Denegación de Servicio (DoS).

Ataques Directos/Distribuidos

- Ataques Directos:
  - Lanzados desde el ordenador del atacante.
  - Fácilmente localizables y neutralizables
- Ataques Distribuidos:
  - Más complejos.
  - Utilizan múltiples máquinas, llamadas agentes o *zombies*.
  - Comunicación cifrada entre el atacante y los agentes.
  - Dificultad para localizar al atacante (múltiples orígenes del ataque).

Ataques automáticos

- La tendencia actual es a la automatización de los ataques.
- Hace unos años, la realización de un ataque requería....
    - Herramienta que busca una vulnerabilidad en concreto.
    - Otra herramienta que explota la vulnerabilidad.
    - Otra para propagar el ataque a otras máquinas.
- Actualmente una sola herramienta o programa autónomo hace todos los pasos anteriores.
- Ejemplos:
    - CodeRed
    - Nimda

Actividades de ataque

- Un ataque comienza con recogida de información sobre los sistemas:
  - Escaneos de Puertos: conocer los tipos de sistemas, entradas al sistema y tipos de estas entradas.
  - Búsqueda de información pública en CVs, foros, grupos de noticias, etc. que ayude a conocer el sistema a atacar.
- Una vez se conocen los sistemas, podemos emplear técnicas más o menos avanzadas apara llegar a la intrusión:
  - Atacar los servicios ofrecidos por las máquinas aprovechando vulnerabilidades o deficiencias de configuración.
  - IP (Internet)/ARP (Intranet) Spoofing: falsear el origen de intento de acceso al sistema con el fin de evitar protecciones o redirigir el tráfico para poder capturarlo.
  - Troyanización: conseguir que en el interior de la red se ejecute un programa que se conecte al atacante de forma automática, instalar programas de escucha, etc.
  - Password cracking: ataques a accesos protegidos con contraseña.
  - Ejecución de exploits: uso de pequeños programas que explotan vulnerabilidades o deficiencias de seguridad específicas.
  - Ataques con virus y gusanos.

Hacking para todos

- Los ataques emplean técnicas cada vez más evolucionadas o que convinan diversos métodos en un mismo ataque.
- La facilidad de uso de herramientas de hacking ha evolucionado como cualquier otro software:
  - El caso del script kiddie o hacker ignorante:
    - Hace unos años, algunos de los ataques requería conocimientos técnicos muy elevados.
    - Ahora existen herramientas que realizan automáticamente los ataques.
    - Herramientas de Point&Click Hacking: muchas veces se realizan ataques sin saberlo o sin conocer qué se está haciendo en ese ataque.
  - El caso del hacker 31337:
    - La información realmente dañina se mueve en ámbitos limitados en manos de gente con elevados conocimientos.
    - Los hackers de la élite siempre van por delante a los sistemas de defensa, o definen nuevos sistemas de defensa.
    - Los expertos en seguridad no siempre están en el lado oscuro.

Índice

- Introducción a los métodos de defensa
- Elementos de protección
- Firewall / IDS
- Antivirus

Introducción

- La seguridad es un proceso.
- Es importante actuar siempre de forma proactiva y no reactiva.
- Son necesarias una política de seguridad en la empresa respaldada por dirección.
- La política de seguridad establece las directrices de la empresa:
    - Necesidades de seguridad.
    - Recursos asignados.
    - Prioridades.
    - Procedimientos de seguridad.
    - etc.
- Planes de contingencia.
- Recuperación ante desastre.

Elementos de protección

- La primera medida de protección es la propia arquitectura de red de la empresa.
  - Red interna separada de la red pública (DMZ - Demilitarized Zone).
  - Acceso a Internet desde la red interna mediante NAT.
- Es necesario disponer de dispositivos de protección en el perímetro de la empresa (seguridad perimetral - entre Internet y la red de la empresa):
  - Firewall o Cortafuegos.
  - Software de Antivirus.
  - Sistemas de detección de Intrusos (IDS).
- Los propios sistemas accesibles desde Internet son elementos de protección:
  - Fortaleza de las contraseñas.
  - Deshabilitación de servicios innecesarios.
  - Hardening de sistemas.

Firewall / IDS

- Firewall:
  - Software / Dispositivo de red que filtra todo el tráfico que entra o sale de la red.
  - Filtran en función de unas reglas en las que se indica el tipo de tráfico permitido y el que no.
  - Existen también firewall personales que se instalan en los PCs personales.
  - Se dividen en:
    - S*creening routers*: Filtran por dirección de origen y destinatario y por servicio que utilizan.
    - *Stateful inspection filters*: En el filtrado tienen en cuenta el estado de la comunicación. Más evolucionados que los anteriores.
- IDS:
  - Software / Dispositivo de red que analiza continuamente todo el tráfico que circula por ella.
  - Parten de una serie de patrones de ataques conocidos que intentan identificar en el tráfico de analizan.
  - Si identifican un ataque pueden actuar en consecuencia (bloquear al atacante, avisar por mail al administrador de sistemas, etc.).

Antivirus

- Antivirus:
  - Detecta la presencia o llegada de virus/gusanos/código malicioso.
  - La detección la realizan a partir de las “firmas” de los virus o por el comportamiento de los programas.
  - Actualmente la infección vírica se realiza a través de los correos electrónicos.
  - ¿Dónde se sitúan los sistemas antivirus?:
    - A nivel de gateway o servidor de correo.
    - A nivel de cliente en los PCs de los usuarios.

- La tendencia actual es fusionar los tres sistemas anteriores en uno.

Índice

- Introducción
- Preparación de los sistemas: Auditoría + Logs
  - Auditoría en Sistemas Windows
  - Auditoría en Sistemas Unix
- Análisis de logs
  - Logs de un servidor web
  - Logs de un firewall
  - Logs de sistema
  - Logs de un servidor de correo
  - Cabeceras de mails
- Investigación mediante herramientas accesibles desde Internet

Introducción

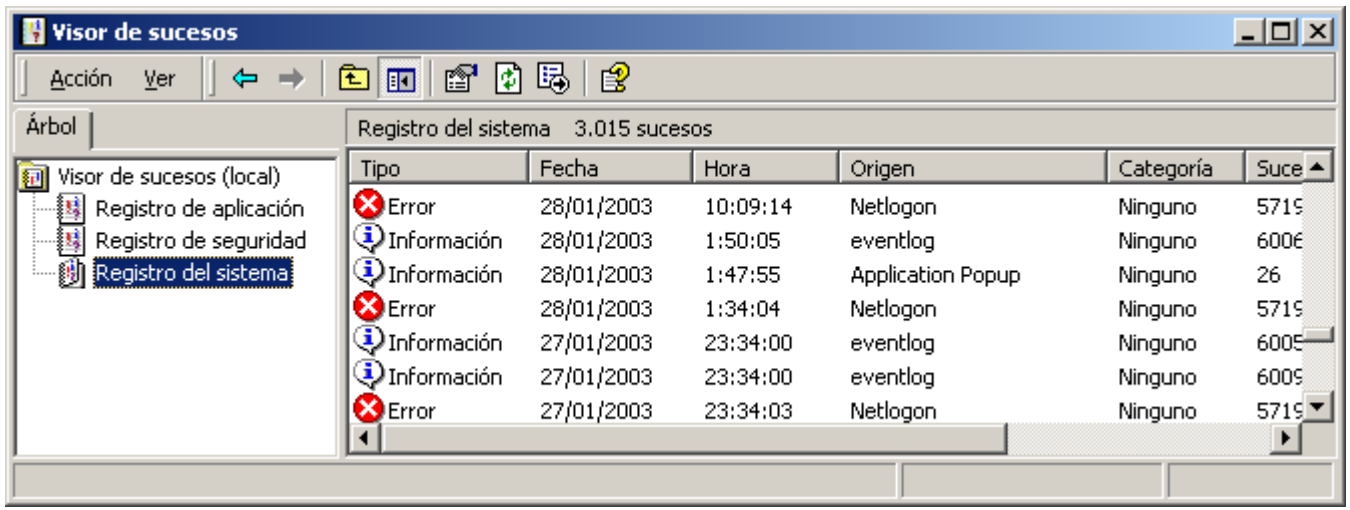
- Las técnicas de detección hacen referencia a las técnicas y herramientas disponibles por el investigador para obtener información en caso de ataque o de una intrusión efectiva en un sistema.
- La detección se realiza a dos niveles:
  - Local: Primero se ha de obtener toda la información posible del sistema atacado. La información a buscar será:
    - ¿Qué se ha hecho en la máquina?
    - Datos de identificación del atacante (IP, SW utilizado, nick, etc.)
    - ¿Cómo se ha conseguido entrar en el sistema?
  - Internet: A partir de los datos obtenidos podemos seguir investigando en Internet.
- Los ataques pueden producirse también de forma interna dentro de la propia empresa.

