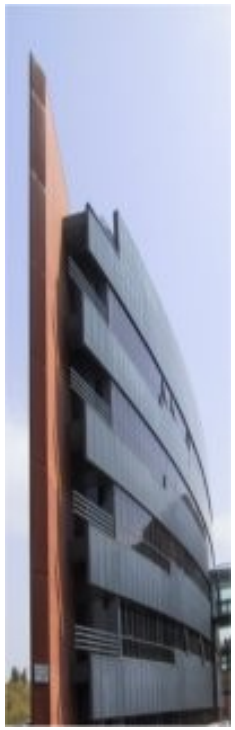
II Reto de Análisis Forense Hispano

http://www.seguridad.unam.mx/eventos/reto

Víctor Barahona
Tecnologías de la Información
Universidad Autónoma de Madrid

Jornadas de Análisis Forense 2005, Madrid

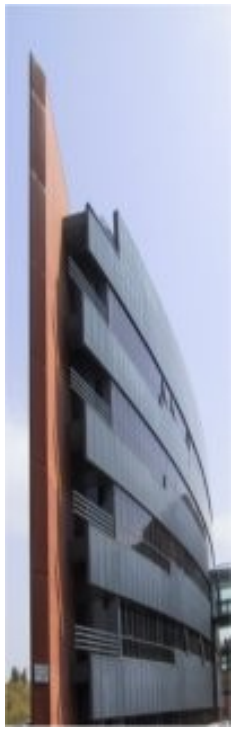


Antecedentes

2001 - Honeynet (Forensic Challenge).

2003 - I Reto Forense Hispano.

2005 - II Reto Forense Hispano.



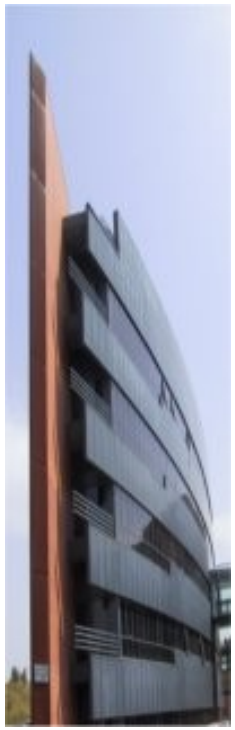
Equipo y Motivaciones

Tres investigadores:

- José Ignacio Parra.
- Enrique López.
- Víctor Barahona.

Motivaciones:

- Aprender.
- Divertirnos.



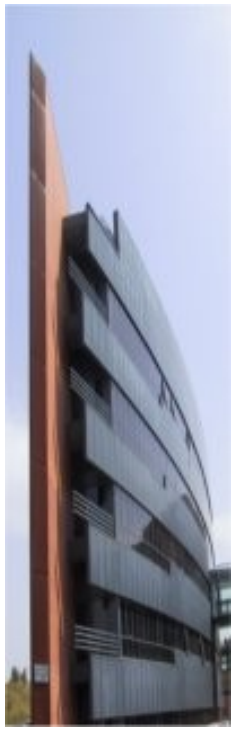
II Reto Forense

Se proporciona:

- 5 imágenes de disco comprimidas.

Se pregunta:

- ¿El sistema ha sido comprometido?
- ¿Desde donde se realizó el ataque?
- ¿Cómo se realizó el ataque?
- ¿Qué hizo el atacante?



Problemas a priori

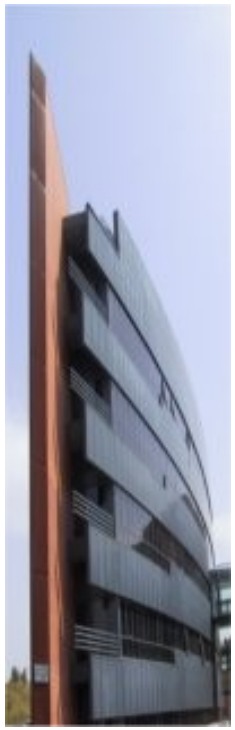
1000 participantes + 6Gb = 4 días para descargar.

Primera descarga corrupta.

