

Primera edición

LINUX Y MI VECINA

Una historia de intriga, amor y
ordenadores

Autor: Templix

templix@tuxapuntos.com

Editado por
cratxer (cratxer88@gmail.com)
en colaboración con
utopianegra (utopianegra@gmail.com)
y www.tuxapunt.es.com
Octubre de 2009



Esta obra está bajo una licencia Reconocimiento-No comercial-Sin obras derivadas 3.0 España de Creative Commons. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-nd/3.0/es/> o envíe una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Índice general

Sobre ACSII...	7
1. Visualizando estadísticas para la vecina	9
2. Scripts para la vecina	13
3. Clonando el HD de mi vecina	15
4. Clasificar datos de la vecina	17
5. Entrando en el pc de mi vecina	19
6. El profesor y el asunto de mi vecina	21
7. Nada en los logs del disco de mi vecina	23
8. Smarteando el sdb de mi vecina	27
9. Un ulimit que no está a la altura de la vecina	29
10.Cerrar puertos de la amiga de la vecina	33
11.Intentó olvidar a la vecina y me voy de vacaciones	37
12.Como extraviar un pc en la playa y un mail de la vecina	41
13.Como acceder al contenido del mensaje de mi vecina	45
14.Nos salvamos gracias a cups	47
15.Juan el Destripador	49
16.Nos acercamos a la vecina con dsniff	53
17.El tiempo justo para que me líe con steghide	57
18.Rkhunter no puede con ellos	59
19.Tune2fs hace reaccionar a .Antúnez	61
20.Juntos al fin	63

Epilogo

65

Sobre ASCII...

¿No estás hasta el gorro de cosas serias? Ya sabes, gandulear navegando sin rumbo fijo por la red, chatear con los amigos, tragarte unas birras y cosas por el estilo. Pues ponte a jugar un rato: «CTRL+ALT+F1» y te logeas. Porque pondría los cataplines en el fuego a que en esta sesión todavía no habías entrado, en la tty1, te rooteas y:

```
# apt-get install bb caca-utils
```

Cuando termine la instalación, nos desrootamos (exit) y ya podemos empezar con el espectáculo ASCII:

```
$ cacademo
```

Cuando nos hartemos pulsamos «Esc» y quemamos la pantalla:

```
$ cacafire
```

Es muy relajante cuando no es posible (o no te atreves) quemar otras cosas. Cuando tus instintos pirómanos esten saciados, atacas el «Esc» nuevamente y respiras hondo. Prendes los altavoces, subes el volumen a niveles de queja vecinal y:

```
$ bb
```

Le das al «Enter» y pulsa «8». La pantalla empezará a llenarse de números cada vez más rápido y pensarás: ¿Por qué carajos me ha dicho el pamplinas que prenda los altavoces? Bien, no te suicides (de momento) espera un rato y disfruta del código ASCII. Como tampoco es cuestión, por mucha música que suene, de que te tires media hora mirando una pantalla estática, a menos que te hayas chutado alguna cosa rara, puedes pulsar «CTRL+ALT+F7» y continuar con las cosas serias que habías dejado de lado al principio. Cuando te canses de la musiquilla escoge:

- 1.- «CTRL+C» (en la tty1)
- 2.- killall bb (en cualquier consola)
- 3.- O el método fácil:

Abres el puerto 5900 del firewall y el mismo puerto del router, te vas a casa de una vecina complaciente (o vecino según se trate), le dices que tienes un problema gordo con el redireccionamiento de los parámetros hectoplásticos helicoidales

de las DNS y que por favor (educación ante todo) te deje usar su ordenata para resolverlo. Te repones al primer impacto visual (seguro que usa guindous) pero tú, que eres muy hábil, en un plisplas le metes el livecd y reinicias (uffff, por poco se te quema la retina) abres consola y:

```
$ vncviewer la_ip_de_tu_chabola
```

Y haces lo del «CTRL+C» o el killall bb pero dando un rodeo de 20 minutos (como mínimo) por todos los comandos que se te ocurran. Mientras ella mira por encima de tu hombro y de vez en cuando va soltando aquello de:

-¡Narices, cuánto sabes! - y tú, sin dar mucha importancia a la cosa,
-Eso es muy complicado, no sé si lo conseguiré...

Al rato y cuando ella ya te ha traído un par de birras y notas que está fundida por ti, exclamas:

-¡Solucionado! Me has salvado la vida.

El final es clásico: Te acuestas con ella y encima le instalas un linux y te comprometes a solucionarle todos los problemas con los que se encuentre.

Y todo gracias a ASCII....

Capítulo 1

Visualizando estadísticas para la vecina

Dormías como un lirón cuando de repente suena el teléfono. Te despiertas del sobresalto y...

- ¿Quién? Vaya, la vecina, aquella con la que te acostaste cuando lo del ASCII, que sin más preámbulos te suelta:

- ¿Amorcito, que hago para saber las estadísticas de la gente que visita mi página web?

Mentalmente te maldices mil veces por haberle prometido que no dudara en consultarte cualquier problema que pudiera surgir.

- Me visto y vengo pitando, mientras llego, rootéate y enchúfale en consola:

```
# apt-get install awstats libnet-dns-perl
libnet-ip-perl libnet-xwhois-perl
```

- No es necesario

- ¿Cómo que no es necesario? ¿Es que ya tienes instalado awstats y sus dependencias?

- No, que digo que no es necesario que te vistas.

La cosa promete. Al azar, agarras un vino de tu despensa (un Chateau Garrulón del 2004 rc2 con un retronasal que se las pela) y sales flechado. Te abre con un camisón con más transparencias que las capas del Gimp y te endiña:

- Aquí tienes al nosequéstats y a toda su parentela.

- ¡Madre mía, dos días en linux y qué dominio de la consola!

- ¿Qué consola ni qué monsergas? Por synaptic como la gente de bien.

Aprietas los dientes pero son más de las 2 y no estás para pláticas filosóficas. Casi sin pestañear editas el archivo de configuración:

```
# nano /etc/awstats/awstats.conf
```

Pones el "2" en LogFile = "/var/log/apache2/access.log" y en SiteDomain = "la_vecinita.com" su nombre de dominio. Guardas, cierras y creas el enlace a los iconos:

```
# ln -s /usr/share/awstats/icon/ /var/www/awstats-icon
```

CAPÍTULO 1. VISUALIZANDO ESTADÍSTICAS PARA LA VECINA

Tus dedos vuelan sobre el teclado...

```
# /usr/lib/cgi-bin/awstats.pl -update
  -config=/etc/awstats/awstats.conf
```

- Ya está

- ¿Como que ya está?

- Que ya está. Mientras lo compruebas abriendo el navegador y escribiendo en la barra de direcciones:

```
http://localhost/cgi-bin/awstats.pl
```

- Yo iré abriendo el Chateau Garrulón del 2004 (no dices nada de que en realidad se trata de una versión beta) y me pondré cómodo.

- Sí, muy bonito, pero cualquiera que sustituya "localhost" por mi ip verá las estadísticas y solo quiero verlas yo, a los demás no les interesan.

Dejas de mala gana el Chateau y aunque te cuesta pensar porque la sangre no fluye muy bien por tu cabeza, ya que se ha desplazado llenando determinados capilares difíciles de disimular, agarras el teclado (procurando no tocar la tecla maldita con la banderita del Gueits) y:

```
# gedit /etc/apache2/sites-available/default
```

Buscas como un poseso la sección que diga algo parecido a:

```
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
  AllowOverride None
  Options Indexes Includes ExecCGI
  Order allow,deny
  Allow from 127.0.0.1
</Directory>
```

Y en Allow bla, bla, bla le encasquetas la ip 127.0.0.1 y reinicias apache:

```
# /etc/init.d/apache2 force-reload
```

- ¿Contenta la niña?

- Oh pichoncito, eres un sol.

El Chateau Garrulón dura menos que un suspiro y el último vaso ya es una amalgama de fluidos de distinta naturaleza. A duras penas te estás reponiendo del tercero cuando te suelta al oído:

- Dulzura, ¿y por qué no le pones una contraseña y así desde tu casa también podré consultar las estadísticas?

- Amorcito, un deseo tuyo es para mi una orden - dices.

Aunque en realidad lo que piensas es: "Lo que tiene que hacer uno por un buen polvete." Tambaleándote de un lado para otro y después de darte con los piños en el canto de la puerta, agarras nuevamente el teclado y casi a puñetazos:

```
# gedit /etc/apache2/sites-enabled/000-default
```

Vuelves a buscar la sección que habías modificado, sustituyes el "127.0.0.1" por el "from all" y le añades las líneas correspondientes:

```
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
    AllowOverride All
    Options Indexes Includes ExecCGI
    Order allow,deny
    Allow from all
    AuthName "Acceso restringido a Estadísticas"
    AuthType basic
    AuthUserFile
        /etc/awstats/htpasswd.la_vecinita.com require valid-user
</Directory>
```

Mientras tecleabas, ella se había acercado y me estaba dando un masaje en el cuello de lo más relajante.

- ¿Qué nombre de acceso quieres?
- ¿A ti qué te parece?
- ¿Y contraseña?
- Ni idea.
- Clarísimo.

```
htpasswd -cm /etc/awstats/htpasswd.la_vecinita.com atiqueteparece
```

Introduces la contraseña "niidea". La confirmas.

- Bueno ahora sí que ya está todo terminado
- ¿No se te olvida reiniciar apache?
- Vaya con la lista

```
# /etc/init.d/apache2 force-reload
```

- ¡Fin!, ¿Dónde estábamos?

- No sé si te has fijado en la hora, pero yo tengo que ir al curro y creo que tú también. Me voy a duchar.

Antes de entrar en el baño se giró y me lanzó un beso.

- Estuvo muy bien

Y cerró la puerta. No quedó claro si se refería a lo del awstats, a lo ocurrido entre sábanas o al Chateau Garrulón del 2004. Mientras bajaba por las escaleras me tocaba la mandíbula, que me dolía horrores, ¡menudo porrazo con la puerta! Me tomé un café en un bar y me fuí al laboro, aquel sería un día muy duro.

CAPÍTULO 1. VISUALIZANDO ESTADÍSTICAS PARA LA VECINA

Capítulo 2

Scripts para la vecina

Tarde varios días en saber de ella. Primero por culpa de las diarreas y vómitos causados, supongo, por el Chateax Garrulón del 2004 y después porque la lectura de la trilogía de Stieg Larsson me había absorbido por completo. Ni siquiera me conectaba a la red. La llamé.

- Es que verás, te he hecho un script para ver de una forma más simple las visitas que recibas en tu página.

No era cierto que lo hubiera escrito para ella, lo tenía de hacía tiempo pero era la excusa perfecta para volver a verla.

- Vale, traigo unas cervezas y charlamos.

Me abrió.

- Así que un script ¿eh?, dame el lápiz que yo me encargo. He avanzado mucho últimamente.

- Me alegro. Antes instala la aplicación necesaria:

```
# apt-get install geoip-bin
```

- No digas más. Copi-pasto el texto:

```
#!/bin/bash
echo
echo Las ips y procedencia de las visitas es:
echo IPS=$(cat /var/log/apache2/access.log |
awk '{print $1;}' | sort -nr | uniq | grep -v ':')
for x in $IPS
do
    echo "$x" 'geoiplookup $x | awk '{print$5}''
done
echo
```

Mientras tecleaba con aquellas manos finas y delicadas, yo permanecía de pie a su lado totalmente ajeno a la pantalla y mirándola sólo a ella. Su belleza era sobria, sin estridencias ni bugs aparentes, más cercana a un gnome 2.26 que a un kde 4, con un par de terminales potentes y, por si fuera poco, todos los puertos USB funcionales y capaces de enloquecer al más friki. Ajena a mis pensamientos, ella continuaba a lo suyo:

- Guardo como "acceso". Cierro. Le doy permisos:

```
# chmod +x acceso
```

- Y lo lanzo:

```
./acceso
```

- Vaya, solo 7 visitas y, seguro, todas mías. Este script es muy seco, awstats al menos tiene más colorines.

- El script no hace milagros, salen las mismas visitas pero es más rápido y casi no consume recursos.

- ¡Los recursos! Ya han salido los recursos. ¿Pero tú de verdad piensas que mi flamante ordenata de chorrocientos núcleos, tanta RAM que se le sale de la caja y una CPU a muchosmil megahercios va a tener un bajón existencial por culpa del exceso en el consumo de recursos? Vamos hombre, eso era en la prehistoria.

La cosa no iba como yo esperaba. Si no me espabilaba aquella noche me quedaría a dos velas.

- Tengo otro script que te dice la IP pública, la privada y la del router que también te puede ser útil.

- Perdona, pero he tenido un día muy malo y encima me ha venido. Tu mismo me lo instalas y cuando salgas cierra, me voy a la cama.