Preparación: Auditoría + Logs

- Los sistemas se pueden preparar para facilitar una investigación en caso de sufrir una intrusión.
- Para ello se han de activar las capacidades de auditoría y de logeo, tanto a nivel de sistema operativo como a nivel de aplicaciones:
    - Auditoría: Identifica el acceso o uso de recursos del sistema y deja constancia de ello.
    - Logs: Los ficheros de log son el resultado de la auditoría donde queda reflejada la actividad del sistema, siendo una prueba clave como evidencia de una intrusión al sistema, pues puede quedar reflejada en ellos.
- El concepto fundamental es AAA (triple A): Autenticación + Autorización + Accounting
    - Autenticación: Permite asegurar la identidad del usuario.
    - Autorización (control de acceso): Delimita el acceso a los recursos en función de los usuarios, perfiles, y privilegios.
    - Accounting: Monitoriza y tracea la actividad del sistema. Si se realiza desde el punto de vista de la seguridad, se llama auditoría.

Auditoría en Windows I

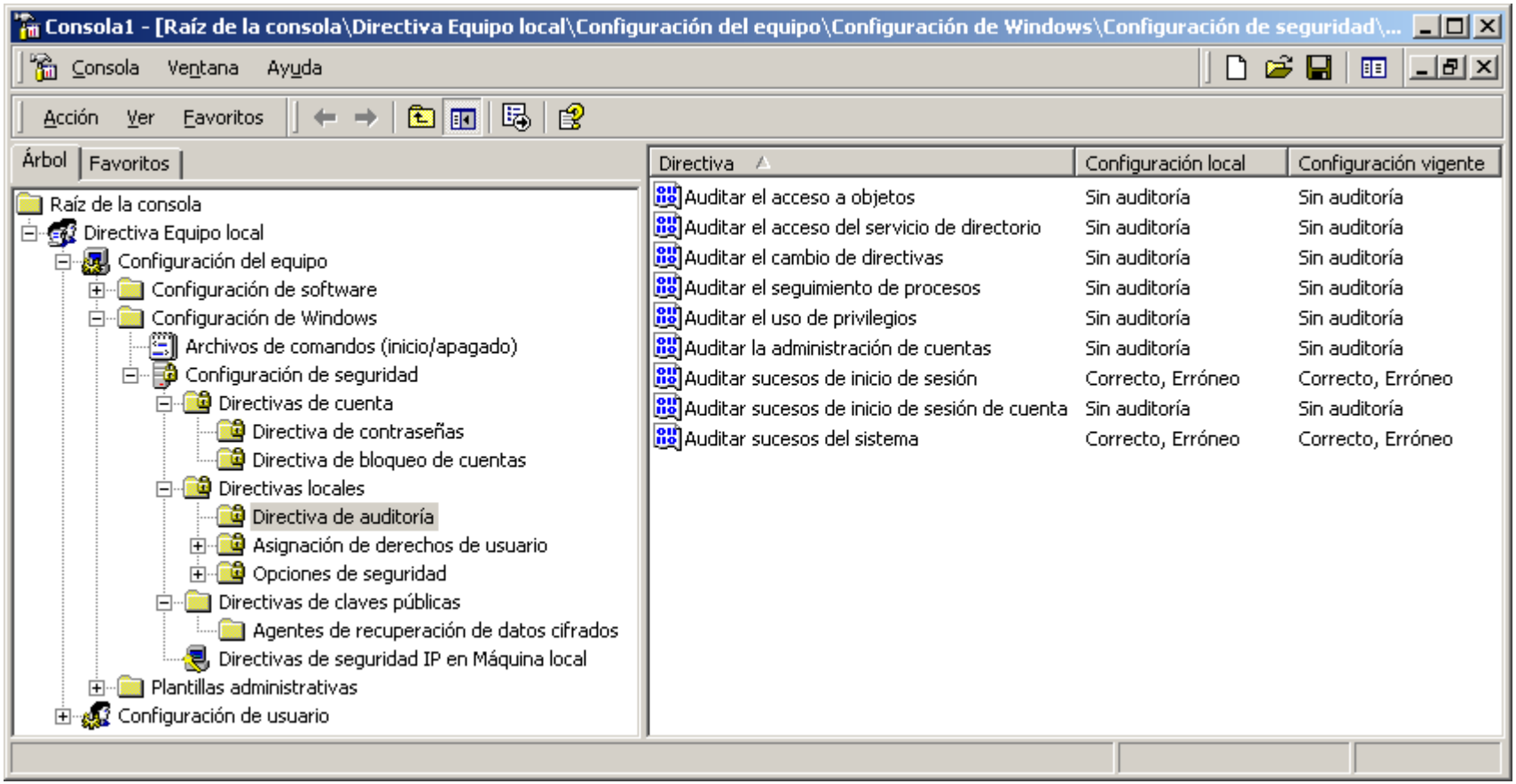
- Las plataformas Windows (95/NT/2000/...) poseen capacidades de autoría.
- Tres niveles de auditoría:
  - Log de Aplicación: Mensajes + info. de estado + eventos reportados, de aplicaciones no esenciales.
  - Log de Sistema: Errores + warnings + eventos, generados por el propio SO o por los sistemas esenciales.
  - Log de Seguridad: Muestra todos los intentos con éxito o fracaso de todas aquellas actividades que se auditan.



Auditoría en Windows II

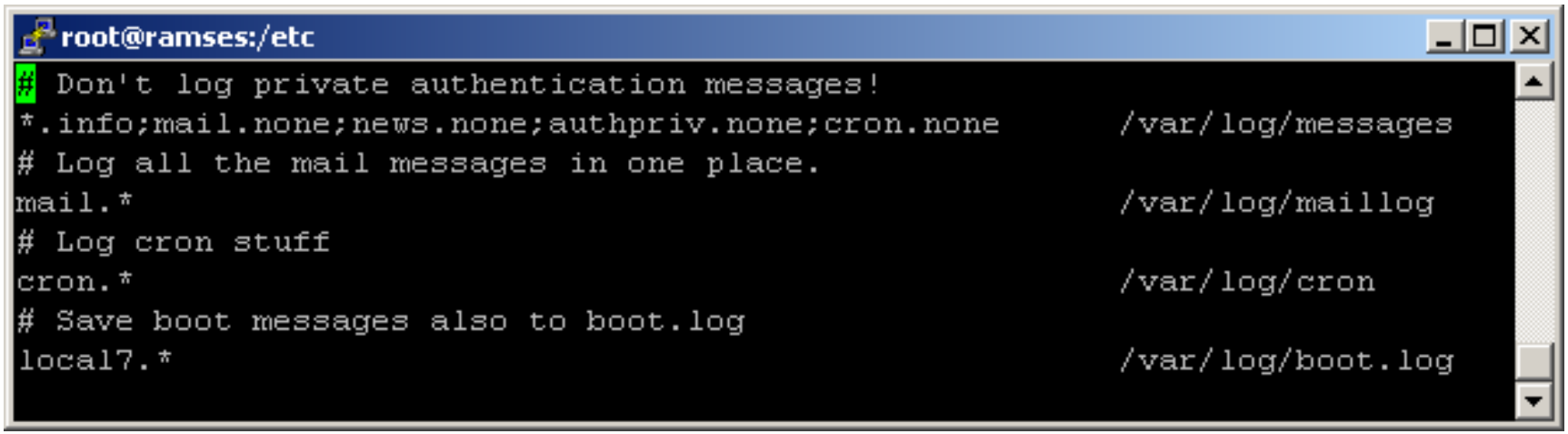
- Clases de eventos o actividades que se pueden auditar en Windows 2000:
  - Eventos de logon
  - Cuentas de Administración
  - Acceso a Servicios de Directorio
    - Eventos de logon
    - Acceso a objetos
    - Cambios de política
    - Uso de privilegios
    - Tracking de procesos
    - Eventos de sistema

