Análisis forense con autopsy

INDICE

Evidencias

- dd if=/dev/hda? of=imagen-hda?.dd
- nohup wget –r –c ftp://ftp.ftp.es/imagen.tar.bz2 &
- Descomprimir y ver las particiones.

Verificación de evidencias

- md5sum *.dd: comprobamos el compendio de cada imagen.
- file *: vemos el sistema de ficheros de cada partición.
  - Linux ext2
  - data (swap)
- Comprobamos la zona horaria del sistema y la versión del mismo, para ello montamos la partición la partición que contiene /etc.
  - mount –o ro,loop 192.168.3.10-hda8.dd hda8/
  - root@miami:/hda8# more etc/redhat-release
    Red Hat Linux release 7.1 (Seawolf)
  - root@miami:/hda8# more /etc/sysconfig/clock
    ZONE="Europe/Madrid"
    UTC=false
    ARC=false
- En autopsy indicamos zona horaria (timezone) ‘MET’.

Preparación del caso

- Crear caso en autopsy.
- Se añade un host: 192.168.3.10
- Se añaden las imágenes

- En /etc observamos una serie de ficheros (eliminados) sospechosos:
  - ***/etc/***

Fichero	Fecha "Modificación“	Fecha "Acceso"	Fecha "Cambio"
group.lock	00:56:39 2002.08.23	00:56:39 2002.08.23	00:56:39 2002.08.23
gshadow+	00:56:39 2002.08.23	00:56:39 2002.08.23	00:56:39 2002.08.23
gshadow.lock	00:56:39 2002.08.23	00:56:39 2002.08.23	00:56:39 2002.08.23
passwd.lock	00:56:39 2002.08.23	00:56:39 2002.08.23	00:56:39 2002.08.23
shadow.lock	00:56:39 2002.08.23	00:56:39 2002.08.23	00:56:39 2002.08.23

Examen inicial de los ficheros sospechosos

- Ordenamos los ficheros de /etc por fecha para buscar aquellos que estén aproximados en el tiempo a la fecha 23/08/2002 00:56:39
- Los ficheros relacionados con usuarios y contraseñas coinciden en la fecha. Es altamente improbable una persona modifique todos los ficheros en el mismo instante de tiempo:
  - A) Se ha utilizado un script
  - B) Se ha SYN la fecha y hora en todos los ficheros para que tengan la misma hora (touch).
  - C) Se ha utilizado alguna herramienta del sistema para editar usuarios y contraseñas.

Examen inicial de los ficheros sospechosos

- Se mira el contenido de los ficheros de usuarios y contraseñas en uso (passwd, shadow, gshadow, group..)
  - /etc/passwd : /bin/bash $\subset$ pepelu, ssh, nerod

$$id = 0 \wedge gid = 0$$

- El usuario ssh no tiene password y no aparece en group gshadow.
  - ssh::11895:0:99999:7:::
- Buscamos en el directorio /home para verificar fechas de creación y contenidos de directorios.
  - nerod i-nodo ∞
  - nerod MAC $\approx$ fecha ficheros /etc (00:27:09 2002.08.23)

Búsqueda por palabra clave ‘nerod’

Partición: hda8 (/)

Texto localizado	Fichero	Comentario
NICK=NeRoD	/root/.,/psybnc/psybnc.conf	Este fichero aparenta ser algún tipo de configuración de irc. observamos que PSYBNC es un proxy de IRC (un "BNC").
NICK=NeRoD	/root/.,/psybnc/psybnc.conf.old	Aparentemente un fichero de copia generado al editar el anterior.
:mesa.az.us.undernet.org 001 NeRoD` :Welcome to the Internet Relay Network NeRoD` :mesa.az.us.undernet.org 002 NeRoD` :Your host is mesa.az.us.undernet.org, running version u2.10.10.pl18.(release) :mesa.az.us.undernet.org 003 NeRoD` :This server was created Mon Apr 8 2002 at 14:49:47 MDT :mesa.az.us.undernet.org 004 NeRoD` mesa.az.us.undernet.org u2.10.10.pl18.(release) dioswkg biklmnopstv :mesa.az.us.undernet.org 005 NeRoD` SILENCE=15 WHOX WALLCHOPS USERIP CPRIVMSG CNOTICE MODES=6 MAXCHANNELS=25 MAXBANS=30 NICKLEN=9 TOPICLEN=160 KICKLEN=160 CHANTYPES=+#& :are supported by this server :mesa.az.us.undernet.org 005 NeRoD` PREFIX=(ov)@+ CHANMODES=b,k,l,imnpst CHARSET=rfc1459 NETWORK=Undernet :are supported by this server :mesa.az.us.undernet.org 251 NeRoD` :There are 37991 users and 51230 invisible on 36 servers :mesa.az.us.undernet.org 252 NeRoD` 76 :operator(s) online :mesa.az.us.undernet.org 253 NeRoD` 445 :unknown connection(s) :mesa.az.us.undernet.org 254 NeRoD` 39393 :channels formed :mesa.az.us	Este texto se encuentra dentro del bloque con número 231495 y tiene una longitud de 1024 bytes.	Es el mensaje (banner) de conexión a un servidor de irc (mesa.az.us.undernet.org).