Para hacer este análisis se necesitan unos 40Gb de espacio.

Se necesita un equipo potente.

Discos rápidos.



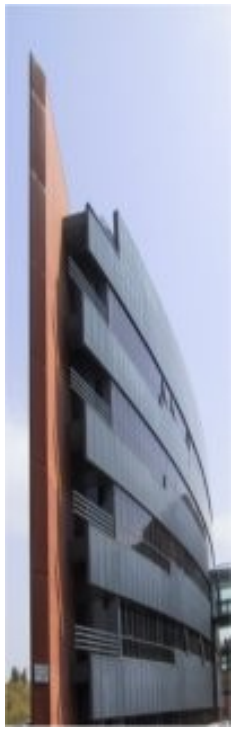
Pasos para hacer el análisis

Preparar el entorno forense.

Análisis Forense.

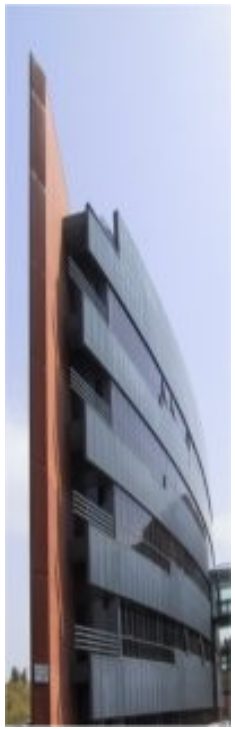
Análisis de herramientas.

Conclusiones.



Preparación del entorno forense

2 Equipos con Linux (RedHat y Debian).
Disco Externo USB (80 Gb).
VMware (RedHat EL y 7.3).
Sleuthkit-1.73.
Autopsy-2.03.
RKhunter.
Herramientas del sistema.
Google y Virustotal.



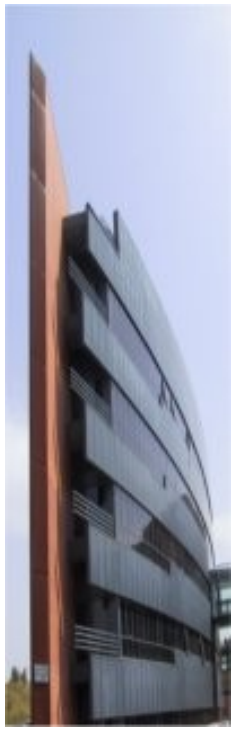
Recogida de datos previa

Almacenamos:

- Timeline (mactime).
- Espacio no asignado.
- Strings.

Lo hacemos por duplicado:

- Sleuthkit (CLI): fls, ils, mactime, dls, sstrings, etc.
- Autopsy (GUI).



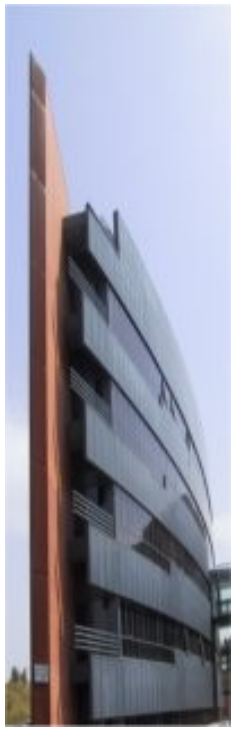
Busqueda de rootkits

Han borrado los logs.

Verificamos con rpm que hay 75 binarios modificados. ¿rootkit?

Corremos rkhunter:

- Suckit. (/proc/kmem)
- SHV4. (tradicional)



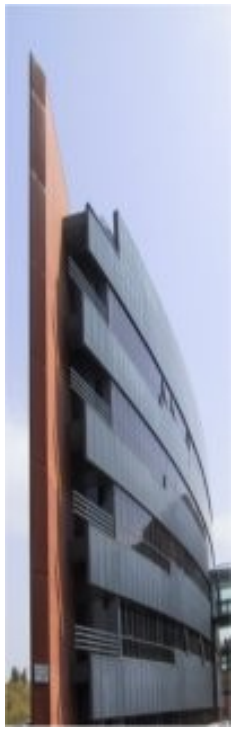
Rootkits

Suckit:

- Se carga en memoria del kernel.
- Crea una puerta trasera inversa.
- Parcialmente instalado.