Auditoría en Windows III



Auditoría en Unix

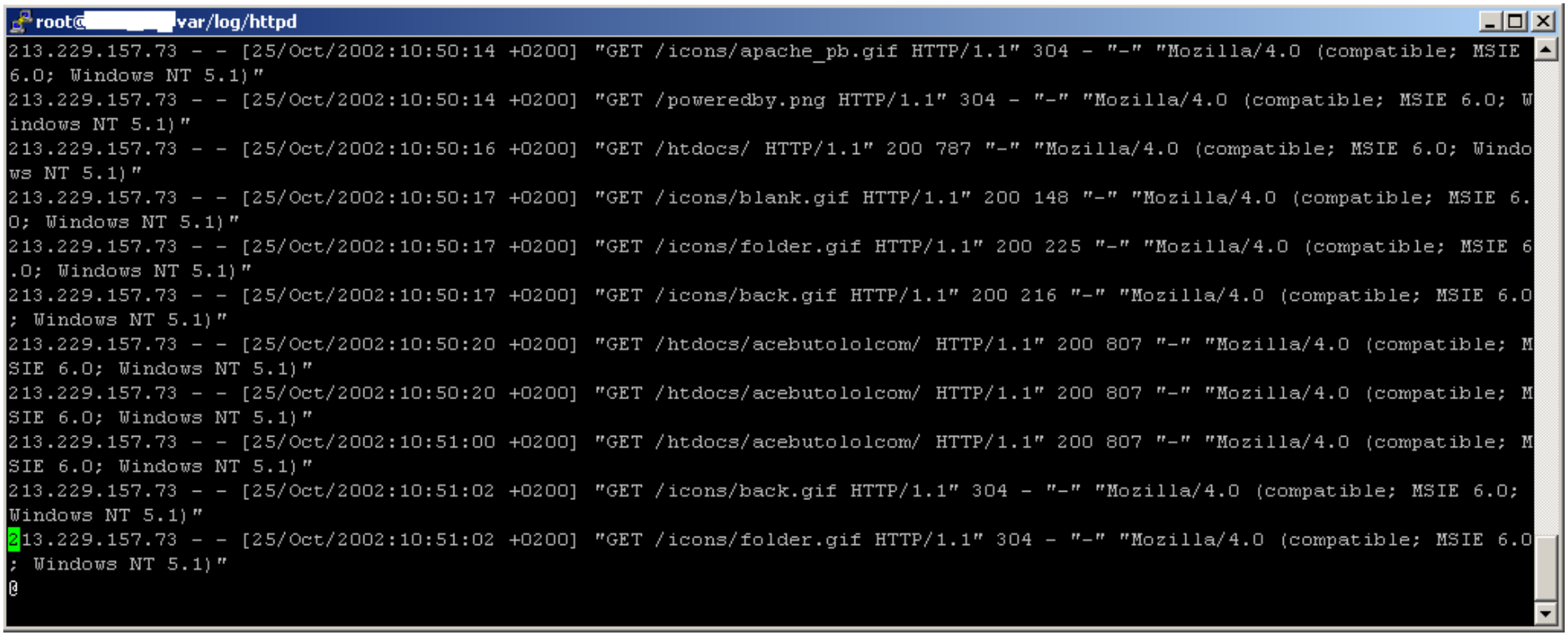
- El responsable de la auditoría en sistemas Unix/Linux es el demonio Syslog.
- El demonio distribuye diferentes mensajes de sistemas a distintos ficheros de log, dependiendo del tipo de mensaje y de su urgencia o severidad.
- Los logs de los diferentes sistemas de una red en entornos Unix se suelen centralizar en una única máquina.



Análisis de logs

- Una vez se ha producido una intrusión en una sistema, los ficheros de logs son una de las principales fuentes de evidencias.
- Pero los logs a veces no son sencillos de entender.
- Existen aplicaciones que interpretan los logs de estos dispositivos.
- Ejemplos de logs que se pueden tener que analizar en caso de una intrusión:
  - Logs del servidor web.
  - Logs de mensajes del sistema.
  - Logs del firewall.
  - Cabeceras de mails.

Ej: Logs de un Web Server



Ej: Logs de un Firewall

PE,2003/06/27,09:46:20 +2:00 GMT,Aplicación de servicios y controlador,219.9.65.14:53,N/A

PE,2003/06/27,09:47:15 +2:00 GMT,FTP Transfer Engine,217.76.135.104:22,N/A

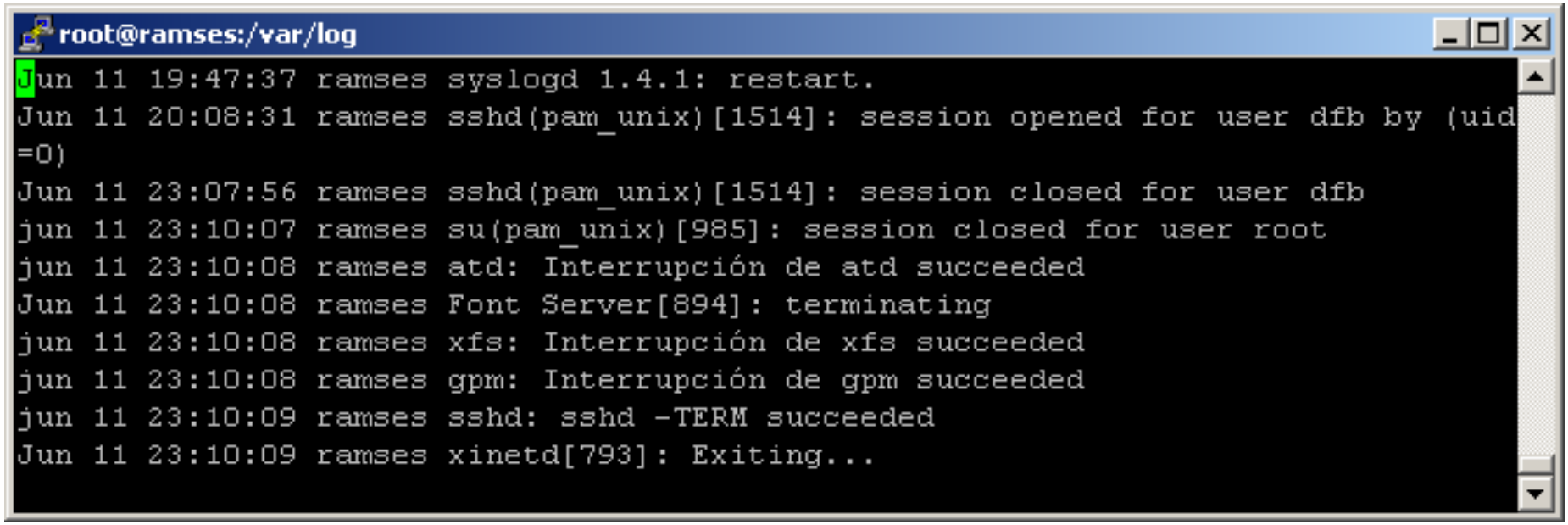
FWOUT,2003/06/23,10:07:38 +2:00 GMT,10.10.0.51:1347,216.34.38.96:80,TCP (flags:R)