Búsqueda por palabra clave ‘nerod’

.undernet.org 255 NeRoD` :I have 11131 clients and 1 servers :mesa.az.us.undernet.org 375 NeRoD` :- mesa.az.us.undernet.org Message of the Day - :mesa.az.us.undernet.org 372 NeRoD` :- 28/7/2002 13:17 :mesa.az.us.undernet.org 372 NeRoD` :- :mesa.az.us.undernet.org 372 NeRoD` :- _____ _____ :mesa.az.us.undernet.org 372 NeRoD` :- | ___|.---.-.-----.--.--.| | |.-----.--.--.--.-----. :mesa.az.us.undernet.org 372 NeRoD` :- | ___|| _ |__ --| | || || -__| | | |__ --| :mesa.az.us.undernet.org 372 NeRoD` :- |_____||___._|_____|___ ||__|____||_____|_____|_____| :mesa.az.us.undernet.org 372 NeRoD` :- irc2.easynews.com |_____| rocking phoenix, arizona, usa :mesa.az.us.undernet.org 372 NeRoD` :- www.easynews.com/irc :mesa.az.us.undernet.org 372 NeRoD` :- .. p o l i c i e s .. :mesa.az.us.undernet.org 372 NeRoD` :- .. - - - - :mesa.a	Continuación del anterior en el bloque 231496 (1024 bytes),	
z.us.undernet.org 372 NeRoD` :- .. no spamming, flooding, or related client-abuse. :mesa.az.us.undernet.org 372 NeRoD` :- .. no clones/virtual-clones permitted at any time. :mesa.az.us.undernet.org 372 NeRoD` :- .. no abusive robots, irc scripts, or bnc/proxys. :mesa.az.us.undernet.org 372 NeRoD` :- .. no additional opers needed; i.e. don't even ask. :mesa.az.us.undernet.org 372 NeRoD` :- .. no additional i-lines. (regular or spoof'd) :mesa.az.us.undernet.org 372 NeRoD` :- .. no abused (open) wingate/proxy server-clients allowed. :mesa.az.us.undernet.org 372 NeRoD` :- .. :mesa.az.us.undernet.org 372 NeRoD` :- .. connections limited to three(3) per user@ip/ip.block. :mesa.az.us.undernet.org 372 NeRoD` :- .. your client must respond to ident[RFC1413] connections. :mesa.az.us.undernet.org 372 NeRoD` :- .. your client must respond to normal ctcp requests. :mesa.az.us.undernet.org 372 NeRoD` :-	Bloque 231497 y 1024 bytes.	

Búsqueda por palabra clave ‘nerod’

.. we reserve the right to sever a connection at our will. :mesa.az.us.undernet.org 372 NeRoD` :- .. we hold the right to dis-allow specific channels/nicknames. :mesa.az.us.undernet.org 372 NeRoD` :- .. abuse related items may be reported to our opers :mesa.az.us.undernet.org 372 NeRoD` :- .. :mesa.az.us.undernet.org 372 NeRoD` :- .. irc is a wonderful privilege, not a right. you won't ruin it. :mesa.az.us.undernet.org 372 NeRoD` :- .. those who abuse our policies will see damnation. ie: DIE! :mesa.az.us.undernet.org 372 NeRoD` :- .. e - m a i l : irc@irc2.easynews.com :mesa.az.us.undernet.org 372 NeRoD` :- :mesa.az.us.undernet.org 372 NeRoD` :- ___ ___ ___ ___ ___ ___ ___ ___ _ _ / o ___ ___ :mesa.az.us.undernet.org 372 NeRoD` :- |___)| )|___ \ )| )|___)| )|___ | | ) | | ) / | | )| :mesa.az.us.undernet.org 372 NeRoD` :- |__ |__/| __/ _/ | / |__ |/\/ __/ |__ |__/	Bloque 231498 y 1024 bytes.	
| / / | | |__ :mesa.az.us.undernet.org 372 NeRoD` :- / o :mesa.az.us.undernet.org 372 NeRoD` :- :mesa.az.us.undernet.org 372 NeRoD` :- GET EASYNEWS USENET ACCESS FOR... :mesa.az.us.undernet.org 372 NeRoD` :- O N L Y $ 9 . 9 8 (US) P E R M O N T H ! :mesa.az.us.undernet.org 372 NeRoD` :- :mesa.az.us.undernet.org 372 NeRoD` :- If you enjoy our services on IRC, just imagine how great our News :mesa.az.us.undernet.org 372 NeRoD` :- services are!!! Sign up now to gain access to the Internet Usenet! :mesa.az.us.undernet.org 372 NeRoD` :- :mesa.az.us.undernet.org 376 NeRoD` :End of /MOTD command.	Continuación (y finalización del bloque del MOTD de Irc) en el bloque 231499.	

Búsqueda por palabra clave ‘nerod’

(extraemos más o menos el mismo texto completo de los bloques anteriores).	/root/.,/psybnc/motd/USER1.MOTD .old	El mensaje de MOTD volcado a fichero.
Id.Id	/root/.,/psybnc/motd/USER2.MOTD	

Partición: hda1 (/boot)

Texto localizado	Fichero	Comentario
No se ha encontrado ninguna cadena de texto igual a "nerod".		