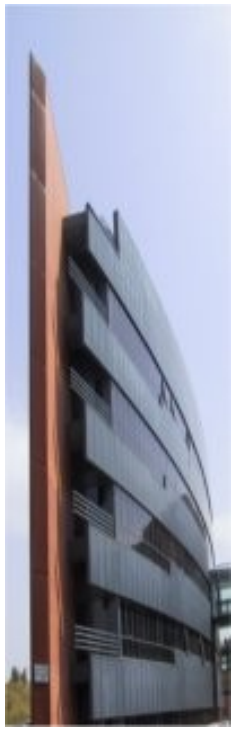
SHV4

- Sustituye binarios del sistema.
- Crea una puerta trasera.
- Troyaniza el servidor ssh.
- Instala un sniffer.
- Parcialmente instalado.



Virus... ¿en Linux?: Linux/RST.b

- /dev/hdx1 y /dev/hdx2
- Forman parte de la instalación del virus Linux/RST.b.
- Infecta 30 binarios del directorio actual y del directorio /bin.
- Introduce una sofisticada herramienta usando EGP.
- Cadena “snortdos” y “tory”.



Segundo virus: Linux/OSF.a

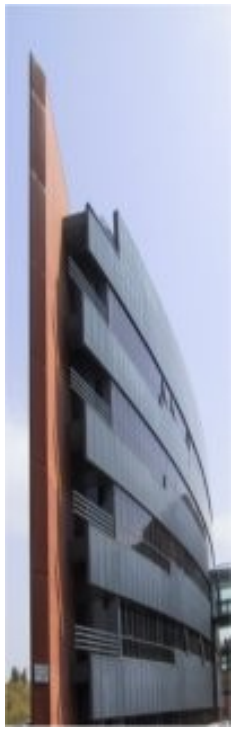
Pasamos un antivirus (fprot) a /bin.

51 de 85 infectados con Linux/OSF.a

Nunca infecta ps.

Escucha en el puerto 3049/udp ordenes:

- Ejecutar un comando.
- Correr un sniffer.
- Redirigir el trafico a otra maquina.



Pero ¿cómo ha entrado?

Usuario apache.

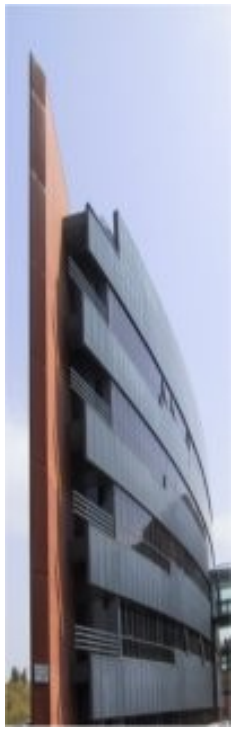
Selena: autorooter apache+ssl.

Lo lanzamos con éxito contra la maquina gemela (VMware + Redhat7.3).

Buscamos el log y lo comparamos con las cadenas no asignadas de hd3 (/var).

```
#grep –i "SSL handshake failed" /reto2/hda3.dd.unalloc.asc

[Sat Jan 29 14:58:51 2005] [error] mod_ssl: SSL handshake failed (server
127.0.0.1:443, client 64.202.43.190) (OpenSSL library error follows)
```



Escalada de privilegios de apache a root

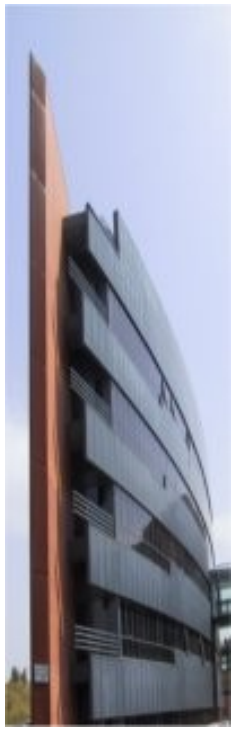
Se descarga algo por ftp.