PE,2003/06/27,09:47:22 +2:00 GMT,putty.exe,217.76.135.104:22,N/A

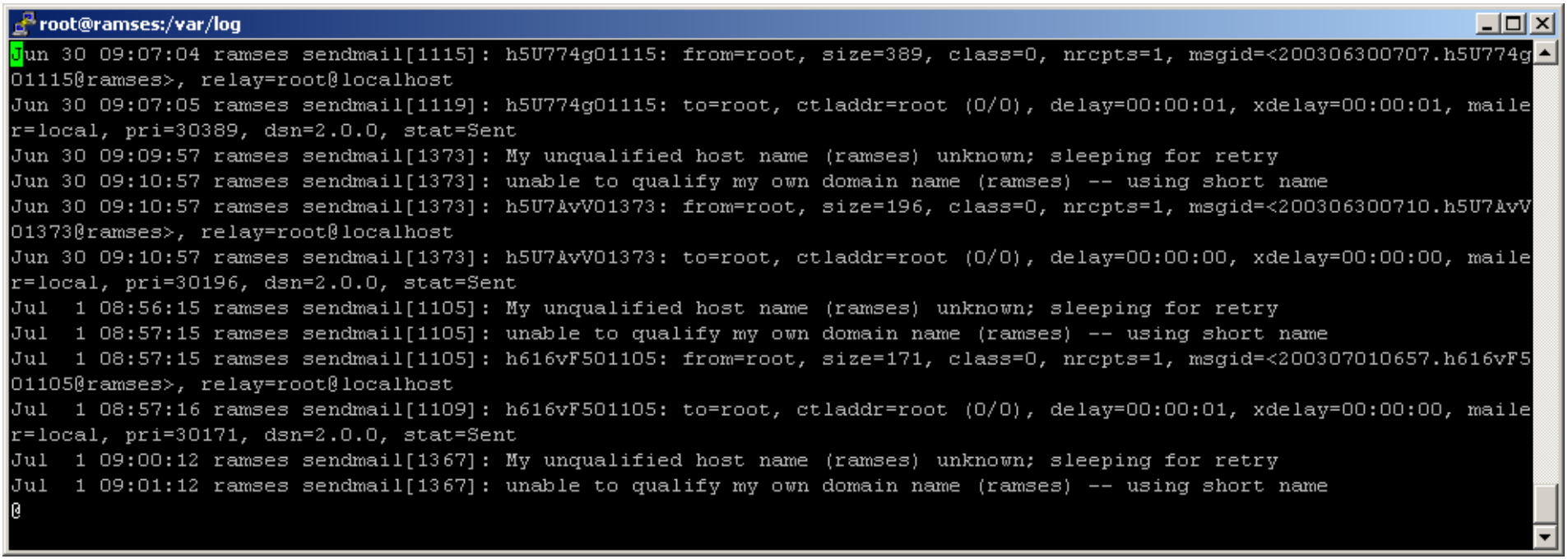
PE,2003/06/27,09:50:22 +2:00 GMT,Generic Host Process for Win32 Services,207.46.249.61:80,N/A

ACCESS,2003/06/26,17:37:27 +2:00 GMT,java.exe was unable to obtain permission for connecting to the Internet (217.76.128.102:SMTP); access was denied.,N/A,N/A

Ej: Logs de sistema



Ej: Logs servidor de correo



Cabeceras de mails I

- Los correos electrónicos son hoy en día una de las principales puertas de entrada para ataques y infecciones en las empresas
- Pero los correos electrónicos también son malévolamente utilizados para:
  - Acosar a las víctimas
  - Enviar demandas de extorsión, amenazas, etc.
  - Contactar con víctimas potenciales (pedófilos, violadores, etc.)
  - Timos (de pirámide, etc.)
  - etc.
- Siendo los propios correos la única pista para identificar al criminal
- Normalmente los criminales no firman el correo con su nombre, dirección y teléfono
- A simple vista puede que no nos revelen información, pero.....

y las CABECERAS de los correos?

Cabeceras de mails II

- Los correos electrónicos “viajan” por diferentes ordenadores hasta llegar al destinatario.
- Cada servidor por los que pasa el correo añade información en la cabecera de este.
- Es necesario conocer qué información podemos obtener y cual no. Los campos más importantes que podemos ver (RFC-822 - email headers):
    - From: Identifica el emisor del mensaje (nombre o dirección de correo)
    - Sender: Identifica el actual emisor del mensaje (puede variar del “from”)
    - Reply-to: Dirección de correo a la que las respuestas tendrán que ser enviadas
    - Received: Cada servidor de correo por el que pasa el email, añade su propia linea de received”
    - Message-ID: Identificador único del mensaje dentro del servidor de correo que lo ha originado.
- Es importante comprender que toda la información puede ser falseada.

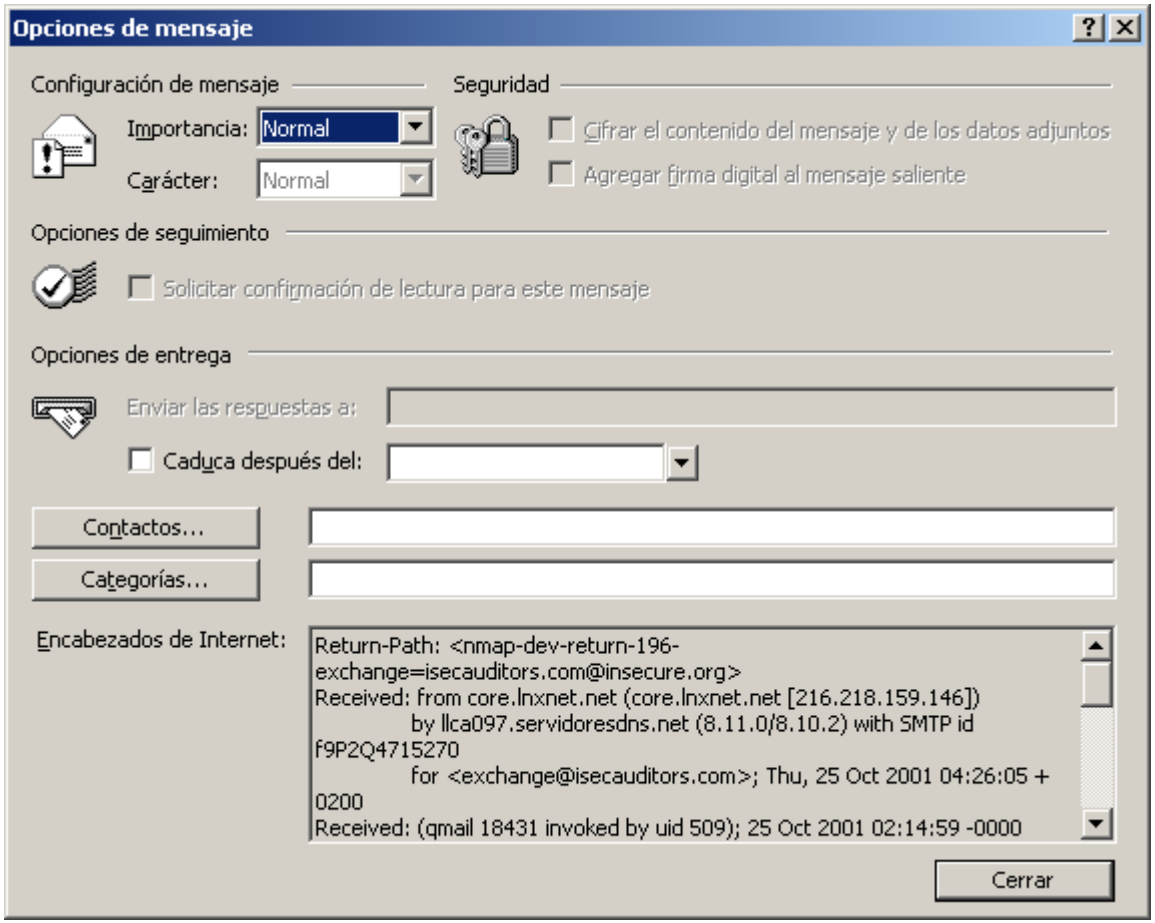
Cabeceras de mails III

```
Return-Path: <boletin@kriptopolis.com>
Received: from localhost (SC1-1A-u-0035.mc.onolab.com [62.42.144.36])
          by llca097.servidoresdns.net (8.11.0/8.10.2) with ESMTP id g4RIaqi10332
          for <dfernandez@isecauditors.com>; Mon, 27 May 2002 20:36:52 +0200
Received: from test (unknown [192.168.3.128])
          by localhost (Postfix) with SMTP
          id D48651A1CC; Mon, 27 May 2002 20:24:11 +0200 (CEST)
From: Kriptopolis <boletin@kriptopolis.com>
To: Boletin <boletin@kriptopolis.com>
Reply-To: boletin@kriptopolis.com
Subject: Sobre nuestro Boletin
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
Message-Id: <20020527182411.D48651A1CC@localhost>
Date: Mon, 27 May 2002 20:24:11 +0200 (CEST)
Content-Transfer-Encoding: 8bit
X-MIME-Autoconverted: from quoted-printable to 8bit by llca097.servidoresdns.net id g4RIaqi10332
Status:
```