Búsqueda por palabra clave ‘nerod’

Partición: hda6 (/home)		
Texto localizado	**Fichero**	**Comentario**
nerod	/home/nerod/	El directorio del usuario "nerod"

Partición: hda5 (/usr)		
Texto localizado	**Fichero**	**Comentario**
Nerodno	/usr/share/emacs/20.7/etc/TUTORIAL.sl	Pensamos que no tiene nada que ver con nuestro análisis, ya que el contenido de este fichero está en un idioma distinto y la palabra "Nerodno" aparece como palabra completa.

Búsqueda por palabra clave ‘nerod’

Partición: hda7 (/var)		
rm -rf nerod	/var/ftp/nerod/install	Dentro del directorio ftp aparece este fichero "install" que al examinar su contenido nos recuerda al fichero de instalación de un rootkit bastante conocido:
/var/ftp/nerod.tar.gz	/var/ftp/nerod.tar.gz	Puede ser el fichero comprimido de un rootkit (lo examinaremos más adelante).
nerod	/var/lib/slocate/slocate.db.tmp (borrado) /var/lib/slocate/slocate.db	¿La base de datos de locate?
---------- Network info: Hostname : localhost.localdomain (192.168.3.10) Alternative IP : 127.0.0.1 Host : localhost.localdomain Distro: Red Hat Linux release 7.1 (Seawolf) Uname -a Linux localhost.localdomain 2.4.2-2 #1 Sun Apr 8 19:37:14 EDT 2001 i586 unknown Uptime 12:25am up 1 day, 5:24, 0 users, load average: 0.60, 0.16, 0.05 Pwd /var/ftp/nerod ID uid=0(root) gid=0(root) groups=50(ftp) ---------- Yahoo.com ping: PING 216.115.108.243 (216.115.108.243) from 192.168.3.10 : 56(84) bytes of data. --- 216.115.108.243 ping statistics --- 6 packets transmitted, 0 packets received, 100% packet loss ---------- Hw info: CPU Speed: 166.196MHz CPU Vendor: vendor_id : GenuineIntel CPU Model: model name : Pentium 75 - 200 RAM: 48 Mb HDD(s): Filesystem Type Size Used Avail Use% Mounted on /dev/hda8 ext2 251M 52M 185M 22% / /dev/hd	/var/spool/mqueue/dfg7MMQ5J 07358	¿un mensaje de correo electrónico enviado al presunto atacante con todos los detalles de la máquina "conquistada"? Examinos este fichero desde autopsy (es un fichero eliminado) y observamos más detalles en ficheros dentro del directorio /var/spool/mqeueu). La dirección a la que se ha enviado el correo es: frumosu99us@yahoo.com

Búsqueda por palabra clave ‘nerod’

Partición: hda9 (swap) **Texto localizado**	**Fichero**	**Comentario**
..<38>Aug 23 00:27:09 adduser[7397]: new group: name=nerod, gid=501	swap	Probablemente la línea del fichero /var/log/messages correspondiente a la orden "adduser" que el presunto atacante inició. Confirmamos además la fecha y hora del incidente, a partir del "timestamp" de la entrada en el fichero de "/var/log/messages".
i586 /usr/local/sbin/sshd.-q.-p.4.-f./etc/ssh/sshd_config PWD=/var/ftp/nerod.HOSTNAME=localhost.localdomain MACHTYPE=i386-redhat-linux-gnu LANG=es_ES@euro.SHLVL=3 SHELL=/bin/bash.HOSTTYPE=i386.OSTYPE=linux-gnu.TERM=dumb.PATH=/usr/local/sbin._= /usr/local/sbin/sshd./usr/local/sbin/sshd	swap	Esta cadena de texto puede corresponder a un inicio de un servidor de ssh, que si leemos con atención observaremos que escucha en el puerto "4" y con la opción "-q" para desactivar el "log".
#bag.pula.in.mata.cu.whoisu.tau.cu.tot : NeRoD NeRoD`` NeRoD` NeRoD``` pdbne @NastyBoy @MASTER-ON @Morcovel @_Ke0Ps_ @ALCATEL @RosKata @Alexel_Aw @BauBauuu @alina99 @diavolita @Cioroi @cocolino @Zmeu_De_I @sarlatanu @YahooBB @Pao_Pao @ela29 @Bau PONG :mesa.az.us.undernet.org	swap	¿usuarios de un canal de irc? El servidor es mesa.az.us.undernet.org y el canal #bag.pula.in.mata.cu.whoisu.tau.cu.tot.

Búsqueda por palabra clave ‘nerod’