Me quedé solo en la habitación con su PC. Me senté y puse los dedos en el teclado que ella estaba pulsando momentos antes. Cerré los ojos y por unos momentos dejé volar la imaginación. Cuando desperté del trance me lancé con el script y la aplicación necesaria:

```
# apt-get install w3m
#!/bin/bash
echo
echo -e "\033[1;31mTus ips son estas:\033[0;0m"
echo
IPU=$(w3m -dump http://cfaj.freeshell.org/ipaddr.cgi)
IPR=$(ifconfig | grep Bcast | awk '{print $2}' | cut -d ":" -f 2)
IRO=$(route -n | grep "^0.0.0.0" | cut -b 17-32 )
echo "IP Pública: $IPU"
echo "IP Privada: $IPR"
echo "IP Router: $IRO"
echo
exit 0
```

Guardé como "ips" le di permisos (`# chmod +x ips`) y lo arranqué (`./ips`) para comprobar si había algún error. Funcionó. Mi faena había terminado pero me sorprendí a mi mismo husmeando en su ordenata. Sólo en las aplicaciones instaladas y en lo que tenía esparcido por el escritorio (¡jamás hubiera entrado en su carpeta de usuario!). Efectivamente podía observarse que se había metido de lleno en el tema. Pulsé:

```
# init 0
```

Y me levanté, antes de salir pasé por delante de su cuarto y pude ver como dormía plácidamente a través de la puerta entreabierta. Le tiré un beso y salí. Aquella noche dormí mal.

Capítulo 3

Clonando el HD de mi vecina

Harto de dar vueltas en la cama, me levanté. Era temprano, demasiado para ir a su casa y, con la excusa de ir a buscar el lápiz que dejé, volver a verla. Para dejar pasar tiempo di una vuelta por los alrededores y me tomé un café en un bar que encontré abierto. Me dirigí a su apartamento. Por si todavía dormía, en vez de tocar el timbre di unos pequeños golpecitos con los nudillos en la puerta. Se abrió un poco. Estaba seguro de que la había cerrado. O quizá no... No sé... No podría asegurarlo. Entré dando algunas voces para no asustarla. La puerta de su cuarto, al final del pasillo, estaba abierta, señal de que ya se había levantado. Debe estar en el baño -pensé. Continué dando voces y haciendo ruido; no quería de ninguna manera darle un sobresalto.

Llegué a su cuarto y miré en el interior. La visión me dejó completamente petrificado: todo revuelto y sangre por todas partes. Ella yacía, exánime, en su cama. ¿Quién podía haber realizado aquella carnicería y con qué motivo? Tardé un buen rato en reponerme. Estaba desconcertado. Me juré ante su cadáver que el culpable lo pagaría muy caro. Intenté pensar con lógica. Yo era la persona que la vió con vida por última vez y mis huellas estaban por todas partes. No tardarían en venir a por mí. Disponía de poco tiempo. Me dirigí al ordenador. El lápiz que había olvidado incluía una iso bootable del parted magic. La arranqué. Por suerte aquel día había dejado netcat corriendo en mi máquina

```
$ nc -l -p 9000 | dd of=/dev/sdb
```

para realizar unas pruebas desde casa de un amigo. Dejar corriendo netcat es una imprudencia totalmente desaconsejable porque, básicamente, lo que hace esta aplicación es escuchar (-l) en el puerto (-p) 9000 y copiar (dd) todo lo que le llegue al disco sdb (of=...) y ese "todo" puede darte muchas sorpresas. Pero en este caso me iba de perlas para clonar el disco de mi vecina. Abrí terminal en el parted magic y:

```
$ dd if=/dev/sda | nc ip_de_mi_chabola 9000
```

Mi sdb tenía doble capacidad que el sda que estaba clonando y el proceso podía durar un par de horas. No podía sacarme de la mente la brutal escena. Que puede pasar por la mente de alguien para cometer algo tan atroz. Debía llamar a la policía, pero yo era el principal sospechoso. Necesitaba tiempo para analizar los datos del disco duro en busca de cualquier indicio que me llevara al asesino.

Me pasó por la cabeza que cuando terminara la clonación podría lanzar desde mi parted magic un entrono chroot previo montaje de la partición para no dejar más rastros de mi presencia:

```
# mount /dev/sda2 /mnt/sda2 # chroot /dev/sda2 /bin/bash
```

Y desde él, borrar varios logs del sistema en el directorio /var, o saliendo de chroot:

```
# exit
```

Y lanzar desde el lápiz

```
# shred -fuv /mnt/sda2/home/la_vecina/.bash_history
```

Y repetir la operación con varios archivos para borrarlos y reescribir su espacio 25 veces o mejor añadiendo "-n 50" para hacerlo 50 veces para estar seguro de que fuera imposible acceder a ellos:

```
# shred -fuv -n 50 /mnt/sda2/home/la_vecina/.bash_history
```

O incluso eliminar todo el disco duro escribiendo montones de números aleatorios con:

```
# dd if=/dev/random of=/dev/sda
```

O simplemente ceros:

```
# dd if=/dev/zero of=/dev/sda
```

O usar el paquete secure-delete y borrar todo el directorio:

```
# srm -r /var
```

Y cualquier rastro en la memoria del ordenador:

```
# smem
```

Y de la swap:

```
# sswap /dev/sda3
```

Estaba enloqueciendo. Incluso se me había pasado por alto que el paquete secure-delete no está entre los del parted magic. Mientras estudiaba posibilidades, la clonación terminó. No hice nada. Si la policía veía que se habían eliminado datos pensaría que tenía algo que esconder y, estaba pensando como un reo y yo no había matado a nadie. Es más, quería pillar al asesino para hacerle pagar su canallada. Empezaba a amanecer, cerré el pc, cogí mi lápiz y salí no sin antes volver a mirar la escena dantesca en la habitación en la que, en otra ocasión, habíamos gozado juntos. Nadie me vió o así lo creí. Me fuí directo a mi casa me duché y me fuí al laboro. Tampoco llamé a la policía, sería difícil convencerles de que había vuelto a por mi lápiz.

Capítulo 4

Clasificar datos de la vecina

Pasaron un par de días antes de que la bofia viniera a buscarme. Me encontraba en el curro y el patrón, que casi estaba tanto hasta las narices de mí como yo de él, aprovechó la circunstancia para echarme a la calle: "rm *, /dev/nul, not found". Gritaba como un energúmeno mientras me llevaba la pasma. En comisaría aguardé una eternidad en la sala de interrogatorios hasta que entraron dos sujetos. Uno se identificó como Subinspector Linares y el otro, cuadrado como un armario, ni se molestó en presentarse. El Subinspector Linares se sentó y hacía como que miraba unos papeles sin decir ni pío, el armario daba vueltas por detrás de mí:

- Con que Linux, ¿eh?
- GNU/Linux para ser más exactos.
- Mmmm...

Hablaba sin mirarme siquiera y continuaba removiendo sus papeles.

- Vd debe ser de esos niños que tanto saben.
- No crea. Simple usuario.
- Ya.

Entre pregunta y pregunta permanecía en silencio largo rato.

- ¿Así que, Linux?
- GNU/Linux. - insistía yo.
- ¿Hay algo que deba contarnos?
- Pues sí, que K3b se chorrea al emperador romano.

El armario se avalanzó sobre mí levantando su puño.

- Mira imbécil, si piensas que vas a tomarnos el pelo...

Me salvó de la agresión la rápida intervención del Subinspector Linares. Si no es por él a estas horas estarían reconfigurándose la interfaz gráfica y parte del xorg.conf en agencias de algún hospital provincial. El Subinspector acompañó amablemente a su compañero a la puerta y le aconsejó que se tomara un café para tranquilizarse. Luego se me acercó:

- Mira muchacho, de momento no tenemos cargos contra ti, pero mejor que no salgas de la ciudad si no quieres tener problemas.
- No pensaba hacerlo.

Me pasó el brazo por el hombro mientras me acompañaba a la puerta.

- Por cierto, ¿cuando se formateó el PC de tu vecina?
- ¿Formatear? Sí, cuando...

El Subinspector Linares esbozó una leve sonrisa de triunfo. Me había pillado. ¡Caray si me había pillado! Caí como un pardillo.

- Volveremos a vernos muchacho.

Salí y analicé la situación: sólo veía una posibilidad y era que alguien había asesinado a mi vecina, se había ido y luego había vuelto a formatear el pc. Porque en el caso de que hubiera estado allí escondido, mientras yo clonaba el disco hubiera sido innecesario el formateo. O el asesino desconocía que alguien hubiera clonado el disco o yo corría peligro. Además, ¿por qué formatearlo? Todo el mundo sabe que un formateo no borra ningún dato, sólo facilita que los nuevos datos se escriban encima de los viejos. Con un simple:

```
# apt-get install testdisk
```

Y lanzar en la terminal maximizada:

```
# photorec
```

Escoger el disco (o cd, o tarjeta) y el lugar donde guardar los datos recuperados y, dependiendo de la extensión a recuperar, en unas cuantas horas tenemos tantas carpetas `recup_dir` y cada una con tantos archivos en su interior, que supuran hasta por las ranuras de la fuente de alimentación. El único problema entre tanta información, si no sabemos qué buscamos, es clasificarla y desechar la porquería. Hay muchos sistemas:

```
# chmod 777 -R /home/usuario/carpeta_de_los_recup_dir
$ cd a_la_carpeta_de_los_recup_dir
$ mkdir pngs
$ mkdir jpgs
$ mv recup_dir.*/*.png pngs/
$ mv recup_dir.*/*.jpg jpgs/
$ rm recup_dir.*/*.html
```

Y así: `mv` a la carpeta correspondiente lo que queremos guardar y `rm` lo que queremos suprimir y en cinco minutos está la información ordenada por extensiones, pero el trabajo de mirar archivo por archivo no nos lo quita ni las barbas de Stallman.

La curiosidad por mirar el sdb con los datos que había clonado de mi vecina me quemaba. Sin curro, disponía de mucho tiempo. Al menos hasta que mi casero me diera el portazo.

Capítulo 5

Entrando en el pc de mi vecina

Sólo conocía el nombre de usuario, la contraseña ya no era la misma que el día de la instalación, la había modificado:

```
# passwd root
```

Se pone la contraseña, se confirma y asunto resuelto. Poner contraseñas sólo es útil si nadie va a tener acceso físico a la máquina, pero si puede accederse a ella es tan absurdo como que un guindous funcione medio bien. Tocaba entrar con el livecd y:

```
# gedit /etc/shadow
```

Buscar el usuario y el root y borrarles el cacho numeraco que va desde los primeros dos puntos a los segundos:

```
usuario:$6$vcqbVspTks/v$1wccuz54JKQjJAL3LV1qceB0GdJxjHBKfiULUTzui2BtInv0mFSuUJRbz5h8B1.:14376:0:99999:7:::
root:$6$bVfUh3Q.$0ggPNP2UvD0b0vKEG4prJXyphxg52r6qLsGA6ztJTUXyVKU4Ez3.pgnRsCXe0kv/:14434:0:99999:7:::
```

dejándolo:

```
usuario::14376:0:99999:7:::
root::14434:0:99999:7:::
```

Reiniciar, y cuando pida la contraseña darle al «Intro». Una vez dentro poner las nuevas contraseñas. Si no se tiene a mano un livecd (o el pc no inicia el boteo por el cd y la bios tiene contraseña y no tienes un destornillador para sacarle la pila y resetearla) cuando salga el menu del grub pulsar "e" sobre el sistema a botear y nuevamente "e" en la linea del kernel para editarla y poner al final:

```
init=/bin/bash (el teclado estará en inglés)
```

Pulsar "b" para iniciar el arranque. Solo se monta la partición / (no la /home si está en una partición diferente) y sólo como lectura (ro), por lo que:

```
# mount -o remount,rw /dev/sda2 # passwd usuario/root
```

La remontamos lectura/escritura (rw) y ponemos la contraseña de usuario o de root que nos plazca y claro, reiniciamos.

El pc de mi vecina tenía su \$HOME lleno de tutoriales de todas clases sobre las áreas mas inverosímiles. No mentía cuando dijo que se había metido de lleno en el mundo GNU/Linux. Los marcadores del navegador totalmente monotemáticos: linuxparatodos.net, espaciolinux.com, tuxapuntos.com, todo-linux.com, fentlinux.com... Y una larga lista de portales. Había creado una carpeta "distro" que contenía una docena larga de isos de distintas distribuciones. Yo figoneaba por todos los rincones del pc en busca de algo que de momento se me escapaba de las manos. Sonó el timbre. Era el Subinspector Linares. Venía solo.

- Hola muchacho.

- No me dirá que pasaba por aquí y..

No fué necesario invitarle a pasar porque ya estaba dentro.

- Bonito apartamento y bonito escritorio.

No dije nada de que el escritorio no era el mío.

- Linux, ¿no?

- GNU/Linux.

Diríase que quería tocarme las aplicaciones: ¡Siempre con la misma observación!

- ¿Has oido hablar de GdV?

- ¿Un plugin?, ¿una distro?, ¿El penúltimo invento de google? ¿tiene relación con el gdm?

- ¿Y de bp?