Cabeceras de mails IV

• Pero y ¿cómo podemos ver estas cabeceras de los correos en los lectores de correo que se utilizan habitualmente?

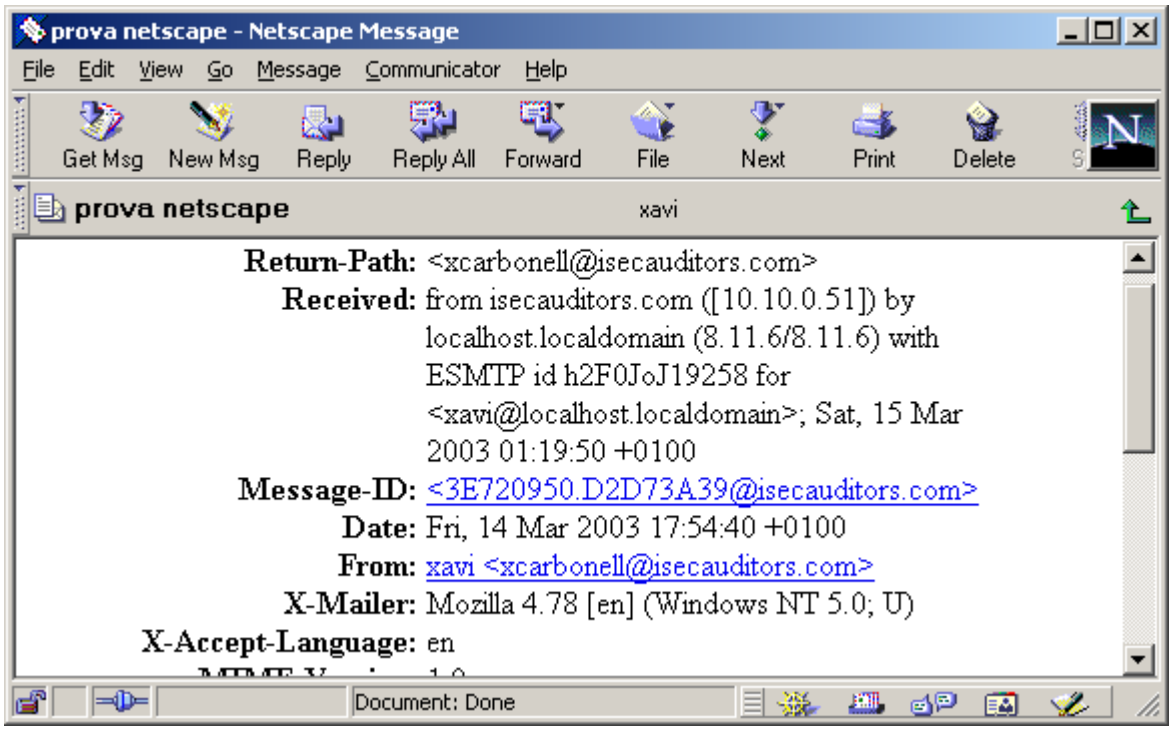
• OUTLOOK: Una vez abierto el mensaje, desde la opción “Ver + Opciones”:



Cabeceras de mails V

• Outlook Express: Una vez abierto el mensaje desde la opción “Archivo + Guardar como” guardamos el mensaje con extensión .eml. Una vez guardado lo podemos abrir con cualquier editor de texto, y podremos ver la cabecera del mail.

• Netscape Communicator: Permite ver la cabecera en todos los mensajes que recibimos de forma automática. Para ello es necesario activar la opción “View + Headers + All”:



Investigación Internet I

- Una vez se han recabado todos los datos posibles en el sistema analizado podemos continuar la investigación en Internet.
- En Internet existen muchas páginas de donde sacar información:
  - Motores de búsqueda genéricos
    - google (www.google.com)
    - terra (www.terra.es)
    - yahoo (www.yahoo.com)
    - altavista (www.altavista.com)
    - lycos (www.lycos.com)
    - etc.
  - Existen programas que realizan una búsqueda automatizada en muchos motores de búsqueda de Internet, facilitando la tarea del investigador al tener centralizada de esta forma toda la búsqueda de información.
    - copernic (www.copernic.com)

Investigación Internet II

• Otra fuente de información en Internet son los nombres de dominios y las IPs. La identificación en el sistema analizado de la supuesta IP desde la que se originó el ataque nos permite proseguir la búsqueda del atacante.....

•Teoría: Cada sistema visible en Internet tiene un identificador único (IP), pero como que no son fáciles de recordar para las persones, también tienen un nombre (p.e. www.collegidetectius.org). La traducción de nombres a IPs la realizan los Servidores de Nombres de Dominios (DNS - Domain Name System).

• P.e. Al poner un nombre como dirección en un navegador (www.google.com), internamente el navegador hace una petición a un DNS para que le traduzca el nombre a qué IP corresponde.

• En una investigación podemos encontrarnos en la necesidad de saber a quién corresponde un dominio, o una determinada IP a quién corresponde:

- dominios .es (www.nic.es)
- dominios .com / .net / .org (www.networksolutions.com)
- relación IPs con dominios (www.ripe.net)
- localizar una IP (www.visualroute.com)

Investigación Internet III

- Webs con herramientas útiles:
  - (www.samspade.org)
  - (http://centralops.net/co/body.asp)
  - (http://www.demon.net/external/)
- También puede ser necesario o a veces útil investigar las historia o cambios que se han producido a lo largo del tiempo en las páginas web:
  - (www.archive.org)

Índice

- Informática forense.
- Introducción a la Informática forense.
- Estándares de localización
- Preservación de la evidencia digital.
    - Preservación de los datos volátiles.
    - Preservación de los datos no volátiles.
- Recuperación de la evidencia digital

Informática forense

- Informática forense: Es la especialidad en la que se fusionan la informática con la investigación y que proporciona las bases para la localización y preservación de la evidencia digital.
- Asociaciones donde encontrar abundante información:
  - The International Association of Computer Investigative Specialists (www.cops.org)
  - Asociación de Expertos Forenses en Tecnologías de la Información (www.aeftic.org)
  - International Organization on Computer Evidence (www.ioce.org)
- Revistas online especializadas:
  - International Journal of Digital Evidence (www.ijde.org)

Introducción

- En el entorno informático una evidencia es de uno de estos 3 tipos:
  - Evidencia Digital: Información de valor para el caso que es transmitida o guardada en formato digital.
    - Evidencia digital original
    - Evidencia digital duplicada
  - Objetos de datos: Información valiosa relacionada con el caso asociada a objetos físicos.
  - Objetos físicos: Soporte físico sobre el que se guarda la información digital.
- Las evidencias “escritas“ las podemos clasificar en:
  - Evidencia demostrativa: Reconstruye la escena o incidente en cuestión.
  - Evidencia de documentación: Documentos escritos que constituyen una evidencia.
- En el mundo digital dado la facilidad de realizar copias exactas de documentos, generalmente se considera la evidencia digital cómo evidencia demostrativa.