Nerod, Alejandro, ~george, 192.168.3.10, numero, 216.206.140.242, zero_cool, ~ASALT, 202.153.36.9, destruct, ~destruct, sutton-fw.pipcom.com, BlackCola, ~second, 63.228.88.49, Ratzushka, ~third, 63.228.88.49, Di-Ang3lo, ~ Born2Love, 63.228.88.49, X, Bau, ~bau, ozuc02.ucsfmedicalcenter.org, ma1.glaystyle.net, Nykey, nykey, fuck.off.you.littlepervert.org, ela29, ~mumu, 213.142.160.120, KABAL_BDC, kaba, httpd.us, Pao_Pao, usen-43x233x195x212.ap-USEN.usen.ad.jp, yester, ~yester, dhcp024-208-132-152.insight.rr.com, YahooBB, YahooBB227016032.bbtec.net, |ReNzO|, ~renzo, 204.96.12.241, |Hera| ~Hera^, 211.219.153.2	swap	¿usuarios de un canal, con algunas de sus direcciones ip? ¿puede ser un grupo de atacantes organizado? Las direcciones ip que observamos, ¿pueden ser sus direcciones origen?
~George .192.168.3.10 A .#hackeri .ntl wget http://packetstorm.decepticons.org/removed/73501867 (http://www.network-tools.com/ use it alL !) USER1.USER.AWAYNICK=NeRoD - P .u!ad1 USER1.USER.LEAVEMSG= HL ! .USER1.USER.AWAY=-) DJ^SHEDY ~DjShedy 64.68.47.238 PuiDe[pl] ~kid arka-noego-hq.gdynia.ids.pl Aalessya ~alex .211.62.36.37 P .dani- ~best .148.247.38.3 P NeRoD`` .~george .192.168.3.10 Luchyan-- .~bogdan .61-220-34-93.HINET-IP.hinet.net B0SS}{ ~boss .219.163.100.90 TiamaT_ .~tiamat .210.248.126.194 D`Ang3lo ~Born2Love 209.217.51.15 .HD Ta|kab0uT .justme best.vhosts.de @ = [ReNzO] .~renzo p3EE25913.dip.t-dialin.net BlaBlaBla .~Dica .216.142.87.19 .0 .[Dj] ~shedy 213.219.111.86 PuiDe[pI] ~kid pa161.smochowice.sdi.tpnet.pl .MaN_EchiN .	swap	Estamos totalmente convencidos de que este es un canal de irc (#hackeri) donde el presunto atacante (o atacantes) conversan. Sabemos el servidor y conocemos el nombre del canal, lo que nos puede ayudar MUCHO en la caza y captura del presunto atacante.

Búsqueda por palabra clave ‘nerod’

~alex .211.62.36.78 8l ALCATEL .~alcat3l 61.221.7.59 @ .h .PuiDeSmeN .~kid 64.68.32.102 anonimus^ ~creator alhamilla.larural.es @ .p .ManiacU . root 61.200.9.162 P .Flubber .~gyurku .66.95.50.98 @ .0 .BoTSeX ~0wnz .pc2-lich1-5-cust157.bir.cable.ntl.com Mihai .~mihai ad66-20.magix.com.sg ^V^ooDoo ~VooDoo computerscience.wc.edu sHpIrE Shpiki 217.98.53.249 @ .X .cservice undernet.org @ L22|Gone leishman blackhole.energybox.co.uk p .MachoBoyS .~mafia 211.184.210.131 P .^Voo^Doo^ .~VooDoo .alhamilla.larural.es 0 .Murdoc ~back .202.105.49.8 @ .NeRoD .~George .192.168.3.10 NeRoD`` YabadaMAD .~adrian .213.154.99.10 .NeRoD``` ~George .	swap	A estas alturas y leyendo el formato de una conexión de irc, sospechamos que nuestro potencial atacante utiliza el alias de ~george.
h .alina99 .~mumu .213.142.160.120 NeRoD` ~george .ma1.glaystyle.net A DeZaXxAtU dezaxatu 22.california-27-18rs.ca.mil-gov.net NeRoD .~George .192.168.3.10 h NeRoD .~George .192.168.3.10 G NeRoD`` .~george 192.168.3.10 H NeRoD` ~george ma1.glaystyle.net H NeRoD``` ~George .ma1.glaystyle.net I pdbne .~mona .adexus.com.ec J Morcovel ~mumu .67.38.108.181 @ .@M @ ._Ke0Ps_ .~keos nimbus.anzio.com @ . N ALCATEL .~alcat3l 61.221.7.59 @ O RosKata .~mumu .213.142.160.120 .@ O Alexel_Aw .	swap	Observamos que NeRoD (~george) aparece con dos máquinas asociadas: 192.168.3.10 (la propuesta por el reto) y ma1.glaystyle.net. Esta última podría ser el punto de inicio de su ataque contra la del reto.

Búsqueda por palabra clave ‘nerod’

P0:NeRoD!George@80.96.68.71 NICK :NeRoD	swap	TENEMOS UNA IP REAL, asociada a su alias y con el nombre de usuario George. Más adelante utilizaremos esta información para contrastarla con la base de datos de WHOIS. El canal es #hackeri y el tema del canal es: http://packetstorm.decepticons.org/removed/73501867 Examinamos el fichero que propone ese enlace y es un ataque-exploit para PHP (ver fichero adjunto, "73501867") y ver detalles en: http://www.packetstormsecurity.nl/filedesc/73501867 Este fichero **TIENE UN VIRUS**, Linux.Jac.8759!!! Una versión más moderna se puede encontrar en: http://www.packetstormsecurity.nl/filedesc/7350fun Se puede encontrar una vacuna para este virus en: http://packetstormsecurity.nl/trojans/vaccine.c y hay detalles del virus en: http://securityresponse.symantec.com/avcenter/venc/data/linux.jac.8759.html
i586.xinetd.-stayalive.-reuse.pidfile ./var/run/xinetd.pid PWD=/var/ftp/nerod.LC_MESSAGES=en_US HOSTNAME=localhost.localdomain LC_TIME=en_US MACHTYPE=i386-redhat-linux-gnu LC_ALL=en_US.LANG=en_US LC_NUMERIC=en_US.SHLVL=3 SHELL=/bin/bash.HOSTTYPE=i386 OSTYPE=linux-gnu.TERM=dumb PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin LC_MONETARY=en_US LC_COLLATE=en_US._=sbin/initlog./usr/sbin/xinetd	swap	¿xinetd?