- Suena como a hidrocarburos, ¿no? ¿O se refiere a fb? O sea framebuffer que vendría a ser la porción de memoria reservada para mantener temporalmente una imagen a la espera de ser enviada al monitor y que con un:

```
# apt-get install hwinfo
# hwinfo --framebuffer
```

Te enteras de los modos (mode) que soporta la máquina. Pero, ¿podría aclararme si su problema es de framebuffers?, ¿dificultades urinarias por culpa de la próstata?, que a su edad ya se sabe, ¿o que no tiene dinero para gasolina?

Mientras le daba la paliza él abría carpetas y, creo no hizo ni caso a mis profundísimas argumentaciones. Abrió la "Imágenes".

- Bonita chica.

No contesté porque se me hizo un nudo en la garganta. Antes la encontraba bonita pero ahora la encontraba rabiosamente bonita.

- Muchacho, puedes estar en peligro

- Subinspector, es Vd un profeta, esta mañana casi me aplasta un cuatro ejes.

- El asunto es muy grave.

- Si me hubiera aplastado sería gravísimo. Cuídese esas almorranas, lo digo porque como ni siquiera se ha sentado...

Capítulo 6

El profesor y el asunto de mi vecina

Google no me aclaró lo del "GdV" ni del "bp" por los que había preguntado el Subinspector Linares. Quizá el Profesor podría ayudarme. Le llamábamos así porque había dado clases de MS-DOS en tiempos del Califato de Córdoba. Fui a visitarle.

- ¡Muchacho! ¡Cuánto tiempo sin verte! Pasa, pasa...

Me hizo pasar y sentarme en el salón.

- ¿Te has casado?, ¿tienes hijos?, ¿en qué trabajas?...

Se le amontonaban las preguntas. Diríase que quería hacer un "cat mi_ vida" sin tubearlo con "less". Respondí de renglón:

- No. Ni pensarlo. En nada.

- ¿Qué sabes de Serrano?, aquel que llamábais "Serrano el melenas, el terror de las nenas"

- Si, buen chaval. Se hizo de una ONG pro salvarlo todo, pero alguien de la dirección descubrió que se había comprado los muebles en Ikea y el pobre no pudo soportar la humillación y lo encontraron colgado de la rama de un árbol en un parque público.

- ¡Qué detalle más tierno! Pobre muchacho... y Menéndez, ¿qué se ha hecho de Menéndez?

- Prometía. Llegó a director de zona de una multinacional. Cobraba un pastón. Un buen día dijo que había descubierto la luz, regaló todos sus bienes y se fué a meditar a no sé que montañas y no he sabido más de él.

- Vaya, vaya. Pero bueno, ¿qué te ha traído por aquí?

- Verá, creo que Vd es el único que puede ayudarme, ¿qué sabe del GdV y del bp?

Al oír aquellas siglas me hizo bajar la voz y se levantó de un salto. Corrió a la puerta, la abrió, miró fuera, volvió a cerrar pasando el pestillo, se fue a la ventana a correr las cortinas, por una rendija miró a la calle.

- ¿Te han seguido? parece que no hay nadie, ¿seguro que no te han seguido?

- Pero ¿qué ocurre?, ¿qué es tanto misterio?

Se sentó nuevamente muy nervioso y mirando continuamente a la puerta y a la ventana. Insistí en plan docto:

- Toda acronimia debe tener un texto subyacente.

- Y lo tiene, muchacho, lo tiene. ¿No has oído hablar nunca de los Guerrilleros del Ventanuco?

Era la primera vez que oía aquel nombre.

- ¿Guerrilleros del Ventanuco?

- Están por todas partes. Muchos que son del grupo, ni saben que lo son. No puedes fiarte de nadie. Algunos lo niegan y reniegan para despistar. Un Guerrillero del Ventanuco nunca dice públicamente que lo es, se han infiltrado en todos los estamentos de la sociedad, lo ven todo, lo saben todo. Vayas donde vayas.

- ¿Y el bp? - pregunté totalmente desconcertado.

- Estos son los peores. Mala gente. Es la facción armada y radical de los Guerrilleros del Ventanuco. Se hacen llamar...

Bajó más la voz y como hablándome al oído dijo:

- ... los Blue Pántallaz. Son como las SS para Hitler, la KGB para Stalin o el ketchup para un frankfurt. ¿Te acuerdas de Antúnez? ¿Aquel que cojeaba? un lince del C++. Pues ahora es .(punto)Antunez. Un personaje no visible ni con «CTRL+H». Muchacho, ¿no te habrás metido en líos, verdad? Yo no puedo ayudarte... Soy viejo. Aunque pudiera no sé cómo. No creí que jamás volviera a escuchar estas siglas. No digas a nadie que has hablado conmigo, te lo suplico.

Salí. A mis espaldas noté como volvía a pasar el pestillo. Sin querer le había ocasionado un kernel panic como la catedral de Burgos. Espero que:

```
# cat /proc/sys/kernel/panic
```

No tenga un cero por resultado, en tal caso nunca volverá a la realidad. Si el Profe fuera un sistema operativo podría hacer que tras un kernel panic se reiniciara a los 3 segundos con:

```
# echo "kernel.panic=3" >> /etc/sysctl.conf
```

y asunto resuelto. O, en plan rápido y para la ocasión, manteniendo pulsadas las teclas «Alt+ImpPant» (la de capturar la pantalla) pulsar sucesivamente las teclas REISUB aunque tengas que hacer virguerías con los dedos. Pero el Profe era una persona y una persona si no lo supera, puede terminar muy mal.

Capítulo 7

Nada en los logs del disco de mi vecina

¡La de información que puede sacarse de un navegador! Siempre que no haya sido limpiada claro. Cuando entré en gmail, los datos de mi vecina aparecieron de inmediato puestos en los lugares correspondientes, sólo tuve que aceptar y allí estaba todo su correo: las clásicas presentaciones chorras que van, vuelven, vuelven a ir y vuelven a volver y en cada paso van acumulando más y más cuentas de correo para delicia de spammers, la nueva pesadilla del bombardeo de invitaciones al Facebook de los amigos (¿amigos?) que fueron borradas sin abrir, varios boletines sobre GNU/Linux y algunos de temáticas varias y entre el correo que no pudo llegar a abrir uno con un .doc adjunto "Vamos a por ti" en comic sans, roja y a 100 de tamaño. ¡Larga vida a los GdV!" en más pequeño y abajo del todo: "BP" el remitente: piauiode@guerrillamailblock.com, una dirección desechable (<http://www.guerrillamail.com>) muy útil para cuando nos queremos registrar en algún lugar en el que tenemos que dar una dirección de correo para que nos manden la contraseña y al que, una vez realizada la gestión que deseamos, es probable que no volvamos nunca más o, como en este caso, para amenazar a alguien. Quise mirar si los logs me decían algo:

```
$ grep "Invalid user" /var/log/auth.log
```

Dos intentos de conexión ssh de la ip 83.58.85.196. No creo que tuvieran relación con el caso.

```
$ geoipllookup 83.58.85.196
```

La procedencia España. Existen muchas páginas que sitúan la ip en un mapa. En realidad lo que sitúan es la isp que son los proveedores de servicios y lo bueno es que en alguna ocasión aciertan. Además, puede darse el caso que la ip esté detrás de un proxy. La diferencia fundamental entre intentar averiguar una ip que esté o no esté detrás de un proxy es que en el segundo caso, si te dice que está en Logroño, puede que no esté en Bollullos del Condado y en el primer caso puede estar incluso en Bollullos del Condado. Si se pretende un comando al estilo de:

```
# apt-get install lacoñanet-bin
```

CAPÍTULO 7. NADA EN LOS LOGS DEL DISCO DE MI VECINA

```
$ lacoñanet -a 83.58.85.196
Starting lacoñanet 3.42 ( http://lacoñanet.org ) at 2009-07-12
07:21 CEST
Amable caballero: La ip solicitada 83.58.85.196 tiene su
origen en Logroño (España), c/ del Barriocepo nº 137 bis,
2 izq y la usuaria calza deportivas del 41. Si quiere
conocer su número telefónico y el saldo de su cuenta
corriente, por favor use la opción -t y -cc respectivamente.
Más información lacoñanet --help y páginas del manual.
```

Y lo habitual: Que puedan configurarse las opciones en `/etc/lacoñanetd.conf` y que para reiniciar el servicio: `/etc/init.d/lacoñanet force-reload` (que queda como de más "enterao" que un simple y vulgar "restart")

Como decía, este comando todavía no existe (aunque Hacienda está en ello). Existe "whois" que, aunque tampoco va por aquí la cosa, lo disimula muy bien:

```
$ whois 83.58.85.196
```

Tampoco existe la página que lo diga online aunque haya un montón que ofrece el servicio. Esta información sólo se consigue si tienes un amigo muy amigo que trabaje en Telefónica y que esté dispuesto a jugarse el puesto de trabajo por tí. Si eres un usuario normalito (lo cual no dudo puesto que estás perdiendo tu preciado tiempo leyendo este mal proyecto de tutonovela negrilla) y no tienes la intención de pasar un rato entretenido jugando al cracker (como es mi caso), no es necesario aptgetear traceroute y otras varias aplicaciones que pueden encontrarse recomendadas en las muchísimas páginas de aspecto oscuro y contenido oscurantista estilo fashion-new-edad-media que pululan por la red. O sea que, resumiendo, para intentar encontrar a mi vecina opté por el método tradicional: intentar averiguar algo en su lugar de trabajo, pero esto sería al día siguiente. Lo que quedaba de tarde (que era poco) me la pasaría jugando con bash, que es como masturbarse pero sin mancharse las manos.

Bash lo abarca todo. Es como la vida misma. Escribes un comando en el prompt y entras en sintonía con la máquina. Al comando le pones el encabezado y entras en sintonía con el universo. Con una silla, una piedra y un libro en un archivo de texto con la clásica primera línea y ya tienes toda la potencia en acción. O traducido para los que todavía no han sido infectados por el virus del prompt: Copias el `grep "Invalid user"` del principio del capítulo en un archivo de texto, lo precedes con un `#!/bin/bash`, le incorporas "awk" y algún "echo" (para darle un toque más aparente), lo llamas "asalto", le das permisos de ejecución (+x):

```
#!/bin/bash
echo Las ip y servicio usado de los que han intentado
asaltar el castillo son:
grep "Invalid user" /var/log/auth.log | awk '{print$5$10}'
```

Y lo lanzas (`./asalto`). Es como el "Hola mundo" pero sin tantas pretensiones. Continúa dándote las ips que han atacado tu pc y el servicio que han usado (en el caso de que hayas sufrido algún ataque) pero la belleza que desprende el script, cualquier script es bestial. Y para protegerse de los ataques, a menos que uno sea el responsable de seguridad informática de alguna empresa que cotice

CAPÍTULO 7. NADA EN LOS LOGS DEL DISCO DE MI VECINA

en el Nasdag 100 o de algún ministerio gubernamental, con fail2ban sobra. Esta aplicación actúa como cualquiera cuando le suena el móvil. Mira el número y este sí, este ni pensarlo, este ya puede ir llamando... Cuando uno consigue formar un todo con bash comprende que en GNU/Linux todo es terriblemente humano. En:

```
# nano /etc/fail2ban/jail.conf
```

Buscas la sección que quieres proteger y que tiene un aspecto:

```
[ssh]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 12000
```

Y sólo tocas los siguientes parámetros: enabled a true, que para algo lo queremos proteger; Si no has modificado el puerto en `/etc/ssh/sshd_config`, nada; maxretry indica los intentos de conexión fallidos que estás dispuesto a soportar hasta que se te hinchen los periféricos y bantime el tiempo en segundos que tardará en pasarte el cabreo. Resulta tan sumamente elemental que es como pretender explicar por qué, a la vista de un número, no has cogido el móvil.

Estaba usando el sdb clonado como si fuera mi propio disco. De vez en cuando no podía evitar volver a la tty7 (ctrl+alt+f7) y mirar alguna de sus fotos guardadas en "Imágenes". Antes de acostarme, miré, actuando casi por inercia, mi correo: ¡El kernel me dió un salto! Pero ¿qué era aquello? ¿una tomadura de pelo? ¿un mensaje del más allá? ¡Un mail de mi vecina! El cuerpo del texto solo tres palabras: "ayúdame por favor".

Capítulo 8

Smarteando el sdb de mi vecina

Durante la noche me levanté varias veces a releer el enigmático mail. Entré en su correo para comprobar que efectivamente había sido enviado desde allí. No entendía nada. Mi vecina estaba muerta. La había visto con mis propios ojos. Quizá los del GdV-bp querían hacerme enloquecer. Apuré el resto de una botella etiquetada como "vodka" pero de color verde césped y algo pastoso. Sin duda no era vodka pero tampoco podía precisar la naturaleza del mejunje aunque no era malo. Me fui a la tty3 «CTRL+ALT+F3». Las tty1-6 son mi refugio cuando todos los rincones de las "X" te recuerdan a alguien. Para distraerme, me bebí el último vaso con smart:

```
# apt-get install smartmontools
```

Comprobé si estaba activado (SMART support is: Enabled) con la opción "-i" y si no lo estaba activarlo con la opción "-s":

```
# smartctl -i -d ata /dev/sdb
(si el disco es ide se le quita el "-d ata")
# smartctl -s -d ata /dev/sdb
# smartctl -A -d ata /dev/sdb
```

Nada en WHEN_FAILED y el campo VALUE (un atributo interno de smart que va del 1 al 253, siendo 1 el peor resultado y los valores normales entre 100 y 200) algún aspecto por debajo de lo normal pero nada grave.

```
# smartctl -H -d ata /dev/sdb
```

El resultado del test fue PASSED. Era improbable un fallo del disco. ¿Las horas de vida cuantas podían ser?

```
# smartctl -l selftest -d ata /dev/sdb
```

Algo más de 5000 horas, nada. El disco estaba bien, era yo el que desde que empezó el asunto de mi vecina, sin dormir, cansado, sucio, mal comiendo y con la cabeza ardiendo, estaba necesitando un killall con hielo y unas gotitas de

angostura. Subí a la azotea. Todavía era noche cerrada (como las tty - pensé). Me senté en el suelo para aclarar ideas.