Estándares de localización

- Las diferentes organizaciones de informática forense coinciden en los estándares a seguir en la localización de las evidencias digitales:
  - La evidencia ha de ser conservada de la forma más parecida a cómo se encontró
  - Si es posible, se realizará una copia o imagen exacta del original, para poder hacer las investigaciones sin dañar el original
  - Las copias que se hagan del original, se tienen que hacer en un medio *forensicamente estéril* (disco virgen sin datos previos, sin sectores defectuosos, etc.)
  - Todas las evidencias han de ser marcadas y documentadas, así como todos los pasos realizados en la investigación documentados en detalle.
- Existe también un RFC (Request For Comments, de la Internet Engineering Task Force) que establece las bases para la localización y preservación de las evidencias digitales:
  - RFC 3227 - “Guidelines for Evidence Collection and Archiving”

    (http://www.ietf.org/rfc/rfc3227.txt?number=3227)

Preservación

- Por naturaleza la Evidencia Digital es frágil:
  - Parte es volátil: Está en la memoria temporal de los ordenadores, y cuando estos se apagan se pierde.
  - Parte es no volátil: La que permanece en el disco duro, pero esta es fácilmente destruida, o modificada (accidental o deliberadamente).

- Pasos básicos para la preservación:
  1. Preservación de los datos volátiles.
  2. Realizar una imagen completa a nivel de bit del medio donde se almacena la evidencia (ficheros ocultos, corruptos, fragmentados, borrados, etc.)
  3. Comprobar la integridad de la imagen realizada.
  4. Apagar el sistema analizado (quitando la corriente).
  5. Conservar el sistema en un lugar seguro.

Datos volátiles

- Donde se encuentran? RAM, Memoria cache, en la memoria de periféricos (tarjeta de video, de red, etc.).
- Problema: su propia recolección implica cambiar el estado del sistema y por lo tanto del contenido propio de la memoria.
- Existen algunas herramientas para obtener esta información volátil:
  - netstat / nbdstat: Muestran las conexiones de red.
  - arp: nos permite conocer que máquinas se han conectado recientemente con el sistema analizado.
  - ps / pslists: Muestran los procesos que están corriendo en la máquina.
  - ifconfig / ipconfig: Nos dan información sobre el estado de la red.
  - dd: Permite hacer una copia del contenido de la memoria en máquinas Unix.

Datos no volátiles

- Donde se encuentran? Básicamente en el disco duro de la sistema analizado.
- Datos no volátiles → duplicado del disco duro (imagen)
- Formas para hacer la imagen:
  - Quitar el disco duro del sistema analizado y instalarlo en otro para hacer la copia.
  - Instalar otro disco duro en el sistema analizado y hacer la copia.
  - Utilizar dispositivos autónomos especiales para hacer imágenes (DIBS Portable Evidence Recovery Unit, Rapid Action Imaging Device).
  - Utilizando una conexión de red para transferir los contenidos del disco a otro.
- Imagen del disco <> Copia de backup
- Consideraciones especiales a tener en cuenta:
  - Factores ambientales: temperatura, campos electromagnéticos.
  - Fecha y hora: Documentar la fecha y hora del sistema analizado antes de apagarlo (puede no ser la actual)

Recuperar Evidencia Digital I

- Hay casos en los que recuperar una evidencia digital puede parecer más difícil:
  - Ha sido borrada del sistema
  - Está cifrada
  - Está oculta
- Cómo recuperar archivos borrados?
  - El borrado normal de un archivo no lo elimina del disco duro!
  - Todo o la mayor parte del contenido del archivo persiste en el sistema y es posible recuperarla con las herramientas adecuadas:
    - Fast File Recover (http://www.savemyfiles.com/fastfile.htm)
    - The Coroner's Toolkit (http://www.porcupine.org/forensics/tct.html)
- Cómo recuperar información cifrada?
  - No siempre es posible. Depende del tipo de cifrado y la clave utilizada.
  - Ataques por fuerza bruta, por diccionarios, etc.

Recuperar Evidencia Digital II

- Donde buscar la información oculta? A nivel básico podríamos buscar:
  - Ficheros ocultos.
  - Papelera de reciclaje.
  - Alternate DataStreams en sistemas de ficheros NTFS (Windos NT, 2000).

- Donde buscar más información:
  - El histórico de URLs visitadas de los navegadores.
  - En las cache que se guarda de las páginas web visitadas.
  - Ficheros temporales creados por las propias aplicaciones (word, etc.)
  - Páginas de swap utilizadas por los Sistemas Operativos.

Índice

- Correos Anónimos
- Investigación post-intrusión

Correos Anónimos I

- El envío:

220 llca201.servidoresdns.net ESMTP Sendmail 8.11.6/8.10.2; Fri, 1 Jul 2003 10:03:48 +0200

EHLO ANONYMOUS

250-llca201.servidoresdns.net Hello docs41-167.menta.net [62.57.40.167], pleased to meet you

250-ENHANCEDSTATUSCODES

250-EXPN

.....

250 HELP

MAIL FROM: ANON@ANON.COM

250 2.1.0 ANON@ANON.COM... Sender ok

RCPT to: DFERNANDEZ@ISECAUDITORS.COM

250 2.1.5 DFERNANDEZ@ISECAUDITORS.COM... Recipient ok

DATA

354 Enter mail, end with "." on a line by itself

SUBJECT: MAIL ANONYMOUS

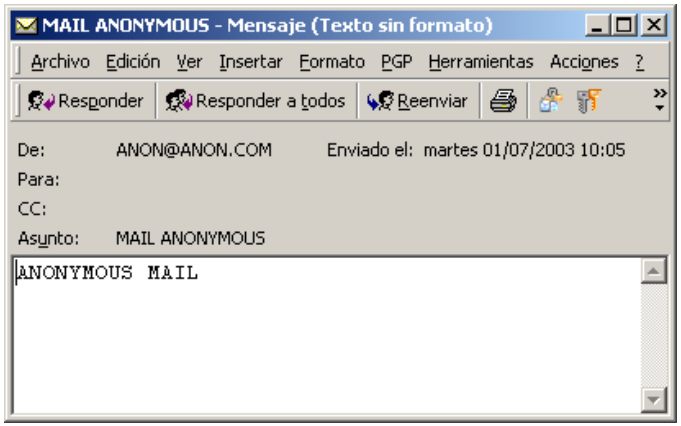
ANONYMOUS MAIL

.

250 2.0.0 h64841g09995 Message accepted for delivery

Correos Anónimos II

- El mail:



- La cabecera del mail:

Return-Path: <ANON@ANON.COM>

Received: from ANONYMOUS (----------)

by **llca201.servidoresdns.net** (8.11.6/8.10.2) with ESMTP id h64841g09995

for DFERNANDEZ@ISECAUDITORS.COM; Fri, 1 Jul 2003 10:04:31 +0200

Date: Fri, 1 Jul 2003 10:04:31 +0200

From: ANON@ANON.COM

Message-Id: <200307040804.h64841g09995@**llca201.servidoresdns.net**>

SUBJECT: MAIL ANONYMOUS

Status:

Correos Anónimos III

- Investigando el origen:
  - Sepamos a quien corresponde este servidor de correo:

```
[d:\]ping llca201.servidoresdns.net

Haciendo ping a llca201.servidoresdns.net [217.76.128.102]
con 32 bytes de datos:
```

  - Ahora obtengamos datos para ponernos en contacto:

http://www.ripe.net/perl/whois?form_type=simple&full_query_string=&searchtext=217.76.128.102&do_search=Search

  - Según la LSSICE los ISP están obligados a almacenar registros de uso de sus servidores.
  - A partir de los registros del ISP podremos obtener la IP de origen de la conexión.

http://www.ripe.net/perl/whois?form_type=simple&full_query_string=&searchtext=62.57.40.167&do_search=Search

  - Ahora deberemos pedir al ISP que proveé la conexión nos facilite el titular de dicha cuenta.