Resumen de la información obtenida

RESUMEN-GUIÓN:	
nerod	Alias de nuestro presunto atacante.
George	Nombre que aparentemente utiliza en el irc.
#hackeri, #bag.pula.in.mata.cu. whoisu.tau.cu.tot.	Canales en los que NeRoD está.
mesa.az.us.undernet.org	Servidor de irc al que se ha conectado.
ma1.glaystyle.net	Nombre de máquina relacionada con NeRoD en el irc.
80.96.68.71	Ip asociada a NeRoD en el irc.
psybnc	proyx de irc que aparentemente ha instalado en la máquina.
/root/.,/	Directorio sospechoso a investigar
/var/ftp/nerod	Directorio sospechoso a investigar.
xinetd	Investigar posible rootkit.
adduser	Revisar "adduser" a las 00:27:09 del 23 de Agosto.
sshd	Revisar servidor sshd en el puerto "4" en modo "silencioso", es decir, sin guardar "log".
"73501867" y "7350fun"	Exploits para php mencionados en el canal de irc en el que nuestro presunto atacante se encuenta; el primero tiene un virus (Linux.Jac.8759) ¿puede ser este el método utilizado para atacar la máquina del reto? Investigamos el fichero "/etc/httpd/conf/httpd.conf" y constatamos que este está configurado para soportar PHP (DirectoryIndex index.html index.htm index.shtml **index.php index.php4 index.php3** index.cgi) y localizamos el log en: CustomLog **/var/log/httpd/access_log** combined

Whois de la IP

- Haciendo un whois a la IP 80.96.68.71 obtenemos que pertenece a Rumanía.

```
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
source:       RIPE # Filtered
```

- La localización física de la IP (Networldmap.com):
  - **País**: Rumanía: **Región**: Bucarest **Ciudad**: Bucarest **LAT**: 44.4330 **LONG**: 26.100

Ficheros de logs /var/log/*

- Comprobamos la hipótesis de que el servidor haya sido la vía de acceso. → El servidor web del sistema no ha sido arrancado nunca.
- /var/log/boot.log:
  - Ago 21 29:02:12 Portmaper = 1, nfslock = 1, fordwarding = 0, SSH =1,
  - Ago 23 00:25:05 klog muere.
- /var/log/messages
  - Agu 21 19:02:13 rpc =1, eth0.
  - Agu 22 23:37:55 ftpd[7020] C, Agu 23 00:12:15 ftpd[7045] C , Agu23 00:19:19 ftdp[7049] C, **Agu 22 22:21:05** ftpd[7049] user: anonymous pass:mozill@

?

Ficheros de logs /var/log/*

- /var/log/secure : Aug 22 08:17:24 localhost xinetd[812]: START: ftp pid=6586 from=218.146.115.18
  Aug 22 08:30:13 localhost xinetd[812]: START: ftp pid=6595 from=213.84.155.131
  Aug 22 13:11:59 localhost xinetd[812]: START: ftp pid=6733 from=210.83.207.251
  Aug 22 19:16:07 localhost sshd[6902]: Did not receive identification string from 195.116.20.232
  Aug 22 23:30:31 localhost xinetd[812]: START: ftp pid=7019 from=213.84.155.131
  Aug 23 00:12:13 localhost xinetd[812]: START: ftp pid=7045 from=200.47.186.114
- ¿El servidor de FTP está en funcionamiento? No aparece en el arranque. Revisamos "/etc/xinetd.d/wu-ftpd" y observamos que **sí está activo**.De nuevo la fortuna nos sonríe y encontramos un directorio borrado, "/etc/xinetd.d/wu-ftpd~". Lo examinaremos más adelante. Observamos una serie de direcciones que intentan conectar al servidor de ftp y con el de ssh.

Investigación de directorios sospechosos

- /root/../ .
  - **M**: 2002.08.23 01:45:58
    A: 2002.08.23 04:03:1
    C:2002.08.23 01:42:58
- ls –la /root/.,
  - Según el nodo-i y las MACs:
    1. psyBCN.tar.gz
    2. awu.tar.gz
    3. aw/ y 4. psybnc/

Fichero	iNode	M	A	C
psyBNC.tar.gz	6081	2002.08.23 01:16:55	2002.08.23 01:17:31	2002.08.23 01:16:55
awu.tar.gz	6082	2002.08.09 22:56:24	2002.08.23 01:42:59	2002.08.23 01:41:51
aw/	12171	2002.08.23 01:43:31	2002.08.23 04:03:11	2002.08.23 01:43:31
psybnc/	42351	2002.08.23 09:48:08	2002.08.23 04:03:11	2002.08.23 09:48:08

Investigación de directorios sospechosos

- Con autopsy descargamos localmente el fichero.
  - tar zxf psyBNC.tar.gz
    - $\subset$ psybnc/ $\equiv \subset$ root/.,/
    - cat psybnc/README → El propósito del programa es conexiones a IRC. Mantener conexiones en el IRC. psyBNC 2.2.1 precompiled linux-i86 glibc2 static
    - file psybnc → está compilado de manera estática.
  - Según el nodo-i y las MACs:
    1. psyBCN.tar.gz
    2. awu.tar.gz
    3. aw/ y 4. psybnc/