¿Que tenía? Mi vecina estaba muerta. O no... Tampoco le tomé el pulso. quedé petrificado en la puerta sin poder entrar en la habitación. Supuse que estaba muerta. ¡Qué imbécil! Igual todo lo supuse: el asesinato, la sangre... Ahora que recuerdo, el Subinspector Linares nunca mencionó nada sobre un crimen. Ni de un cadáver... Mi cabeza no podía más, iba a estallar en mil pedazos. Debía empezar nuevamente de cero y para ello, en mi cerebro hice mentalmente:

```
$ rm historia_de_mi_vecina
$ touch nueva_historia_de_mi_vecina
```

Esta vez empezaría bien y con premisas más solidas. Me puse en pie y levanté la cabeza para mirar cara a cara hacia la inmensidad de las tty. En mi interior edité el nuevo documento:

```
$ nano nueva_historia_de_mi_vecina
```

y mis neuronas teclearon en la primera linea del documento imaginario lo único que podía asegurar el éxito de mi misión:

```
#!/bin/bash
```

Empezaba a llover. Me aproximé al extremo de la azotea y levantando mis brazos al cielo grité con todas mis fuerzas hasta quedar exhausto:

- ¡Bash!, ¡Todo es bash!

Capítulo 9

Un ulimit que no está a la altura de la vecina

Cuando abrieron en el bar donde trabajaba mi vecina, yo hacía rato que aguardaba en la puerta. Había llovido con ganas durante toda la noche y estaba chorreando. La chica me sirvió un café con leche y una pasta. Le pregunté por mi vecina.

- ¿La conocías? - me preguntó.

- Bueno, nos acostamos juntos en alguna ocasión.

No tantas como hubiera deseado. En realidad solo fue un par de veces, pero en cada ocasión fue como si me hubieran lanzado un forkbomb que me agotó la totalidad de los recursos. Lanzas:

```
$ ulimit -u
```

Y si da un resultado de "ilimitado" o un valor extremadamente alto, puede ocurrirle al sistema lo que a mí con mi vecina. Para resolverlo podemos limitar el número de procesos abiertos para que estos no puedan llegar a colapsarlo:

```
# nano /etc/security/limits.conf
```

Y ponemos antes del "End of file":

```
* hard nproc 1000
```

Y los limitamos a 1000 que para una máquina está bien. Ojalá mi "ulimit" personal fuera 1000, bueno con 10 ya me conformaría, o 5, el caso es que no paso de 3 por mucho que modifique mi limits.conf y para terminar el tercero con éxito, uno tiene que sacar inspiración hasta del parpadeo de las lucecitas del router. Para acabar reiniciar ulimit, el de la máquina claro:

```
$ ulimit -a
```

- Los últimos días estaba radiante de alegría - prosiguió la chica de la barra - por lo visto había conocido a un chico... se deshacía por él y no se que decía de un velo en los ojos o, no se, algo relacionado con informática, o de ordenadores y pingüinos... en fin, no me hagas caso que yo, fuera del messenger y cuatro cositas, nada de nada. Oye, por casualidad ¿No serás tú el chico?

CAPÍTULO 9. UN ULIMIT QUE NO ESTÁ A LA ALTURA DE LA VECINA

¿Era yo el chico? ¿era yo el chico! tenía que serlo, quería serlo, ha dicho que se deshacía por mí, te quiero, te amo. Se me había puesto aquella cara de pamplinas tan característica porque cuando uno se enamora por muy bash scripting que sea se "imbeciliza" tanto como sin bash scripting. ¡Tengo que encontrarla! Tengo que decirle que la quiero más que a la tty4 ... quiero fundirme con ella:

```
$ cat tu yo >> tuyo
```

Pero, ¿por dónde empezar? Tenía que ver nuevamente al Profesor. Necesitaba datos, muchos datos y quizá él podría facilitármelos. Le di un beso y un fuerte abrazo.

- Me has ayudado mucho, te quiero.

Le decía mientras salía del bar. Corrí más que un dual core quad para llegar cuanto antes al apartamento del Profesor. Subí los peldaños de tres en tres.

- ¡Profesor! ¡Profesor!

Gritaba mientras tocaba el timbre insistentemente. Una vecina, ya mayor, del piso contiguo salió para ver qué era aquel escándalo. Le conté que tenía que ver urgentemente al Profesor, pero tras la puerta solo silencio. Mi euforia inicial fue convirtiéndose en pánico. La señora mayor me contó que siempre coincidían en la panadería de la esquina, pero aquella mañana el Profesor no apareció. Los balcones de los dos pisos no estaban muy separados y pude acceder al interior de la vivienda. La escena, muy parecida a la vista en casa de mi vecina: desorden, pintura roja por las paredes (que, tonto de mí, tomé por sangre) y el pc como si le hubiera pasado un trasatlántico por encima. Los autores eran, sin lugar a dudas, los GdV-bp y del Profesor ni rastro. Le dije a la anciana que llamara a la policía y le contara lo ocurrido al Subinspector Linares y yo me fui volando hacia mi casa. Entré y el espectáculo que vi era dantesco: todo revuelto y el pc hecho trizas. Los Blue Pántallaz venían a por mí. Me había salvado porque aquella noche...

- ¡Te hemos pillado escoria!

Sin darme cuenta, el armario de comisaria y un par de acompañantes habían entrado en mi apartamento y me habían inmovilizado.

- Confesarás, te juro que confesarás, pero antes de llevarte a comisaría nos divertiremos un poquito, ¿verdad muchachos?

El primer puñetazo en la boca del estómago me dolió una barbaridad pero me dejó k.o. y aunque me levantaron varias veces para continuar aporreándome ya no me enteré. Sangraba por la nariz y el labio y al ojo derecho no había forma de hacerle un mount.

- Venga, venga muchachos, que os lo vais a cargar...

El Subinspector Linares se había convertido en mi ángel de la guarda, pero en esta ocasión, con diez minutos de retraso. Me ayudó a levantar.

- ¿Como está nuestro Linux?

- GNU/Linux.

Dije balbuceando, soltando grumos de sangre por la boca y casi de forma inaudible.

- Deja que te vea.

- Siento no poder decir lo mismo...

- No morirás de esta.

- De nuevo el profeta. Me da una alegría.

CAPÍTULO 9. UN ULIMIT QUE NO ESTÁ A LA ALTURA DE LA VECINA

- Te aconsejo que cambies temporalmente de domicilio. ¿Te llevo a alguna parte?

- No se. Gracias. Al bar donde trabajaba mi vecina. ¿Puedo preguntarle? ¿Está viva?

- Muy probable, pero dejanos esto a nosotros y no quieras jugar a los detectives. Procura descansar. Mis muchachos, que a veces tienen unos métodos demasiado expeditivos, y yo tenemos tanto interés como tú en resolver este caso.

Me dejó en el bar. Era primera hora de la tarde y no estaba muy concurrido. Cuando la chica de la barra vio mi estado vino corriendo y me acompañó a una especie como de reservado, pero pude observar como un hombre de mediana edad que también estaba detrás de la barra y que por su aspecto podría ser el dueño, no puso buena cara

- En media hora termino mi turno. - dijo.

Desmontado como estaba, solo podía salvar mis errores de disco un:

```
# fsck.ext3 -vpf /dev/yo
```

*CAPÍTULO 9. UN ULIMIT QUE NO ESTÁ A LA ALTURA DE LA
VECINA*

Capítulo 10

Cerrar puertos de la amiga de la vecina

Me desperté en una cama desconocida completamente desnudo. Recuerdo que salimos juntos del bar y subimos a un coche, pero a partir de este punto, los recuerdos se espesan. El reloj de la mesita marcaba más de las dos de la tarde. Llevaba durmiendo un montón de horas. Fui al aseo. Del espejo colgaba una nota de la chica: "Buenos días pendejo, he ido a trabajar. En la cocina encontraras algo de comer. Tu ropa está en el tendedero y espero que seca, sino, busca algo mío en el armario. Vuelvo a las tres". Me duché. Cuando me miré en el espejo, pude observar que mi aspecto facial era penoso pero al menos andaba, dolorido, pero casi normal. Me vestí; mi ropa estaba seca y me ahorré hurgar en sus trapitos. Me comí unas galletas integrales que encontré en un bote de la cocina y mientras, di una vuelta por el apartamento. Era pequeño, muy pequeño, pero para una persona sola o una pareja muy, muy, muy enamorada, más que suficiente. En el cuarto libre, en medio de montones de cosas perfectamente colocadas y medio oculto por unas cajas, un ordenador con el espacio justo para trabajar con él. Tenía el clásico salvapantallas de las banderitas del logo activadas, su mera visión casi me echa a perder el ojo que me quedaba. De repente me acordé del lápiz. Lo busqué en los bolsillos y me asaltó la terrible visión de verlo formateado en la lavadora con Ariel automáticas.

- ¿Buscas esto?

¡Mi lápiz!

- Es que sin él me encuentro desnudo.

- ¿A sí?

De la forma que dijo aquel "¿A sí?" y la media sonrisa que esbozó su cara deduje que, a la vista de como había dormido, el símil no era el más apropiado.

- He traído del bar tortilla de patatas y un reserva Marques de Paparrucha del 2006

Mi otra debilidad (la tortilla, no el reserva) junto con el sexo y las tty1-6 (sin precisar el orden). Nos sentamos a comer y empezamos a hablar. O mejor, empecé mi monólogo. Le conté que mi amigo, no visible .(punto)Antúnez, mucho antes de meterse con C++ decía que haciendo chorradas uno va entrando en la lógica de la programación. Uno de sus primeros y más impresionantes scripts que nos tubo a todos anonadados mucho tiempo era:

```
#!/bin/bash
#
clear nombre='who | grep tty7 | awk '{print $1}''
hora='date +%H:%M'
sleep 2s
echo
Hora=$(date +%H)
case $Hora in
  0? | 1[01]) echo ";Buenos días! $nombre la hora es
$hora de la mañana"
;;
  1[2-7] ) echo ";Buenas tardes! $nombre la hora es
$hora de la tarde"
;;
  * ) echo ";Buenas noches! $nombre la hora es $hora
de la noche"
;;
esac
echo
echo "y el listado de archivos y directorios de tu carpeta
en la que te encuentras es:"
ls
```

Que, como deja muy claro la última línea, viene a ser como un "ls" pero sin tanta amabilidad. (punto) Antúnez decía que cuando uno consigue hacer unos cuantos cientos de scripts inútiles debería de haber obtenido suficientes conocimientos como para ofrecerse voluntario para terminar de una vez el núcleo HURD (para los muy valientes: <http://ftp.debian-ports.org/debian-cd/K16/>). Ella escuchaba y de vez en cuando decía "¿A sí?, ¿case qué?, ¡no me digas!" pero estaba claro que no tenía ni repajotera idea de lo que le hablaba, lo único que quería era acostarse conmigo y enseñarme python.

- ¿Sabes que para conocer los puertos abiertos y los servicios que corren en ellos basta con... ?

```
# apt-get install nmap
# nmap -O localhost | grep "open"
```

- Y con esto ¿sabes los puertos abiertos?

A saber en qué puertos pensaba o, mejor dicho, tenía la certeza absoluta de en qué puertos pensaba, pero yo, entre sorbo y sorbo del reserva Marqués de Paparrucha, proseguía impasible:

- También podemos hacer un pequeño script y lanzarlo como root:

```
#!/bin/bash
echo "Los puertos y servicios que tienes abiertos son: "
echo
nmap -O localhost | grep "open" | awk '{print$1,$3}'
echo
```

Y así solo tendremos que teclear ./puertos o también lo podemos poner como alias, pero no así:

CAPÍTULO 10. CERRAR PUERTOS DE LA AMIGA DE LA VECINA

```
$ alias puertos='sudo nmap -O localhost | grep "open"'
$ puertos
```

Porque esto durará menos que el último trozo de tortilla de patatas, sino directamente en el archivo `.bashrc` en el apartado de los alias:

```
$ nano .bashrc
```

Y le encasquetas: `alias puertos='sudo nmap -O localhost | grep "open"'`

Y si cuando lo ejecutas (`# puertos`) te dice "command not found", "hacer releer" bash:

```
$ source .bashrc
```

- Y... ¿Qué podemos hacer con los puertos abiertos?