Investigación post-intrusión I

El Caso Ideal:

- Identificación: ¿Nuestro sistema ha sido realmente comprometido? Debemos revisar los logs de los Detectores de Intrusos, registros de acceso anómalos, etc.
- Preservación de la evidencia: Hay que congelar la escena del crimen sin dar pistas que se está haciendo.
    - Hay que intentar preservar archivos de memoria (archivos swap Windows, /proc en Unix, etc.).
    - Realizar una copia inmediata del disco duro.
- Construir una linea temporal de actuación:
    - Qué sucedió en el sistema antes de su compromiso.
    - Qué hizo el intruso durante el compromiso (cantidad de intrusos, acciones, etc.)
    - Porqué salió del sistema.
- Análisis de toda la información:
    - Las intrusiones crean alteraciones en los sistemas, cuanta más operaciones realizan los intrusos más ruido crean en estos y cuantas más huellas quieren borrar, más huellas dejan.

Investigación post-intrusión II

El Caso Real: servidores en producción de una empresa de servicios on-line 24x7.

- El rendimiento de la red de servidores había descendido un 80%.
- 4 horas para descubrirse si la máquina había sido o estaba siendo comprometida.
- Descubrir los puntos de entrada al sistema y cerrarlos.
- Analizar cuáles habían sido las acciones que se habían producido en su interior
- Intentar averiguar quién había sido en intruso, o el origen de la intrusión.
- Restituir el servicio en la máquina.

Contras:

- No se dispone de herramientas de análisis forense.
- No se dispone de acceso físico al sistema.
- Únicamente se cuenta con el software básico de una máquina Linux y las herramientas propias del servidor Windows, supuestamente comprometido.

Puertas de entrada

Port scanning

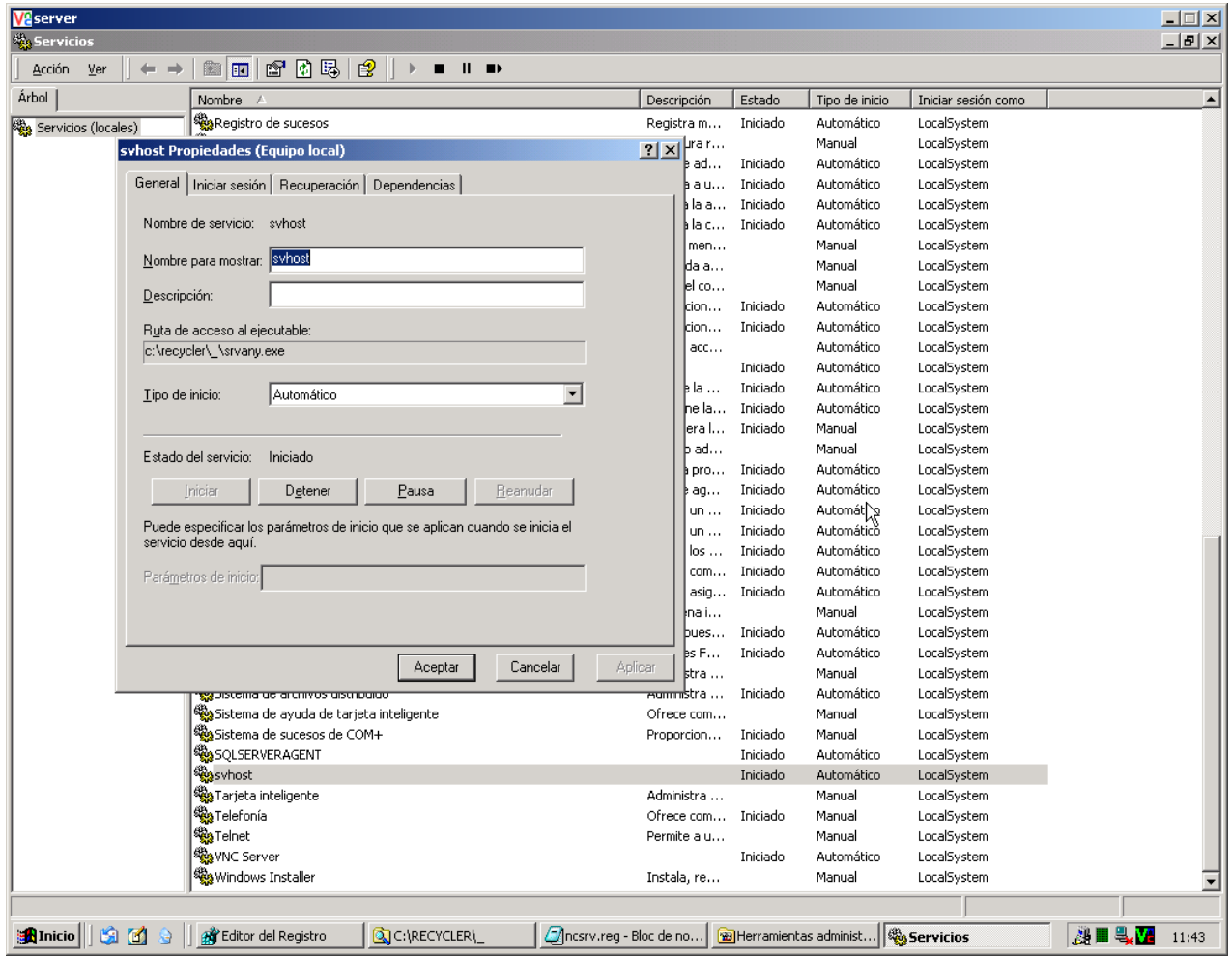
Estado de los puertos				
Puerto	Protocolo	Estado	Servicio	Comentarios
20	TCP	Cerrado	FTP-Data	
21	TCP	Abierto	FTP	Servidor de FTP
80	TCP	Abierto	http	Servidor web
1025	TCP	Abierto	NFS o IIS	
1026	TCP	Abierto	LSA o nterm	
1032	TCP	Abierto	Iad3	
1042	TCP	Abierto		Win Server lo utiliza para administrar sus recursos.
1043	TCP	Abierto		
1045	TCP	Abierto		
1046	TCP	Abierto		
1047	TCP	Abierto		
1402	TCP	Abierto	Prm-sm-nc	
1433	TCP	Abierto	Ms-sql-s	Servidor de SQL
3372	TCP	Abierto	Msdtc	
3389	TCP	Abierto	Ms-term-serv	Servidor de Terminales
5631	TCP	Abierto	Pcanywheredata	PCAnyWhere
5800	TCP	Abierto	VNC-http	Acceso VNC
5900	TCP	Abierto	VNC	Acceso VNC
15876	TCP	Abierto	Desconocido	
54321	TCP	Abierto	Desconocido	

Referencias a alguno de los servidores en listas de Internet:

Inclusión en listas publicas o *underground* de máquinas	
Gusano Sapphire	http://www.netsys.com/library/sapphire-hosts.txt