Investigación de directorios sospechosos

- psybnc:
  - Se traslada el binario a una máquina aislada con VMWare y con discos no persistenes para evitar cualquier modificación (cabayo de troya).
  - Strace: comprueba llamadas al sistema.
  - No se encuentran nada anómalo
- Convconf. Análogo al caso anterior

Investigación de directorios sospechosos

- awu.tar.gz
  - aw/
    - Makefile. Risktra + awu ‘worm’ y ‘autorooter’. http://www.giac.org/practical/Jerry_Pierce_GCFA.doc
    - auto, awu, awu.list, awu.log, pscan2 (escaneo de puertos), ss..
    - wu: se ejecuta en un entorno controlado. → exploit para las WU-FTP, que intenta logearse con el usuario FTP contraseña mozill@. (trans 20)
  - Conclusión: rootkit/autorooter “autowu” escrito en Rumano (babelfish.altavista.com)

Investigación de directorios sospechosos

- /var/ftp/nerod ≡ nerod.tar.gz
  - ls –la
  - file *
  - Se examinan los diferentes fichero. Básicamente lo que hacen es modificar ficheros y entradas en el sistema.
  - install:
- 1.quita el histórico de la shell.

……..

Investigación de directorios sospechosos

- 1 .quita el histórico de la shell.
- 2) cambia los atributos de los ficheros siguientes, para que sean "modificables", "editables" (no solo de añadir) y "borrables" (chatttr -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 /usr/local/sbin/sshd /usr/sbin/sshd /bin/ps /bin/netstat /bin/login /bin/ls /usr/bin/du /usr/bin/find /usr/sbin/atd /usr/bin/pstree /usr/bin/killall /usr/bin/top /sbin/fuser /sbin/ifconfig /usr/sbin/syslogd /sbin/syslogd /etc/rc.d/init.d/inet
- 3) borra el fichero de bloqueo de atd y mata el proceso con la orden "killall"
- 4) Sustituye "/etc/rc.d/init.d/syslog" (y también "/etc/rc.d/init.d/syslogd" si existe) y detiene "syslogd".
- 5) Verifica que haya un sistema de arranca compatible SYSV ("/etc/rc.d/...") o vuelve a lanzar el syslogd y para la instalación.
- 6) Busca la orden "md5sum" o detiene la instalación (volviendo a lanzar el syslogd).
- 7) Copia los ficheros ".1*" dentro de directorio "/dev" intentando camuflarlos como dispositivos:
- cp -f .1proc /dev/ttyop
  cp -f .1addr /dev/ttyoa
  cp -f .1file /dev/ttyof
  cp -f .1logz /dev/ttyos
- 8) Mediante touch (-acmr) se asegura de sincronizar las "MAC" de los archivos que va a substituir con ficheros referencia (para volver a situar las originales).
- 9) Le pone bit de "setuid" a chsh y lo copia al directorio "/usr/bin/"
- 10) Substituye la orden "/bin/ps" y además se asegura de contar con "/bin/.ps" y con "/bin/lps".
- 11) Hace lo mismo con "top" y "ltop".

Investigación de directorios sospechosos

- 12) añade al fichero "/etc/securetty" las terminales 0,1,2 y 3 (imaginamos que para poder acceder con uid=0 en remoto).
- 13) añade un usuario a "/etc/passwd" y al "/etc/shadow" (usuario ssh). Luego envía por mail con tema "valissh" una copia del archvio "/etc/shadow" a nightman@myplace.com .
- 14) Hace la misma substitución de archivos con "pstree" y "lpstree". También con "killall" y "lkillall" (copia el original en /usr/bin/pidof).
- 15) Lo mismo con "ls". Copia su "ls" en /usr/bin/dir y copia "vdir" en el /usr/bin.
- 16) Crea el directorio "/usr/include/rpcsvc".
- 17) Find, du, netstat, syslogd e ifconfig son substituidos.
- 18) Copia el script clean ("sauber") a "/usr/bin/" y también copia "wp".
- 19) Copia "shad" en "/bin/" y en "/usr/bin/".
- 20) Mueve "/bin/login" a "/usr/bin/xlogin" y copia el suyo encima.
- 21) Copia "md5bd" encima de "atd" e inserta su script de arranque modificado. Es listo y verifica que exista la orden "chkconfig" en caso de que no exista, manualmente enlace el script de arranque para que "atd" funcione en todos los runlevels.
- 22) Copia "vadim", "imp", "slice" y "sl2" en "/usr/bin".
- 23) Crea el directorio "/usr/local/games" y copia dentro "linsniffer" como "identd" y "sense" como "banner".
- 24) Añade el contenido de "functions" al original del sistema.
- 25) entra dentro de "sshd/" y ejecuta "sshd-install" (veremos más abajo que hace).
- 26) Sincroniza la hora de su "xinetd" y lo inserta en el directorio de arranque. Si no hay xinetd lo hace con "inetd".
- 27) Se asegura de arrancar "inetd" (o "xinetd") "atd" y otros.
- 28) Instala el "crontab" dentro del cron del usuario "operator".
- 29) Verifica a ver si encuentra otros rootkits en el sistema.