Dijo apoyando su cabeza por la barbilla con su mano. Yo desgañitándome por explicarle una profundísima filosofía de la vida y ella, con la boquita de piñón preguntando que "qué podíamos hacer con los puertos abiertos". Llegué a pensar que la chica que tenia delante era una Guerrillera del Ventanuco. Por esto y por el intento de asesinato por ingestión del Marqués de Paparrucha del 2006 que más que reserva debía ser un "veinte años y un día" porque era condenadamente malo.

- Bueno si queremos cerrar uno y desconocemos la aplicación (o demonio) que corre en él:

```
# fuser -n tcp puerto
```

Te da el PID, luego:

```
# ps -l PID
```

Te muestra la aplicación, concretamente la ruta al ejecutable y luego puedes pararla de un montón de formas antes de usar el mazo del 5 y la botella de ácido. Algunas a lo fino

```
# /etc/init.d/aplicación stop
```

O a lo pedreste:

```
# fuser -nk tcp puerto
# killall servicio
# kill -9 PID
```

Escoger cada cual según el temperamento. Y si no se consigue de ninguna manera, ahora ya sí, el mazo y la botella de ácido.

- Así que...¿Demonio? ... ¿Kill?... ¿Matar?....

Madre mía, madre mía, si la mato... y a golpes de ntop, que uno, aunque tenga voluntad de hierro, no ha nacido ni de piedra ni con vocación de santo, y, con el tiempo que llevo sin darle al cupsys, se te pone por delante una noble doncella que, como dice el poeta, poco de noble y menos de doncella y con un iptables que desconoce la política DROP puedes terminar montando una intranet de lo más gratificante.

CAPÍTULO 10. CERRAR PUERTOS DE LA AMIGA DE LA VECINA

Capítulo 11

Intento olvidar a la vecina y me voy de vacaciones

Un amigo, cuyos padres tenían un apartamento en la costa, me había invitado, con otro par de colegas, a pasar unos días en la playa. Podría desconectar del asunto de mi vecina. Cuando uno no sabe por donde tirar es bueno e incluso aconsejable realizar un alto en el camino. Mi amiga del bar, que hacía un par de días había empezado sus vacaciones, se iba a tirar un mes en casa de unos parientes en un pueblo de Extremadura. Por suerte para mi pobre cuerpo me había ofrecido alojamiento en su casa mientras mi vida corriera peligro (y la corría, caray si la corría). Me costó mucho convencerla, y eso que yo en estos temas soy muy ducho, para que me dejara instalar, junto a su amado güindous, otro sistema más divertido. Transigió, pero me hizo jurar con mi mano derecha encima de la pantalla del messenger (que poco faltó para que me borrara las huellas digitales) que si algo le ocurría a su sistema me convertiría a una secta animista y jugaría con ella al tu te deborphan y yo te la finger durante una semana. Dudé entre pasar directamente a:

```
# mkfs -t ext3 /dev/sda1
```

O instalar un GNU/Linux. Me incliné por lo segundo (En mi vida siempre he escogido el camino equivocado).

Antes de partir debía preparar algunas cosillas básicas en el pc: cambiar el puerto ssh del 22 a uno menos usual:

```
# nano /etc/ssh/sshd.config
```

En <http://www.iana.org/assignments/port-numbers> buscar uno libre y:

```
Port 40500
```

Guardar y reiniciar servicio (`# /etc/init.d/ssh restart`)

Redireccionar los puertos 40500 (ssh) y 5900 (vnc) en el router para que apunten a la 192.168.1.2 (la única en esta triste y escuálida red) y abrir los mismos puertos en el cortafuegos:

```
# apt-get install ufw
# ufw allow 40500
# ufw allow 5900
# /etc/init.d/ufw restart
```

Preparar la máquina para que las X chuten viento en popa en caso de que, donde íbamos, el ancho de banda fuera tercermundista, cosa más que probable porque ya en mi ciudad lo es....

```
# apt-get install tightvncserver
```

Iniciar sesión:

```
# tightvncserver -depth 16 -geometry 640x480
```

Terminados los arreglos elementales, tocaba el turno a la prevención de posibles catástrofes; que si se interrumpía el flujo eléctrico, se pudiese arrancar la máquina desde la playa. Los pcs modernos, con fuentes de alimentación ATX y con la tarjeta de red integrada vienen con el wake-on-lan (wol) activado (Enable) desde la bios (en power management setup -> power on by ring) Si no está integrada se deberá conectar la tarjeta con un cable a la placa (a googlear toca. Para empezar: http://es.wikipedia.org/wiki/Wake_on_LAN) Si la fuente de alimentación es antigua (una AT) olvidarse del asunto porque ni GNU/Linux hace milagros (Si los dioses sueltan el código, tal vez)

```
# apt-get install ethtool wakeonlan
# ifconfig (apuntamos la red y la MAC)
```

Comprobar si el driver de la tarjeta tiene soporte WOL.

```
$ ethtool eth0
```

Si en el apartado "Wake-on:" pone una "g" indica activado si sale una "d" inactivo. Para activarlo:

```
# ethtool -s eth0 wol g
# ethtool eth0
```

Vemos la "g" pero de poco nos servirá si se para el pc porque esto solo afecta a la presente sesión. Si no lo hemos modificado en la bios (por gandules, porque no nos aclaramos, no encontramos el wake on lan de las narices o porque nos gusta más bash) toca, como no, un bonito y simple script:

```
#!/bin/bash ethtool -s eth0 wol g exit
```

Guardar como wolinit (p.e.), darle permisos (# chmod +x wolinit) y:

```
# mv wolinit /etc/init.d/
```

Al pararse el ordenador, la tarjeta de red vuelve a poner Wake-on en disabled (siempre que no se haya modificado la bios). Esto se soluciona haciendo que el script se ejecute en el runlevel 0 (cuando se apaga la joya) y ya puestos lo ponemos en todos los runlevel:

CAPÍTULO 11. INTENTO OLVIDAR A LA VECINA Y ME VOY DE VACACIONES

```
# update-rc.d -f wolinit defaults
```

Aunque un rayo exterminador desintegrara el repetidor de la compañía eléctrica, mi cordón umbilical permanecería conectado a la máquina lanzando desde cualquier pc:

```
$ wakeonlan -i nombre_de_host.com numero_MAC
```

Arrancaría el ordenador de mi amiga. Llené una bolsa con las cuatro cosas imprescindibles, sin olvidar unos live y el lápiz (nunca sabe uno qué se va a encontrar por ahí fuera) y salí. Habíamos quedado en el bar de una plaza céntrica para recogerme. Era temprano y tenía tiempo de sentarme a tomar una caña y abandonarme a mis pensamientos:

¡Qué jugada la del amigo Billy! En algunos casos cuando se redimensiona el Vista con un gparted como tradicionalmente se hacía con el XP, a tomar por el ripperx (# apt-get install ripperx) el sistema del ventanas, eso en el caso de que pueda llegar a hacerse porque, en algunas ocasiones, es muy probable que ni nos lo permita, pero sólo con intentarlo, mismo resultado y luego, ¡toma! a recuperar el sistema con el repelús que esto produce. La forma más segura de hacerlo (en el caso de que lo que se busque no sea mandarlo a paseo que sería lo civilizado), sin que se inmute el enemigo, es redimensionando desde el propio Vista. Muy importante cuando se va a manipular productos altamente tóxicos: Usar guantes de látex (previenen muy bien la urticaria), mascarilla (protección contra virus, bacterias y hongos) y gafas de seguridad (riesgo de posibles pantallazos varios). Arrancas la cosa y Panel de control, Sistema y mantenimiento, Herramientas administrativas, Crear y formatear particiones del disco duro, seleccionas algo llamado C (para los que desconocen este pintoresco sistema equivaldría al sda1) y con el botón derecho, reducir volumen. Te dará el máximo que puede reducirse. Se acepta el máximo y descartas aumentarlo si no quieres liarla. Cuando termine, salir, reiniciar con el live/install y proceder como es habitual instalando el GNU/Linux de tu elección en el espacio vacío. Para hacerlo desde un sistema normal y sin causar ningún estropicio, necesitamos un live o un lápiz con la herramienta ntfsprogs (puppy, parted magic ...).

Estaba ensimismado con mis cavilaciones, cuando por el otro lado de la calle vi pasar a alguien vagamente conocido. No había duda, algo desmejorado pero se trataba de .(punto)Antúnez. Me levanté de un salto y corrí hacia él.

- ¡Antúnez!
- ¿?
- ¡Si hombre! las clases con el Profesor, ¿ya no te acuerdas de los viejos amigos?
- Perdona, así a primera vista...
- ¡Cuánto tiempo sin verte!
- Sí... es que ando muy ocupado. ¿Sabes? Yo... inicio, programas...
- ¿Inicio, programas...? Sí... Sí claro... Inicio, programas... Veo que andas muy estresado, ¿no?

Mientras, habían llegado los que venían a recogerme y me estaban pegando voces desde el coche.

- ¡Venga que hacemos tarde!
- Tengo un poco de prisa. Nos veremos - dijo .(punto)Antúnez.
- Si, tengo que hablar contigo. ¿Cómo te localizo? ¿vives en el mismo antro?

*CAPÍTULO 11. INTENTO OLVIDAR A LA VECINA Y ME VOY DE
VACACIONES*

Los del coche insistían con mucho alboroto en que subiera y .(punto)Antúnez se iba en dirección opuesta y paso acelerado.

- Sí, sí... Nos vemos. - dijo mientras desaparecía por la esquina.

Subí al coche, todo un clásico. Seguro que ya corría antes de empezar el diseño del tercer cinturón. En el interior del habitáculo, la juerga era impresionante. Aparté las latas vacías de cerveza, me acomodé como pude entre el equipaje y me uní al jolgorio. Enfilamos rumbo a la costa, eso si no nos pillaban los de tráfico porque entonces directos al trullo.

Capítulo 12

Como extraviar un pc en la playa y un mail de la vecina

El mar es fantástico. Para mi el verano no es la mejor época, pero continúa siendo fantástico. Desde el apartamento no podía verse el agua, aunque no estaba lejos, pero habían suplido el detalle pintando un mar con oleaje, un barquito y peces de colores en el muro del edificio vecino que daba una sensación muy cutre-acuática. Dejamos el equipaje por allí tirado y, desde aquel momento hasta cuatro o cinco días más tarde, no me quedan más que pequeños recuerdos de lo ocurrido. Verano y playa es una mezcla explosiva propensa a que pasen estas cosas. Con la cabeza retumbando, abrí los ojos con gran esfuerzo. Clareaba. El apartamento era un conjunto de cuerpos entrelazados indicativos de los restos del naufragio de la última fiesta. Me quité de encima a una chica que tampoco recordaba de nada, cogí mi bolsa, que uno usaba de almohada y me vestí. En el suelo, entre vasos y botellas vacías había un portátil, cuyo dueño, supongo, no echaría en falta en un par de horas. Me fui a la playa y, como que en la parte frontal lucía el logo del Vista, no quise arriesgarme y lo boteé directamente con el lápiz. Aprovechando que estaba un poco espeso, me dije: "Vamos a jugar un rato, le instalaré un sistema civilizado y así pruebo si funciona el ntfsprogs del parted magic".

```
# fdisk -l | grep NTFS
```

Averiguamos la partición contaminada, pero en fondo como somos buenas personas, le hacemos el favor de repararle los posibles errores:

```
# ntfsfix /dev/sda1
```

Cuando termina, pasamos al ataque. Comprobamos que la partición ha sido correctamente detectada y el mínimo espacio que necesita, aunque Vista siempre quiere un trozo más (es muy señorito):

```
# ntfsresize -P -i -f -v /dev/sda1 --ad-sectors
```

Nos dirá varias cosas y entre ellas algo como:

```
... You might resize al 37828673100 bytes or 37829 MB (freeing 43780 MB).
```

Como queda claro, 37829 es el espacio mínimo del Güindous y 43780 el espacio que puede dejar libre. Probamos, en una simulación (parámetro -n) a dejarle 5 GB más de la cifra que nos ha dado:

```
# ntfsresize -f -s 4200000000 -n /dev/sda1 --bad-sectors
```

ERROR:..... Please try to free less space.

El muy zorrón quiere más. Haré más simulaciones hasta que diga:

Updating Boot record test run ended successfully.

Y, ya para hacerlo efectivo, quito el parámetro -n:

```
# ntfsresize -f -s 4300000000 /dev/sda1 --bad-sectors
```

... Successfully resized NTFS on device '/dev/sda1'.

Luego en el trozo libre le instalo de la forma habitual, cualquier distro sencilla para el usuario (Gentoo, Arch, Slackware ...) con lo que se consigue, por un lado, un nuevo ordenata en la galaxia GNU/Linux y, por otro, un enemigo para el resto de su vida. Antes de apagar la máquina un vistazo al correo. Varias cosas y entre ellas, un mail de mi vecina. El texto, un enlace.

- ¿Usuario y contraseña?