Se produce la infección del virus RST.b.

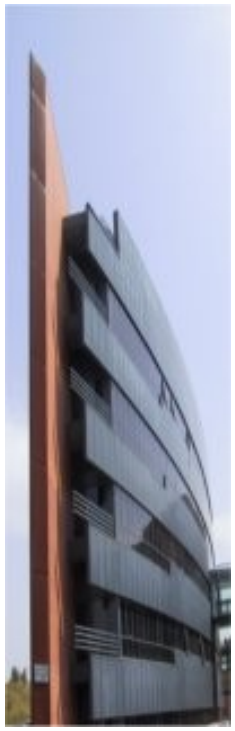
Por lo tanto el exploit que usa esta infectado con el virus.

Exploit local del kernel.

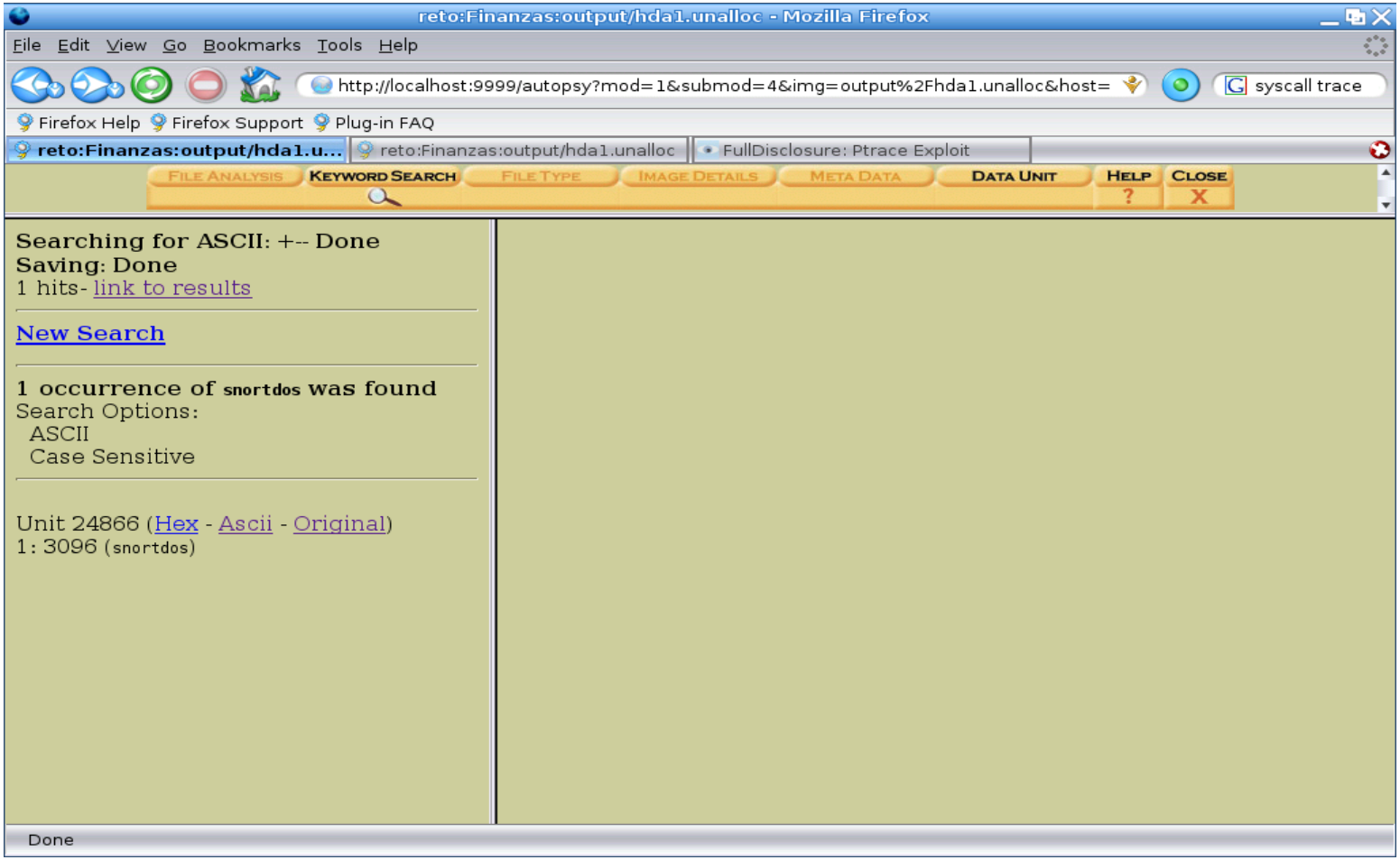
http://www.securityfocus.com/bid/7112

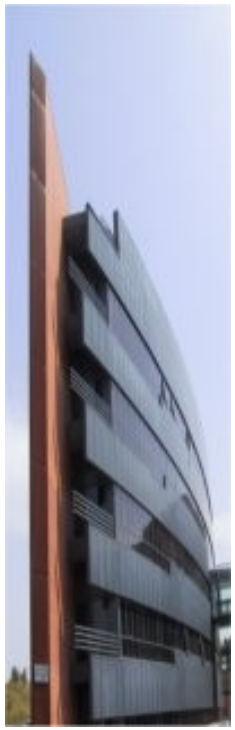


Recuperación del exploit borrado I



Recuperación del exploit borrado II





Recuperación del exploit borrado III

reto:Finanzas:output/hda1.unalloc - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://localhost:9999/autopsy?mod=1&submod=5&case=reto&host=Finanzas&inv=sr_

syscall trace

Firefox Help Firefox Support Plug-in FAQ

reto:Finanzas:output/hda1.unalloc | reto:Finanzas:output/hda1.u... | FullDisclosure: Ptrace Exploit

FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP | CLOSE

Unit Number: 24865

Number of Units: 6

Unit Size: 4096

Lazarus Addr:

VIEW

LOAD ORIGINAL