Investigación de directorios sospechosos

- 30) detiene el portmaper y lo elimina del arranque del sistema.
- 31) Añade con ipchains reglas de cortafuegos que solo permiten conexión a los puertos 111, 465 y 24452 desde localhost.
- 32) copia "me" a "/bin/".
- 33) Crea el directorio "/usr/man/man1/psybnc" y mueve dentro "get".
- 34) Fuerza a "rpm" a instalar una versión de wget directamente desde: ftp.intraware.com
- 35) Manda dos mails con la información del sistema, uno a "frumosu99us@yahoo.com" y otro a "nightman@myplace.com".
- 36) Vuelve a iniciar el syslog, cambia los atributos de los ficheros modificados a Inmutables, y deja vacíos los logs del sistema con ">" (messages, boot.log, cron, secure, maillog).
- 37) Para finalizar descarga "www.kelets.org/kel.c" y lo compila como "kernel", lo copia a "/dev/" y lo ejecuta.
- 38) Borra el directorio "nerod" y el fichero "nerod.tar.gz".

Investigación de directorios sospechosos

- /usr/local/bin/sshd → forma parte del rootkit. (md5)
- Wget instalado 23/08/2002 se instalo a través del ataque.

/etc/xinet.d/wu-ftp

- Hay un psyBNC borrado, donde existe un fichero de configuración que configura:
  - Servidores de conexión
  - Canales #irc
  - Alias: George y NeroD
  - M: 2002/08/23 09:48:08 A: 2002/08/23 04:03:11 C:2002/08/23 09:48:08

/usr/local/games

- Se copian a este directorio: ‘linsniffer’ como ‘identd’ y ‘sense’ como ‘banner’. Además existe un tercer fichero ‘tcp.log’

/var/tmp/.,/

- EnergyMech: mas evidencias el nick George y el proxy PsyBNC

Usuarios “nerod” y “ssh”

- /home/nerod/.bash_history → θ
  - Presuntamente se ha usado el usuario ‘ssh’.
  - El home de ‘ssh’ apunta a /root
    - Miramos el .bash_history para ver que órdenes ha ejecutado.
      - ……
      - Descarga del psybnc,
      - añade ftp, ssh y anonymous a /etc/ftpusers, añade ssh a /etc/ftp y /etc/ssh.
      - borra el usuario ftp (para evitar el acceso anonimo)
      - Con wget descarga psyBNC de otro servidor.
      - Intenta lanzar ataques de ping flood a una máquina.
      - Descaga el awu.tgz y lo instala.
      - Descarga el emech.

Cronología

- **Viernes 23 de Agosto de 2002 00:22:47 m.c -/-rw------- root/ssh root 12054 /var/log/secure**
  - *Un acceso al fichero /var/log/secure modificando y cambiando (probablemente añadiendo una línea por una conexión remota), verficamos el archivo y obtenemos:*

    Aug 23 00:22:47 localhost xinetd[812]: START: ftp pid=7052 from=200.47.186.114
- ***Viernes 23 de Agosto de 2002 00:22:48 104 .a. -/-rw------- root/ssh root 28244 /etc/ftphosts***
  Viernes 23 de Agosto de 2002 00:22:48 4096 mac -/-rw-r--r-- root/ssh root 38169 /var/run/ftp.rips-all
  Viernes 23 de Agosto de 2002 00:22:48 168 .a. -/-rw------- root/ssh root 28245 /etc/ftpusers
  - *Accesos normales al logearse.*

Cronología

- ***Viernes 23 de Agosto de 2002 00:24:19 544317 m.c -/-rw-r--r-- root/ssh root 30143 /var/ftp/nerod.tar.gz***
  - ***Se sube el fichero nerod.tar.gz por primera vez al sistema.***
- ***Viernes 23 de Agosto de 2002 00:24:45 880 .a. -/-rwxr-xr-x 503 503 18082 /var/ftp/nerod/sshd/ssh_config***
  - ***Es en este momento cuando se descomprime el contenido de nerod.tar.gz. La descompresión dura unos dos segundos, hasta las 00:24:46.***
- ***Viernes 23 de Agosto de 2002 00:25:02 12060 ..c -/-rwxr-xr-x root/ssh root 159499 /usr/bin/pstree, ifconfig, sshd…***
  - ***En este instante se empiezan a manipular ficheros del sistema operativo, comenando aparentemente por pstree. Recordemos como funcionaba el instalador que el rootkit llevaba.***

Cronología

- **Viernes 23 de Agosto de 2002 00:22:47 m.c -/-rw------- root/ssh root 12054 /var/log/secure**
  - *Un acceso al fichero /var/log/secure modificando y cambiando (probablemente añadiendo una línea por una conexión remota), verficamos el archivo y obtenemos:*

    Aug 23 00:22:47 localhost xinetd[812]: START: ftp pid=7052 from=200.47.186.114
- ***Viernes 23 de Agosto de 2002 00:22:48 104 .a. -/-rw------- root/ssh root 28244 /etc/ftphosts***
  Viernes 23 de Agosto de 2002 00:22:48 4096 mac -/-rw-r--r-- root/ssh root 38169 /var/run/ftp.rips-all
  Viernes 23 de Agosto de 2002 00:22:48 168 .a. -/-rw------- root/ssh root 28245 /etc/ftpusers
  - *Accesos normales al logearse.*