Seguido de un texto para descubrir el mensaje a modo de jeroglífico. Absorto como estaba pensando en como acceder a la cuenta y releendo el proceso, no me apercibí de que cuatro barbudos con uniforme caqui se me acercaban, golpeaban en la cabeza y me introducían en una furgoneta.

Cuando volví en mí, sin saber el tiempo que había transcurrido, me encontraba maniatado, con un saco cubriéndome la cabeza y una tira adhesiva en la boca. Les oía muy levemente sin entender sus palabras pero el acento era sudamericano. Al cabo de mucho rato pero todavía de día, llegamos a nuestro destino. Me llevaron a una habitación y me quitaron el saco:

- Queremos hacerte algunas preguntas.

- Espero que sobre GNU/Linux y justito pero de los demás...

- Eso lo veremos.

Me dejaron solo. Por una ventana con barrotes se podía apreciar que me encontraba en un campamento en el bosque y se veían muchos barbudos con uniforme caqui yendo de acá para allá.

Parece que estoy en Cuba... No, no puede ser Cuba. ¿Cómo va a ser Cuba si esto es un pinar? Claro que tampoco sé si en Cuba hay pinares... Esto como mucho es Sierra Morena... Pero, ¿qué hacen todos estos barbudos en Sierra Morena? No parecen maquis extraviados de la guerra civil... ni de la banda de Curro Jiménez...

Entró un grupo con uniforme de campaña y fuertemente armados que me rodearon. Pasaron algunos segundos y entró otro barbudo.

- ¡El Comandante Vargas! - Gritó uno. Extendí la mano para saludarlo.

- Mucho gusto. Verá ...

- ¡Silencio!

- Eres un infiltrado del expresidente Mendoza, ¡confiesa!

- ¿Mendoza?, no tengo el placer de cono...

- ¡Silencio! Te vimos hablando con uno de sus agentes. Firma tu confesión... mañana volveremos.

CAPÍTULO 12. COMO EXTRAVIAR UN PC EN LA PLAYA Y UN MAIL DE LA VECINA

Dejaron boli y papel en la mesa y se fueron. ¿Me vieron con un agente del expresidente Mendoza? ¿El comandante Vargas? ¿Pero dónde me había metido? Recuerdo una noticia aparecida en la prensa de hace unos meses, que en un país latinoamericano hubo un golpe de estado. Si claro, tenía que ser aquello. A ver si podía recordar algo más. Solo leí los titulares porque la noticia no me interesaba lo más mínimo. Sí, sí, el presidente Mendoza había sido derrocado; claro, por el Comandante Vargas que gobernó por unas cuantas semanas y a su vez, fue derrocado por los seguidores del antiguo presidente y entre derrocado y contraderrocado las arcas estatales se esfumaron. ¿Y el agente? ¿la chica del bar? ¿.(punto)Antúnez? ¿Mi amigo del apartamento de la playa? ¿Los de la juerga en el "clásico"? El agotamiento pudo conmigo y me quedé dormido.

*CAPÍTULO 12. COMO EXTRAVIAR UN PC EN LA PLAYA Y UN MAIL
DE LA VECINA*

Capítulo 13

Como acceder al contenido del mensaje de mi vecina

Me despertaron unos gritos de afuera. En la cabeza me daba vueltas el texto del mail de mi vecina:

"Entra en <http://www.fileupyours.com>¹ (usuario y contraseña, el que una vez me pusiste), bajas el paquete y

```
# apt-get install p7zip p7zip-full p7zip-rar
```

lo abres con el nombre del usuario que en el 7º capítulo postea el comentario "lost in de comentarios"². Craqueas el pdf,

```
# apt-get install pdftcrack
$ pdftcrack archivo.pdf -n 6 -c abcdefghijklmnopqrstuvwxyz -s
```

copias el texto del pdf a un documento de texto llamado encriptado.txt y

```
$ openssl aes-256-cbc -d -a -in encriptado.txt -out
desencriptado.txt
```

con el nombre (en minúsculas) de uno de los exalumnos por los que se interesa el Profesor.

```
$ cat desencriptado.txt
```

No resistiré mucho"

La puerta se abrió y entró una anciana con una perola de fabes que olía de maravilla. Detrás suyo el vigilante armado no nos quitaba ojo de encima. Con la cabeza gacha y cubierta con una capucha me acercó la perola.

- A hora tan temprana hubiera preferido un café con leche y una pasta pero se agradece el detalle.

Levantó un poco la cara. ¡Por todos los fdisk -l ! ¡Si era la amiga de mi vecina! Con un rápido movimiento se giró y le arrojó el contenido de la perola

¹Nota.- Por favor, no borrar el archivo de fileupyours.com para permitir, al que quiera, jugar un rato.

²El enlace es: <http://www.tuxapuntos.com/drupal/node/1516>. Ver Epílogo.

a la cara del guardia y al momento, un puntapié en los hostname que me dolió hasta a mi.

- ¡Lastima de fabada!
- ¡Más lastima de hostnames!

En un momento se despojó de los harapos con los que se había disfrazado y se quedó con camiseta "albañil" y tejanos que le sentaban de miedo. Alargó su mano y agarrándome por la nuca con un fuerte movimiento, acercó mi cabeza a la suya hasta unir nuestros labios.

- ¡Venga, venga tonto! No tenemos tiempo que perder...

Mientras huíamos, agazapados con todo lo que se nos ponía por delante, alguien descubrió mi ausencia y dio la alarma. El campamento era un hervidero de uniformados corriendo por todas partes. De vez en cuando se escuchaba una ráfaga de ametralladora que te ponía los bzips por zarcillos.

- Además de matar procesos según se conozca el PID, el puerto o la aplicación, también puede matarse conociendo sus atributos o características. Si alguien se conecta a nuestro pc por ssh y queremos echarle:

```
# netstat -pnat | grep ESTABLISHED tcp 0 0 346 192.168.2.3:22
69.64.155.119:65733 ESTABLISHED 13802/sshd: impostor
```

Nos dice el puerto (22) y el proceso (13802) que ya sabes como matarlos, pero con:

```
# who ... impostor pts/4 2009-07-27 18:44 ....
```

Nos indica la terminal que está corriendo el impostor: pts/4 que es como se conocen las terminales que se abren en la "X" las otras son las tty1-6.

- Así que... Corriendo el impostor...

No hice caso de la observación, al fin y al cabo el problema de aquella chica era que se confundía con las conjugaciones verbales; Cualquiera sabe que no es lo mismo "intentar salir corriendo" en gerundio que "intentar salir..." en participio.

```
# pkill -9 -t pts/4
```

Y el amigo "impostor" verá en su pantalla: Connection to 192.168.2.3 closed (traducción: A tomar por el cdrecord)

Había tal cantidad de uniformados buscándome que era una temeridad salir del escondite en el que estamos.

- Veamos. Como podemos arreglar lo del... pkillpts4...

Dijo de aquella forma tan sensual que hacía añicos cualquier fail2ban que se le pusiera por delante y mientras, se acomodaba en unos sacos y se quitaba la camiseta dejando sus pts en grep LISTEN:

- Tendremos que esperar a que anochezca. ¿Se te ocurre algo para entretenernos?

Suerte que me daba pistas porqué sino ni se me habría ocurrido. Iniciamos clase de python en & (background). Espero que no nos pillen a medio proceso y nos hagan un pkill -9. Y aquella noche salí "en participio".

Capítulo 14

Nos salvamos gracias a cups

Llegó la noche y con ella la calma en el campamento. La amiga de mi vecina salió para ver como estaba el patio: Los centinelas lejos y algunas risas de los barracones. Vía libre, me hizo un gesto para que la siguiera. Estábamos avanzando ya fuera de la zona de control miliciano cuando noté en la nuca algo parecido a un cañón de pistola.

- ¡Quietos o te reviento la sesera!

Ni parpadeamos.

- Daros la vuelta pero muy, muy despacio y las manos que las vea.

Hicimoslo.

- ¡Linux! ¿Qué diantre hacéis aquí?

- ¡Subinspector Linares! ¿Y usted?

De sorprendido ni puntualicé lo de GNU...

- Por lo que veo, viejos amigos... ¿No será éste aquel mamonazo que me dijiste que siempre te estaba tocando los cups?

La fulminé con la mirada. El Subinspector apretó los dientes y diríase que iba a darle al gatillo. Cerré los ojos y me encogí de hombros. No sé por que se hacen estas cosas cuando uno se espera un disparo en la nuca, será para que duela menos... Pero rápidamente reaccioné:

- No, lo entendiste mal, yo lo que te dije fue que para configurar una impresora en una red local con cups, en el pc al que está conectada (el servidor) sólo tienes que:

```
# gedit /etc/cups/cupsd.conf
```

Comentar la línea que dice "Listen localhost:631" sustituyéndola por "Listen 192.168.2.3:631" y poniendo el "Browsing off" en "on" y claro, reiniciar:

```
# /etc/init.d/cups restart
```

- Y en las máquinas cliente... ¿Qué? A ver... (dijo el Subinspector Linares)

- ¡Hombre, elemental querido Linares! Pues edit.

¡El Subinspector vacilando sobre los pcs clientes! Me lo quedé mirando, sorprendido.

- No pensarás que eres el único usuario de GNU, ¿verdad? En cada máquina de la red editas:

```
# gedit /etc/cups/cupsd.conf
```

- Y también pones el "Browsing off" a "on" y en "BrowseAllow 192.168.2.0/24" para que la use toda la red y reinicias el servicio.

Le mirábamos anonadados y, aunque continuaba apuntándonos, no sé por qué, el Subinspector Linares empezaba a caerme bien.

- Luego vas a la máquina donde está conectada la impresora pones

```
http://localhost:631
```

te logueas, vas a la pestaña "printers" seleccionas la impresora y en la barra del navegador tendrás algo así como:

```
http://localhost:631/printers/nombre_de_la_impresora
```

- Sustituyes "localhost" por la ip local (192.168.x.x) de la máquina a la que está conectada y ya tienes la URI del dispositivo, que es el que tienes que poner en todas las configuraciones de los clientes, ya sea por "impresoras" o por `http://localhost:631 (cups)` aunque mejor acostumbrarse a usar cups porque es independiente del escritorio que se use.

Irrumpimos en un estruendoso aplauso.

- ¡Bravo! ¡bravo!

- Sssshhh queréis que nos descubran los milicianos. Mis hombres están apostados por allí, mejor que os larguéis por el otro lado. ¡Linux!

Dijo, levantando su índice hasta escasos milímetros de mi espalón.

- Llévate a tu amiguita lejos y no quiero verte más jugando a detectives.

- No, si yo no jugaba, resulta que estaba en la pla...

- ¡Fuera de mi vista!

Dimos unos pasos y me giré:

- Y si la impresora necesita drivers especiales, ¿Los tienes que instalar en todas las máquinas de la red?

- ¡No! Sólo en la que actúa de servidor. ¡Largo!

Salimos pintado en la dirección que nos había indicado. Estábamos bordeando el campamento protegidos por la maleza cuando nos topamos con un "jeep Willys" y dado que la amiga de mi vecina no recordaba por donde había dejado su vehículo optamos por el "Willys". Subimos. Mi "amiguita", como la definió el Subinspector, manipuló los cables hasta ponerlo en marcha mientras yo, a falta de sacacorchos, hundía el tapón de una botella de un blanco Viña Farruco que encontré en la guantera. Nos largamos a toda velocidad. Aquella chica conduce de infarto. Y más chupando del gollete del Viña Farruco...

Capítulo 15

Juan el Destripador

Fuimos directamente a su apartamento. Por lo visto se aburría en el pueblo de sus ancestros, regresó, se enteró de que nos habíamos ido a la costa a casa de un amigo y se dirigió hacia allí, me vio en la playa y quiso darme una sorpresa pero la sorpresa me la dieron los hombres del comandante Vargas, les siguió y el resto es conocido. Dado que todavía le quedaban un montón de días de vacaciones se ofreció voluntaria para ayudarme a encontrar a mi vecina. Acostarse con alguien que usa el Messenger tiene un pase, pero trabajar codo con codo con ella requiere poner en marcha un curso acelerado de GNU. Nos encerramos dos días en el apartamento, alternando las tty con python. En una de las pausas para reponer fuerzas le conté mi visión cosmológica: que GNU en realidad quiere decir "GNU is not a frigid users" con la "f" en consola virtual lo que explica nuestras ganas de guerrear; que ha hecho muchos más nuevos usuarios HAL (simplificando: el automontador automático de dispositivos) que cuarenta mil líneas de código del kernel y que los G-Linuxeros tenemos ciertas tendencias patológicas a creernos los últimos descendientes de una caballería espiritual de la edad media cuya misión capital es la custodia del Santo Grial versión apócrifa y GPL.