PREVIOUS NEXT

EXPORT CONTENTS ADD NOTE

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)

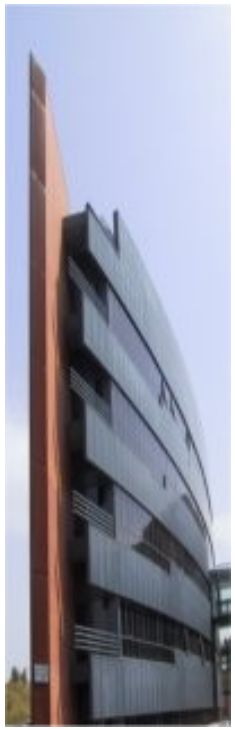
File Type: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), stripped

Units: 24865-24870

View Original

```
GLIBC_2.0
PTRh
j(h
/proc/self/exe
[-] Unable to read /proc/self/exe
[-] Unable to write shellcode
[+] Signal caught
[-] Unable to read registers
[+] Shellcode placed at 0x%08lx
[+] Now wait for suid shell...
[-] Unable to detach from victim
[-] Fatal error
[-] Unable to attach
[+] Attached to %d
[-] Unable to setup syscall trace
[+] Waiting for signal
[-] Unable to stat myself
root
/bin/sh
[-] Unable to spawn shell
[-] Unable to fork
SQRWW
_^ZY[
SQR1
SQRV
H^ZY[
SQRWW
_^ZY[
_^ZY[
QSP1
```

Done



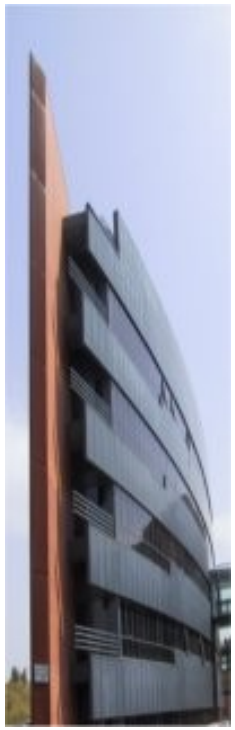
Actividades del atacante I

Crea el usuario weed con privilegios de root (hasta tres veces).