Cronología

- ***Viernes 23 de Agosto de 2002 00:25:16 a 00:25:18***
  - *Con casi absoluta seguridad podemos afirmar que en este momento se reinició el xinetd.d, despúes de que el atacante retocara la configuración (le vemos por los ficheros que se acceden, ficheros que se modifican, el acceso a los ficheros de LOCALE...).*
- ***Viernes 23 de Agosto de 2002 00:25:19 0 mac -/-rw-r--r-- root/ssh root 30128 /var/lock/subsys/atd***
  Viernes 23 de Agosto de 2002 00:25:19 5 mac -/-rw-r--r-- root/ssh root 38161 /var/run/crontab.pid
  Viernes 23 de Agosto de 2002 00:25:19 465 m.c -/-rw------- root/ssh root 26110 /var/spool/cron/operator
  - *Es en este momento cuándo se instala el crontab del usuario operator que captura la información y al envía por mail.*
- ***Viernes 23 de Agosto de 2002 00:25:34 1423144 .a. -/-rwxr-xr-x root/ssh root 36233 /bin/rpm***
  - *Es en este momento cuando se accede al ejecutable de "rpm", ¿instalando el wget como hemos visto anteriormente? Sí. Observamos en los segundos siguientes que se accede a los diversos ficheros de configuración relacionados con "rpm", y finalmente vemos la confirmación clara en el siguiente evento en rojo.*

Cronología

- ***Viernes 23 de Agosto de 2002 00:25:44 2428 ..c -/-rwxr-xr-x root/ssh root 160476 /usr/bin/rmold***
  Viernes 23 de Agosto de 2002 00:25:444983 ..c -/-rw-r--r-- root/ssh root 112985 /usr/doc/wget-1.5.3/ChangeLog
  Viernes 23 de Agosto de 2002 00:25:44 126024 ..c -/-rwxr-xr-x root/ssh root 159682 /usr/bin/wget-RPMDELETE (deleted-realloc)
  - *Observamos claramente la instalación que se ha hecho del "rpm" de wget.*
- ***Viernes 23 de Agosto de 2002 00:26:05 hasta 00:27:09***
  - *Vemos que el atacante en este intervalo de tiempo está revisando el contenido de los archivos de configuración y arranque del usuario "pepelu" (en estos ficheros pueden encontrarse usuarios y contraseñas, y en el fichero bash_history siempre aparece información interesante para un potencial atacante). Observamos también como revisa todos los ficheros de arranque y de configuración inicial de shell también en /etc.*

Cronología

- ***Viernes 23 de Agosto de 2002 00:27:09 52348 .a. -/-rwxr-xr-x root/ssh root 159006 /usr/sbin/useradd***
  - ***Utiliza la orden "useradd" y añade el usuario "nerod" (observamos como se accede a los ficheros de "skel" y como se van creando los ficheros dentro de "/home/nerod").***
- ***Viernes 23 de Agosto de 2002 01:16:55 557964 m.c -/-rw-r--r-- root/ssh root 6081 /root/.,/psyBNC.tar.gz***
  Viernes 23 de Agosto de 2002 01:17:30 262 .ac -/-rw-r--r-- pepelu pepelu 22289 /root/.,/psybnc/help/RELAYLINK.TXT
  - ***Accede al directorio "/root/.,/" y ejecuta una acción sobre el fichero psyBNC.tar.gz que probablemente sea la de crearlo y descomprimirlo al instante siguiente. La descompresión termina a las 01:17:31.***
- ***Viernes 23 de Agosto de 2002 01:17:37 121180 .a. -/-rwxr-xr-x root/ssh root 159412 /usr/bin/make***
  Viernes 23 de Agosto de 2002 01:17:37 227 .a. -/-rw-r--r-- pepelu pepelu 42359 /root/.,/psybnc/Makefile
  - ***Ejecuta "make" (lo hemos visto en el bash_history) para compilar el proxy-cliente de irc.***

Cronología

- *Viernes 23 de Agosto de 2002 04:03:11 1024 m.c d/drwxr-xr-x root/ssh root 24101 /var/log/sa*
  - *Le vemos actuar sobre algunos ficheros, y particularmente le vemos borrar el directorio "/etc/xinetd.d/wu-ftpd~". también observamos que accede a la configuración del automounter del sistema, e inmediatamente despúes accede a /mnt/floppy y /mnt/cdrom (¿en busca de un disquete o cdrom que alguién haya olvidado dentro de la unidad?).*
- *Viernes 23 de Agosto de 2002 08:18:36 161 .a. -/-rw-r--r-- root/ssh root 26115 /etc/hosts.allow*
  Viernes 23 de Agosto de 2002 08:18:36 347 .a. -/-rw-r--r-- root/ssh root 26116 /etc/hosts.deny
  - *Observamos que se revisa la configuración de hosts.allow y hosts.deny (en busca de sistemas confiables que el atacante puede localizar).*
- *Viernes 23 de Agosto de 2002 09:11:17 4741 m.. -/-rw------- root/ssh root 56294 /root/.,/psybnc/motd/USER1.MOTD.old*
  Viernes 23 de Agosto de 2002 09:40:19 4741 .a. -/-rw------- root/ssh root 56294 /root/.,/psybnc/motd/USER1.MOTD.old
  - *Ejecuta el proceso de psybnc.*
- *Viernes 23 de Agosto de 2002 10:17:17 1024 m.c d/drwxrwxrwt root/ssh root 46185 /var/tmp*
  - *Accede al directorio /var/tmp creemos para descomprimir aquí el código fuente de otra copia de psybnc*

Roberto Gutiérrez

Ángel Alonso Párrizas