También le conté que:

```
# apt-get install john
```

Luego vas a <http://md5encryption.com/> y pones a encriptar alguna palabra fácil de desencriptar para el amigo john, por ejemplo "adas". El hash MD5 lo pones en un archivo de texto con formato: Nombre, dos puntos y el numeraco:

```
churras:09726305e74bab5e09c9d6c9672e6085
```

Se guarda como "nada" y lanzamos al prenda para comprobar si nos pilla la contraseña:

```
# john nada
```

Si en un abrir y cerrar de ojos, john te ha resuelto la papeleta: ¡bingo! En caso contrario, no has instalado john de Ripper si no el magnífico sucedáneo Juanito el Mariposón, que viene a ser como el otro pero sin algunos parches, por tanto:

```
$ mkdir john
```

```
$ cd john
$ wget http://www.openwall.com/john/f/john-1.7.2.tar.bz2
$ bunzip2 john-1.7.2.tar.bz2
$ tar -xvf john-1.7.2.tar
```

Bajar y aplicar el parche:

```
$ cd john-1.7.2
$ wget ftp://ftp.openwall.com/pub/projects/john/contrib
/john-1.7-rawmd5-ipb2-4...
$ gzip -d john-1.7-rawmd5-ipb2-4.diff.gz $ patch -p1 <
john-1.7-rawmd5-ipb2-4.diff
```

Y compilar:

```
$ cd src
$ make
```

Para optimizar john escoger la arquitectura de la máquina:

```
$ uname -m
```

Y para comprobar si la cpu tiene soporte sse2:

```
$ cat /proc/cpuinfo | grep sse2
```

En caso de desconocerla o de que el comando anterior, probando con distintas opciones, no arroje información siempre nos queda el "generic"

```
$ make ARQUITECTURA
```

Y volvemos a probar:

```
$ cd ..
$ cd run
$ ./john /home/usuario/nada
```

Pueden consultarse otros parches en <ftp://ftp.openwall.com/pub/projects/john/contrib> procediendo de la misma manera que con el rawmd5 y asegurándonos que son para la versión de john-1.7 si no el pobre y desconsolado john nos quedará tiritando. En tal caso volvéis a empezar de cero, no ripeareis muchas contraseñas pero al menos se pierde el miedo a parchear una aplicación.

Al tercer día de encierro, salimos temprano. Si alguien podía ser la clave en la desaparición de mi vecina éste era .(punto)Antúnez. Vivía en un antro de un barrio marginal de la afueras, en el que, en los años estudiantiles, organizábamos charlas filosóficas sobre software libre, programación y lo cercano que estaba el triunfo de nuestras posiciones (que a saber cuales eran las de cada cual). En realidad lo único que buscábamos era acostarnos con alguna chica que tuviera su software tan libre como el nuestro. Cuando salió .(punto)Antúnez, le seguimos discretamente a cierta distancia. Se dirigió a un gran edificio del pulmón económico de la ciudad y entró. Destacaba un gran cartel con el nombre "Group V Insurance Company". Para entrar en el recinto, previamente debía de

teclearse algo. Me acordé del jeroglífico del mensaje de mi vecina, y dio resultado. Seguimos a .(punto)Antúnez por pasillos y escaleras hasta que lo perdimos en algún lugar de la 7 planta. Entonces le dije a la amiga de mi vecina:

- Para desencriptar contraseñas, tú, que eres más sofisticada, puedes emplear la mini suite Pentbox (<http://www.pentbox.net/download-pentbox/>)

- Déjate de desencriptaciones que hemos perdido al pavo.

Intentamos abrir algunas puertas pero, o estaban cerradas o daban a oficinas ocupadas por diligentes trabajadores que ni se inmutaban por nuestra irrupción. Hacia el final de pasillo, una se abrió. Parecía una habitación, donde reinaba un gran desorden, dedicada a almacén y con una pequeña sala contigua. Entre archivadores, mesas y sillas y demás material en desuso había varios ordenadores.

- Esperemos que alguno funcione...

Capítulo 16

Nos acercamos a la vecina con dsniff

Mientras ella vigilaba yo había boteado mi lápiz, esta vez con BackTrack (<http://www.remote-exploit.org/cgi-bin/fileget?versión=bt3-usb>) las herramientas que necesitaba eran, digamos que más informales y aunque todas están en esta formidable distro (<https://wiki.remote-exploit.org/backtrack/wiki/Alphabetical>) en este capítulo se actuará como si se instalaran en el HD. Primero, qué menos que conocer la ip de mi improvisado equipo :

```
# ifconfig
```

Y ver las máquinas que hay en la red en la que me encuentro:

```
# nmap -sP 192.168.1.0/24
```

Bajo e instalo arp-sk-0.0.16.tgz (<http://sid.rstack.org/arp-sk/>) junto con libnet1 y el paquete que nos va a permitir husmear por la red para intentar descubrir datos del paradero de mi vecina.

```
# apt-get install dsniff
```

Activo forwarding para que los paquetes vayan a sus verdaderos destinatarios:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Y lanzo arpspoof para redirigir los paquetes del router a la máquina atacada y viceversa:

```
# arpspoof -i eth0 -t 192.168.1.1 192.168.1.135 2> /dev/null &  
# arpspoof -i eth0 -t 192.168.1.135 192.168.1.1 2> /dev/null &
```

Para ver las todas posibilidades de jugar, integrados en esta aplicación:

```
# dpkg -L dsniff | grep bin
```

Empiezo a abrir consolas, las esparzo por la pantalla, me rooteo en todas y en cada una lanzo un proceso. Para esnifar contraseñas (si hay suerte, que no siempre ocurre):

```
# dsniff -m -i eth0
```

Si la red es inalámbrica sustituir "eth0" por "wlan0". Con -m se intenta determinar el protocolo automáticamente a partir del archivo /usr/share/dsniff/dsniff.magic. No lanzo "macof" porque no tengo la intención de dejar la red inservible pero sí para capturar tráfico nfs, correo (Outlook, Thunderbird..) y sesiones de chat (Messenger, Yahoo, ...):

```
# filesnarf -i eth0
# mailsnarf -i eth0
# msgsnarf -i eth0
```

Para analizar el tráfico ssh (Aunque, a veces, las contraseñas siendo correctas se detecten como "Password authentication failed")

```
# sshow -i eth0
```

Ver todas las páginas que visita el husmeado:

```
# urlsnarf -i eth0
```

- Oye, ¿sabes que los famosos protocolos de cifrado de contraseñas wifi, las famosas WEP y WPA, se craquean en menos que canta un gallo?

- Y, ¿Qué?

- Pues que las noches en las que no tengo nada que hacer voy de pesca...

- ¿De pesca?

- Dejo la wifi abierta (sin contraseña) y espero que alguien pique. Luego con dsniff me divierto un buen rato hasta que el piratilla se asquea...

- Mira que eres malo

- Con # tcpkill -i eth0 host nombre_del_host.com le mato conexiones, con # tcpnice -A -i eth0 tcp se las ralentizo y con # websploit -i eth0 IP y en la barra del navegador pongo la IP del intruso veo por donde navega... Oye, es divertidísimo que te chupen wifi...

- Vaya pedazo de keron estás hecho...

Analizando todos los datos que arrojaba cada una de las terminales pudimos averiguar un montón de cosas importantes. Desconectamos el equipo y lo volvimos a dejar todo como estaba. Salimos de nuestro escondite y nos dirigimos a las dependencias 98 Milenium, en la quinta planta. Los pasillos estaban muy concurridos. Unos guardias de seguridad pasaron por nuestro lado y, por lo que comentaban, había algún intruso en la 7 planta. Sin duda nos buscaban a nosotros. El administrador de la red, que se le supone "estar al tajo", seguro que había detectado MACs duplicadas, síntoma de que alguien está figoneando donde no debe, con:

```
# arp -a
```

Yo, en mi pc antes de que me lo destrozaran, para evitar el envenenamiento ARP había creado tablas ARP estáticas:

CAPÍTULO 16. NOS ACERCAMOS A LA VECINA CON DSNIFF

```
# arp -s 192.168.2.2 00:35:4c:31:1A:12
```

O para hacerlo permanente:

```
# touch /etc/arp.conf
# nano /etc/arp.conf
```

Y en su interior poner la MAC (o MACs) del equipo y separado por un espacio la IP del/los pcs:

```
00:35:4c:31:1A:12 192.168.2.2
```

Se edita:

```
# nano /etc/network/interfaces
```

Y en la última línea se pone:

```
post-up /usr/sbin/arp -f /etc/arp.conf
```

En cuestiones de seguridad nada es infalible, pero siempre puedes tocarles los bzipos a los curiosos. Mientras pasábamos por un pasillo flanqueado por grandes vidrieras que daban a estancias repletas de oficinistas, volvimos a ver a (punto) Antúnez. Nos mimetizamos con los que estaban esperando su turno alrededor de una máquina de café sin quitarle ojo de encima. Al rato salió, acompañado de otra persona con la que mantenía una animada charla. Entraron en el ascensor y descendieron hasta la planta -2. Hacia allí nos dirigimos. Por aquella planta no se veía un alma. Decidimos entrar por una puerta al azar.

- ¡Alto! a qué departamento están adscritos...

Nos asaltaron al abrir la puerta...

- .dll

- Esto está en la 3ª planta

- Perdón...

Cerramos.

- ¿Te has fijado?

- ¿Me engañó la vista o todos estaban atados a las sillas delante del monitor?

- Viste bien... y les torturaban con el "tour de güindous"... Sssssshhhh... Se oyen pasos... ¡entremos aquí!

Nos metimos en los servicios.

- Precisamente buscaba unos...

- Ella tan tranquila haciendo sus necesidades...

- ¡Pues no! Me permites coger un poco de papel...

CAPÍTULO 16. NOS ACERCAMOS A LA VECINA CON DSNIFF

Capítulo 17

El tiempo justo para que me líe con steghide

Abrieron la puerta mientras nosotros aguantábamos la respiración en uno de los excusados.

- Y no te demores que te haremos recuperar el tiempo perdido.

Dijeron mientras reían a carcajada partida. Alguien entró en el excusado de al lado. Con gran sigilo, me subí a la taza del water y miré por encima del pequeño tabique separador. ¿Recontra-mysql-server! era mi vecina. Cuando me vio hizo una, casi imperceptible, mueca de alegría. Se la notaba descompuesta, ojerosa y ausente.

- Venga, venga, que el tiempo pasa...

Increparon los dos que aguardaban en la puerta. Antes de salir me alargó un papel.

- Has estado mucho tiempo, te has ganado media hora más de sesiones

- No por favor....

- Ya sabes, te lo puedes ahorrar volviendo al redil..

- ¡Nunca!

- ¿Dije media? Una hora extra..

Con mi amiga, miramos el papel. Era la imagen en jpg que ilustra la cabecera del capítulo.

- Conociendo a mi vecina, seguro que tiene algún mensaje oculto.

- ¿Tipo tinta invisible o cosas por el estilo?

- Más fino, escritura oculta. Y me juego los gparteds que el resultado del jeroglífico del capítulo 14 nos puede conducir a la solución de éste.

- Si pierdes, me encargo de pasártelos de ext3 a ext4.

Dijo relamiéndose los labios con expresión morbosa. No quería ni pensar en que podía consistir una formateada de estas características realizada por mi amiga. Nos pusimos mentalmente (ya que la taza del water no tenía entrada usb) manos a la obra, al desencriptado, no al formateo. Descargamos la imagen de cabecera¹ y:

```
# apt-get install steghide
```

¹El enlace es: <http://www.tuxapuntes.com/drupal/node/1588>. Ver epílogo.

Y comprobamos si tiene algo escondido en su interior y si entramos la clave nos mostrará información:

```
$ steghide info imagen.jpg
```

Para extraerlo:

```
$ steghide extract -sf imagen.jpg
```

Como me temía, el nombre de usuario de la solución del capítulo 14 nos permitió extraer un archivo codificado de la imagen. Para realizar el proceso inverso, o sea incrustar un texto en una imagen:

```
$ steghide embed -cf imagen.jpg -ef archivo_texto
```

Y si somos amantes de la música:

```
# steghide embed -cf archivo.wav -ef archivo_texto
```

Que siempre le dará una aire más lírico. Para descodificar el gpg:

```
$ gpg archivo_texto.gpg
```

Y el proceso inverso:

```
$ gpg -c archivo_texto
```

- Muy curioso tu amigo steghide.
- Uy, y lo que no sabes, si le das:

```
$ steghide encinfo
```

te lista algoritmos y tipos que pueden usarse, y luego lo especificas con el parámetro -e:

```
$ steghide embed -cf imagen.jpg -ef archivo_texto -e cast-256 ctr
```

- Pero, ¿para qué quieres variar el algoritmo que viene por defecto (Rijndael-128) si para extraer al archivo oculto se usa la misma parida (steghide extract -sf imagen.jpg) para todos los algoritmos?

- Porque te hace más interesante con las mujeres...

- ¿A sí? ¿Y cual es el algoritmo que debemos usar para ocultar...

Me dijo algo en la oreja...

- ...dentro de...

Nuevamente se me acercó para susurrarme otra cosa...

- ¿Crees que este retrete es el sitio apropiado para probar algoritmos estenográficos?

- Todo es cuestión de probar... y con el parámetro -e....