Servicios anómalos

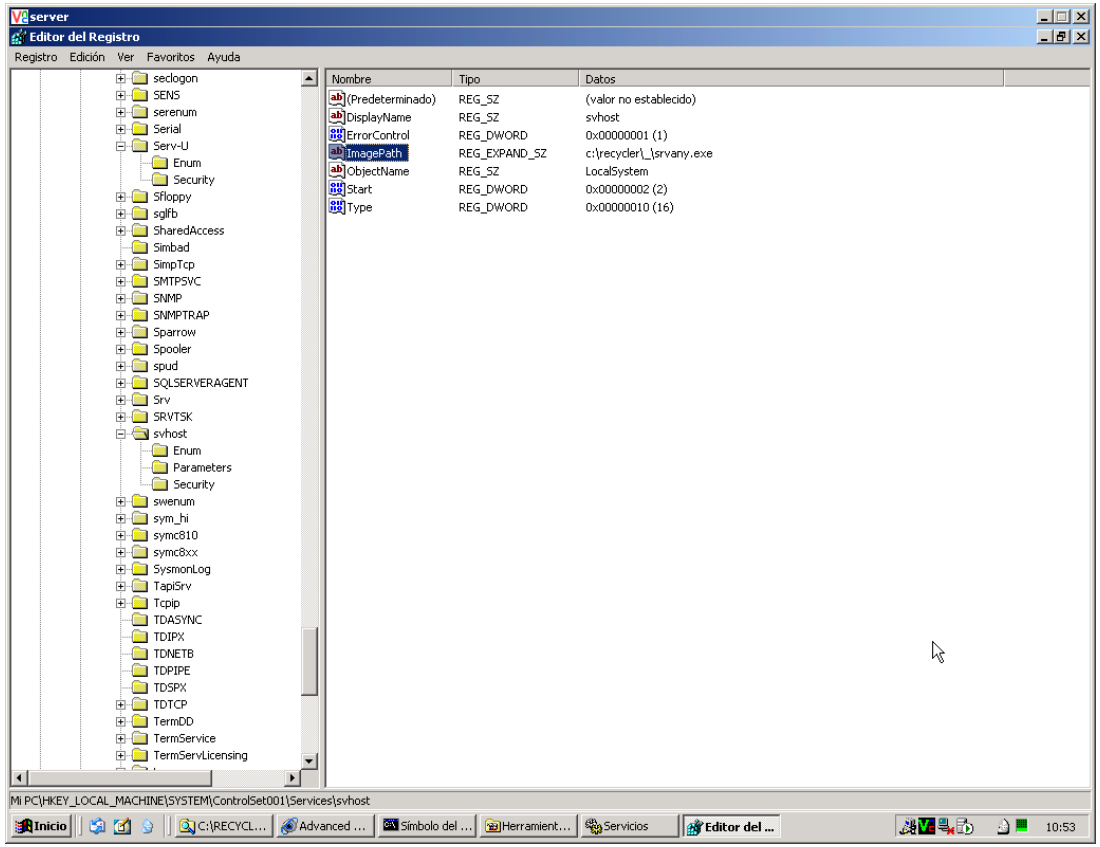
- Hay servicios no habituales en ejecución.
- Los puertos no estándar que están ofreciendo servicios se deshabilitan parándolos.



Entradas en el registro

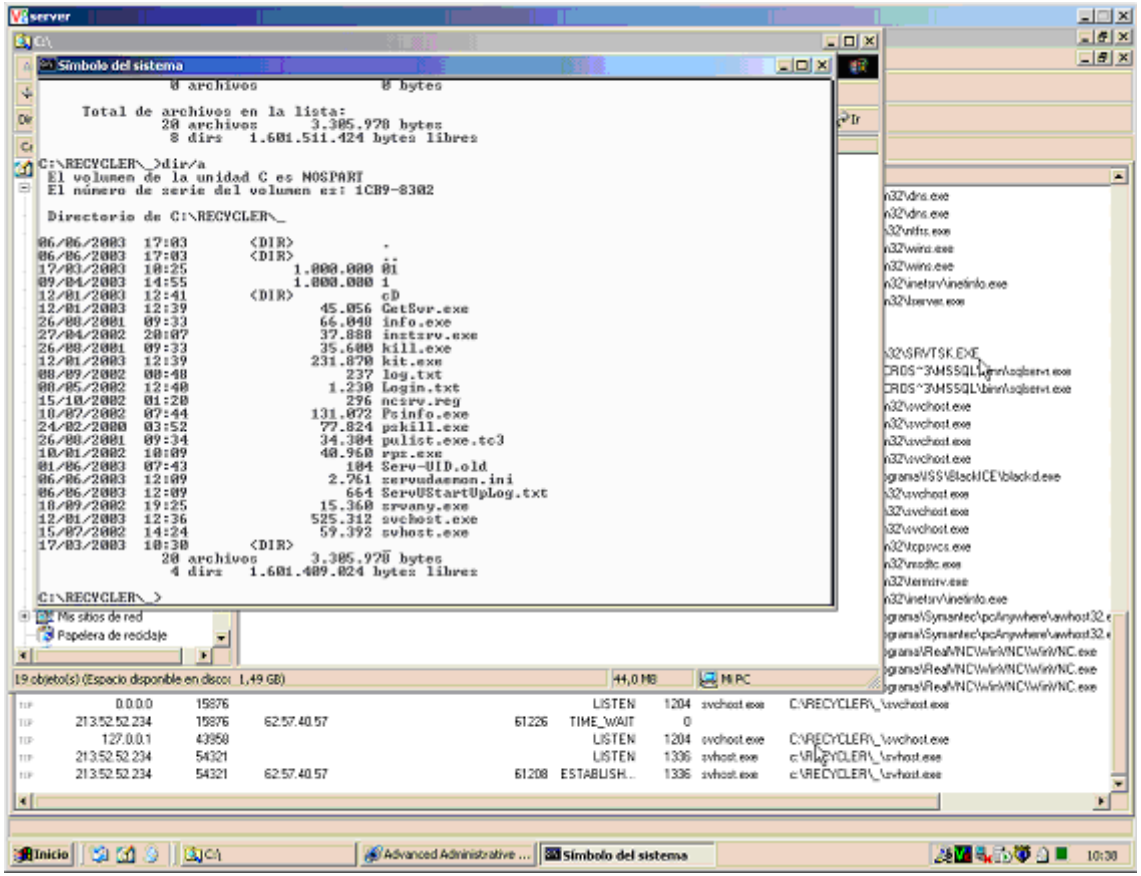
• El registro de Windows mantiene información sobre los servicios que se arrancan al encender el ordenador, donde están estos programas, etc.

• Se localizan las entradas en el registro que arrancan estos servicios y se localizan los ejecutables en el disco duro.



Localización de los troyanos

- Se ha troyanizado alguno de los servidores, se han instalado FTPs y se emplean para el intercambio de software, películas, música pirata y como foro de hackers.
- La red había sufrido una caida debido al flujo de datos que implicaba esto.



Limpieza y restitución

• La máquina se había preparado de forma que parecía que intentaba borrar sus huellas si la conexión al exterior se perdía.

• Había que localizar las herramientas instaladas y ocultadas en el sistema con tal de proteger las Bases de Datos, ya que se todavía no se conocía completamente que operaciones realizaban estos troyanos.

• Eliminados éstos, se revisa el sistema, con el objeto de salvaguardar la mayor cantidad de información sobre el origen de la intrusión.

• La intrusión no fue realizada desde un único punto. Los resultados fueron que los servidores en concreto no eran el objetivo, sino las capacidades de la infraestructura para sus fines y la intrusión era cuanto menos, desordenada y sin coordinación.

• No se habían realizado accesos a las Bases de Datos y las alteraciones en los directorios del sistema habían sido mínimas, con el fin de no levantar sospechas

• La intrusión se había producido gracias a un indebido mantenimiento de las máquinas durante unas semanas, hecho que facilito la entrada a los sistemas aprovechando una vulnerabilidad publicada.

• La red y los servidores estuvieron funcionando al 100% en 3 horas y 15 minutos.

• Este tipo de intrusión más común en Internet.

CURSO DE PRÁCTICA OPERATIVA EN INVESTIGACIÓN

MÓDULO 5

INTERNET, DOCUMENTACIÓN Y BASES DE DATOS

HERRAMIENTAS DE INVESTIGACIÓN

Y

SEGURIDAD EN INTERNET

Muchas gracias su vuestra atención

Daniel Fernández
dfernandez@isecauditors.com

Xavier Carbonell
xcarbonell@isecauditors.com

4 de Julio de 2003