Se descarga y trata de instalar dos veces el rootkit SHV4.

Se descarga y trata de instalar el rootkit suckit.

Descarga y ejecuta una puerta trasera hecha en perl (https)



Actividades del atacante II

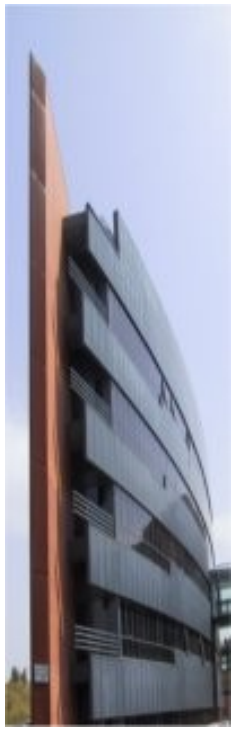
Se conecta con el usuario weed.

Se descarga otro backdoor (pico).

Le cambia el nombre “ “ y lo ejecuta.

Envia información sobre la maquina a radautiteam@yahoo.com

Mata zbind (4000/tcp) antes de desconectar.



Actividades del atacante III

Autorooter samba: woot.tgz.

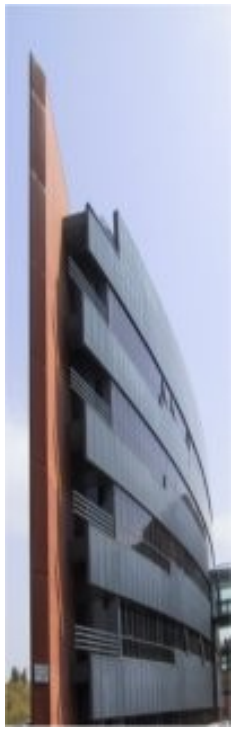
Ataca la clase B de Brasil 200.207.0.0/16

Se produce la infección de OSF.a.

Bouncer IRC: psybnc.

Realiza dos instalaciones, pero borra la primera.

Renombra psybnc por “ps xa”.



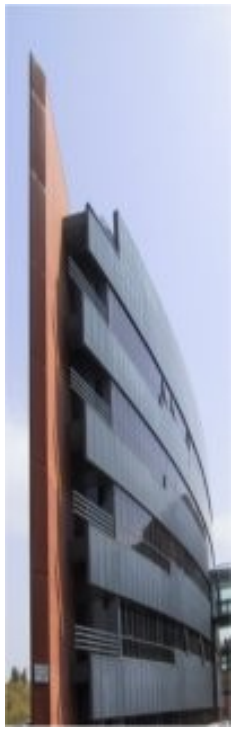
Actividades del atacante IV

Autorooter apache+ssl: selena.tgz

Ataca la clase B 217.172.0.0/16

Lanza el exploit a 422 hosts!!!

A las 15:38:57 del 31 de Enero la maquina es apagada (hard-reset).



Respuestas al reto I

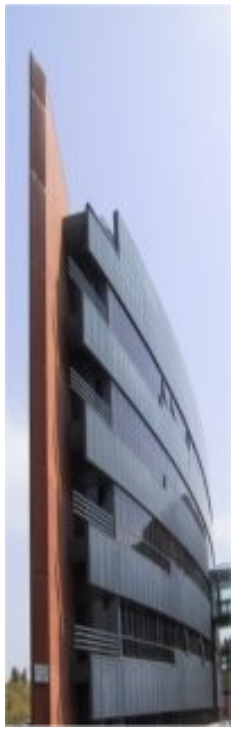
El sistema fue vulnerado.

La instrusión se produce a las 14:58:51 del 29 de Enero (GMT-6).

El ataque viene desde la IP 64.2002.43.190 (Reno, Nevada, USA).

Atacantes rumanos (Radauti, Rumania).

Nivel técnico de los atacantes bajo (script-kiddies).

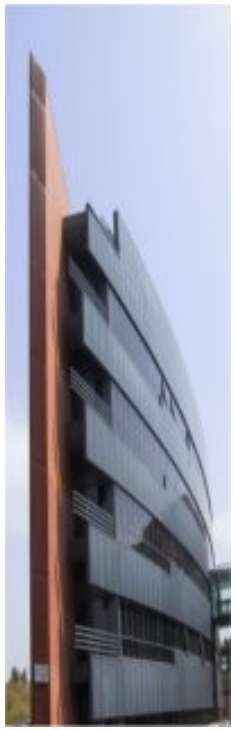


Respuestas al reto II

Servicio atacado: apache+ssl.

Elevación de privilegios: vulnerabilidad del kernel.

Instalación de rootkits, backdoors, ircbot y autorooters.



Conclusiones

Actualizaciones.

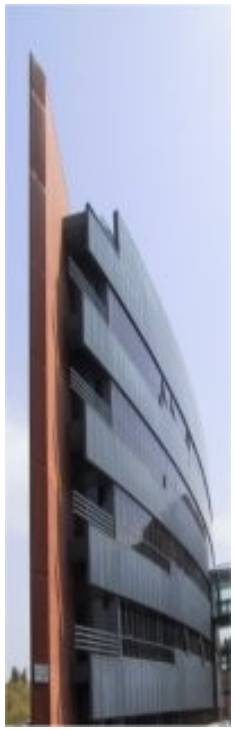
Bastionización.

Integridad de ficheros.

NIDS.

Antivirus y anti-troyanos.

Política de backups.



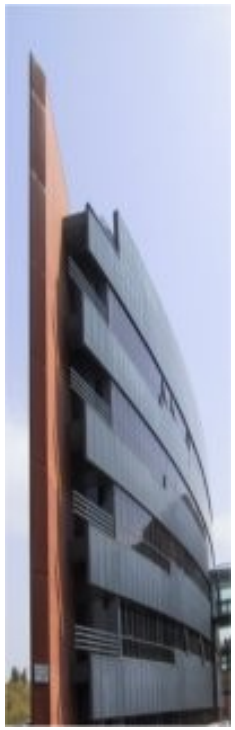
Informes del reto

Infome Ejecutivo (5 pag.):

http://www.seguridad.unam.mx/eventos/reto/uno_ejecutivo.pdf

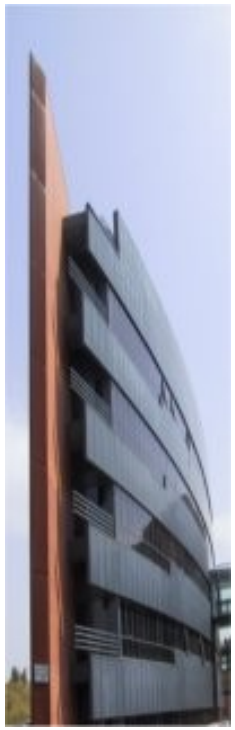
Informe Técnico (43 pag.):

http://www.seguridad.unam.mx/eventos/reto/uno_tecnico.pdf



Enlaces de interes

VMware. http://www.vmware.com
VirusTotal: http://www.virustotal.com
Sleuth Kit y Autopsy http://www.sleuthkit.org
Rkhunter: http://www.rootkit.nl/
Suckit Rootkit http://www.phrack.org/phrack/58/p58-0x07
SHV4 Rootkit
https://tms.symantec.com/members/AnalystReports/030929-Analysis-SH
Linux/RST.b http://www.security-focus.com/archive/100/247640
Linux/OSF.a: http://www.viruslibrary.com/virusinfo/Linux.OSF.8759.htm
selena.tgz: http://www.lurhq.com/atd.html
Exploit openssl-too-open:
http://www.phreedom.org/solar/exploits/apache-openssl/
CA-2002-23: http://www.cert.org/advisories/CA-2002-23.html
Vul. del kernel 2.2 y 2.4: http://www.kb.cert.org/vuls/id/628849
PsyBNC: http://www.psychoid.net/



MUCHAS GRACIAS

¿PREGUNTAS?