Capítulo 18

Rkhunter no puede con ellos

Tres veces tuvimos que silenciar nuestro ímpetu estenográfico por la irrupción de sendos personajes en busca de alivio intestinal y esto, quien lo ha sufrido puede confirmar, destroza mogollón. Pero así es la vida y el clímax conseguido justifica todas las vicisitudes. Salimos en busca de algún ordenador para averiguar el misterio de la foto (real y no mentalmente). Lo encontramos en un despacho, en aquel momento, desocupado. Aparentábamos normalidad porque una gran empresa como aquella, seguro que tenía cámaras de seguridad por todas partes.

```
# apt-get install motion
# /etc/init.d/motion start
```

Y todo movimiento detectado lo plasmará en una instantánea en /tmp/motion según los parámetros especificados en /etc/motion/motion.conf (los que vienen por defecto son más que suficientes). Dimos con la planta .exe. Para entrar nos mimetizamos con un grupo loando con ellos las grandes virtudes de la bandera ondeante, pero el acceso a las celdas estaba fuertemente vigilado. Nos sentamos en unas butacas situadas en una especie de sala de espera para estudiar la situación. No la estudiamos mucho. Entraron unos matones.

- ¿Pero a quiénes tenemos aquí? A los curiosones....

- Pues sí, mira por donde, siempre me ha intrigado eso de los chequeos del sistema automáticos cada cierto número de arranques, ya sabes:

```
# tune2fs -l /dev/sda1 | grep -i 'mount count'
```

- Y la diferencia entre "Mount count" y "Maximum mount count" es el número de arrancadas que te faltan para que fsck te chequ....

No terminé del puñetazo en la jeta que me arrearón. Mi amiga se abalanzó sobre el agresor en un acto tan inútil como desesperado y también le dieron en todo el morro terminando dando tumbos por el suelo y sangrando por la nariz. Nos levantaron.

- Si no quieres saber las arrancadas que te faltan para que fsck te haga un chequeo de la partición tampoco tienes por qué ponerte así muchacho.

- ¡Tiene razón, animal más que animal!

Le increpó mi amiga para echarme un cable aunque lo que consiguió fue que nos dieron con más ganas, no sé si porque interpretaron lo del "fsck" como literal

y lo de "animal" como figurado, al revés o ni siquiera lo interpretaron. A estas alturas empezaba a dudar de en qué bando jugaba mi amiga. Nos metieron en unas celdas que como único consuelo carecían de "Vistas" y allí nos quedamos hasta al día siguiente. Mira por donde como son las cosas, no sabíamos como entrar en esta sección y entramos de la forma más fácil y por la puerta grande, eso sí, un pelín magullados. Nos vinieron a buscar. Mientras íbamos a no sé donde, nos cruzamos con una hilera de personas que más parecían zombis que seres humanos. Eso me recordó que para conocer el número de procesos abiertos incluidos los zombie:

```
$ top | grep Tasks Tasks: 191 total, 2 running, 186 sleeping,
2 stopped, 1 zombie
```

Y para visualizar sólo los procesos de ultratumba:

```
$ ps auxw | grep defunct
```

Estos procesos no consumen cpu ni cerveza de la nevera y tampoco pueden matarse a lo espagueti western (\$ kill -9 PID). Pasan a mejor vida al reiniciar o incluso desaparecen de forma espontánea o sea que no es necesario poner ajos en la puerta o empezar un curso de vudú por correspondencia para protegerte de sus maleficios. Los que pasaban por nuestro lado parecían zombis en el sentido literal de la palabra. La expresión de sus rostros indicaba que lo estaban pasando muy mal. Pudimos ver a mi vecina entre los del grupo. Intercambiamos unas miradas. La mía intentaba decirle "aguanta". Creo que lo entendió. Nos llevaron a una habitación donde nos aguardaba alguien y a su lado, evitando mi mirada, estaba .(punto)Antúnez. El que parecía el jefe tenía la cara rara, inexpresiva. Hablaba casi sin mover los labios.

- Bien, amigos míos..... dentro de algún tiempo, depende de Vds, volverán al redil.... tenemos métodos muy convincentes, pronto podrán comprobarlo.

- Agradecemos su hospitalidad pero como no nos suelten hago explotar la bomba que llevo adherida a la...

No sé por qué será que nunca me dejan terminar la frase del guantazo que me propinaron.

- ¡Imbécil!

Antes de perder el conocimiento todavía pude decir:

- Bueno, bomba no, pero si quieres buscar rootkits en tu sistema:

```
# apt-get install rkhunter
```

Recargas la base de datos:

```
# rkhunter --update
```

Y, dado mi precario estado que ni al intro podía darle, que los busque solito:

```
# rkhunter -c -sk
```

Aún noté el puntapié en el hígado. Menuda panda de insensibles....

Capítulo 19

Tune2fs hace reaccionar a .Antúnez

Cuando recobré el sentido estaba solo en una celda con varias literas. Supuse que sería la hora del lavado de coco y los demás estaban aguantando las sesiones. Los métodos tenían que ser agresivos puesto que incluso un irreductible como .(punto)Antúnez había sucumbido. Se abrió la puerta.

- ¿Estás loco, cómo se te ocurre venir aquí?

Hablando del lobo... Era .(punto)Antúnez

- Bueno, pensé que podía interesarles cambiar el número de arranques para que fsck realice el chequeo automático

```
# tune2fs -c 60 /dev/sdxx
```

y te los hará cada 60 reinicios, y con

```
# tune2fs -i 3m /dev/sdxx
```

será cada 3 meses, y substituyendo "3m" por "3w" cada 3 semanas

A .(punto)Antúnez le brillaban los ojos y me escuchaba absorto. Cuando terminé mi parrafada él continuó:

- Y si lanzas

```
# tune2fs -l /dev/sdxx |grep 'Last checked'
```

te dice la última vez que se chequeó el sistema.

- Y con:

```
# tune2fs -l /dev/sda1 | grep -i check
```

las veces que se fuerza el chequeo.

- Y, a menos que seas un temerario, lo aconsejable es no poner jamás

```
# tune2fs -i 0 /dev/sdxx
```

porque entonces se desactiva el chequeo de la partición.

La expresión de su cara había cambiado totalmente, ahora era radiante, como si de repente hubiera recobrado la lucidez. Fue entonces cuando pasé al ataque.

- ¿Qué te han hecho para que traicionaras nuestros valores? Nuestra lucha por el programario libre, ¿te acuerdas? Y de aquel maldito módem que tardamos 2 semanas en configurar y que cuando lo conseguimos descorchamos un reserva que guardabas para las grandes ocasiones ¿Cómo se llamaba... ? Sí, un Gran Heredad Segismundo Sintierra.

- ¡Un reserva memorable!

- ¿Y de aquella rubia? ¿No te acuerdas que decías que era la que mejor hacía el mount del instituto y que ni poniendo en su fstab "noauto" conseguías frenar su fogosidad?

Parecía que mi terapia funcionaba. Continué hablándole de nuestra época juvenil y él iba asintiendo con la cabeza. Se le veía feliz inmerso en sus recuerdos. Creí llegado el momento de apretar un poco más la tuerca.

- Qué podemos hacer para liberar a toda esa gente de las garras de los Blue Pantallaz?

La puerta se abrió y entró el de la cara rara con varios hombres. Intenté reaccionar rápido para no comprometer a la única persona que podía hacer algo por nosotros. Me abalancé sobre .(punto)Antúnez y agarrándole por el cuello:

- ¡Jamás conseguirás que cambie un lanzador por un acceso directo! ¿Has oído? ¡Jamás!

Rápidamente me redujeron y me aplastaron la cara contra la pared mientras me retorcían el brazo a la espalda. Grité:

- Y si quieres forzar el chequeo de una partición siempre cuando la arranques, crea el fichero vacío.

```
# touch /forcefsck
```

A trompicones y de mala manera me llevaron a una sala grande repleta de pantallas en la que, en cada una, había inmovilizada una persona sin posibilidad de zafarse de lo que por ellas se retransmitía. Mi vecina estaba en una de la primeras filas y mi amiga y yo, recién llegados, nos pusieron en las últimas. Rápidamente empezaron las proyecciones. Me refugié en mis pensamientos para no hacer ni caso a lo que me forzaban a ingerir.

- Si esto de delante fuera un sistema operativo normal podría ver la resolución máxima, mínima y la usada por este monitor con:

```
$ xrandr
```

Y la podría cambiar con:

```
$ xrandr -s 1280x1024
```

O especificando la tasa de refresco:

```
$ xrandr -r 76
```

Estuve cambiando mentalmente la resolución de pantalla varias veces. Cuando me harté del xrandr dejé mi mente con un protector de pantalla formado por múltiples comando de la shell en constante movimiento.

Capítulo 20

Juntos al fin

Al día siguiente, después del primer palizón propagandístico, nos concentraron en el pasillo para llevarnos nuevamente a la sesión educativa. Dentro de la gran sala y una vez atados a las sillas, el de la cara rara nos dirigió unas palabras contándonos que fulanito y menganito habían vuelto a las buenas formas. (punto)Antúnez estaba a su lado. De repente:

- ¡Todo el mundo quieto!

El subcomisario Linares y algunos de sus hombres entraron por la puerta como un torbellino. Me vio.

- ¡Linux! ¡Qué narices haces aquí!

- Nada, verás... es que estos señores querían saber como funciona el nessus para ver los puntos flacos de nuestra máquina, ya sabe:

```
# apt-get install nessus nessusd nessus-plugins
```

Creamos el usuario nessus:

```
# nessus-adduser
```

- Entramos nombre, escogemos autenticación por contraseña (pass), la entramos y confirmamos, «CTRL+D», «Intro» y salimos...

Mientras, disimuladamente, el de la cara rara se había ido desplazando hacia una puerta, alguien gritó:

- ¡Se escapa!

Al verse sorprendido echó a correr por entre las filas, con tan mala elección que fue a pasar por donde mi amiga, que sin dudarlo le puso la zancadilla, cayendo de bruces a mis pies. Aprovechando el bullicio le propiné un puntapié en los dientes que le desconfiguró la cara por completo y mientras lo miraba le solté:

- ¡Pedazo de bruto! No podrás usar nessus si no te registras en

<http://www.nessus.org/plugins/index.php?view=register> te mandarán un correo con la clave. La copias y:

```
# nessus-fetch --register xxxx-xxxx-xxxx-xxxx-xxxx
```

Lanzas el demonio y arrancas nessus:

```
# nessusd -D
# nessus
```

- Te identificas con el nombre y contraseña puestos en nessus-adduser, en plugins (que queda más fino que llamarlo "ataques"), marcas los deseados (por el mismo precio los marcas todos si no están ya marcados) y en la pestaña target pones la IP a escanear de tu máquina o de alguna de la red local (192.168.x.x) o una IP remota (80.24.xxx.xx) o el nombre de host (dominiodeljefe.com) que siempre resulta más divertido y luego con las vulnerabilidades encontradas vas a ver al jefe gordo y le dices: "Amado jefe, verá, he encontrado ciertos agujeros de seguridad en su pc y algún desalmado, que los dioses no lo quieran y perdonen mi osadía, podría usarlo con fines, digamos que, no muy lícitos" y con esta buena acción, puedes conseguir ganarte un lugar en el cielo y que te echen por gilinetstat (que conste que el que avisa no es traidor, es un avisón).

Llegó el subcomisario Linares y agarró por los pelos al de la cara rara y le levanto la cabeza pero, al hacerlo... ¡Zas! Le arrancó la peluca. ¿Que digo la peluca? Toda la máscara. ¿Quién se ocultaba detrás de aquella careta? Volvió a levantarlo por los pelos, esta vez lo suyos, y:

- ¡El armario!

El ayudante del subcomisario Linares, que en varias ocasiones me había calentado de lo lindo.

- Hace tiempo que sospechaba de ti - Le dijo el subcomisario. - Con razón tenía la cara rara. Se escondía detrás de una máscara. Le miré nuevamente y le solté:

- Y si quieres eliminar un usuario nessus, porque has olvidado la contraseña o porque estás hasta los GUI de él:

```
# nessus -rmuser usuario_a_suprimir
```

Nos iban desatando a todos. Miré por toda la sala pero .(punto)Antúnez, haciendo honor a su punto, ya no estaba por allí. Me alegré de que hubiera hecho un «CTRL+H» tan rápido. Corrí hacia mi vecina con la que me fundí en un fuerte abrazo. Me di cuenta que tampoco mi amiga estaba por el lugar. Al poco, entró uno de los hombres del subinspector Linares y la traía cogida del brazo.

- ¿Cómo estamos señorita Vargas?

- ¿Vargas?

- Más bien "señora de..." Siento decirle que deberá acompañarnos para contestar a algunas preguntas sobre cierto dinero desaparecido.

- Fue bonito mientras duró. - Dijo antes de salir debidamente escoltada.

El Subcomisario Linares nos hizo un guiño de complicidad, asintiendo con la cabeza.

- ¿Me permite una pregunta?

- ¿Porqué siendo Vd usuario de GNU/Linux siempre se olvida del GNU?

- No le busques ningún trasfondo muchacho, es simplemente porque GNU o ÑU o como quieras llamarlo suena como un garrotazo en los ñus. Linux, en cambio, tiene una sonoridad que ni las arias de Verdi y Puccini. Llámalo marketing si quieres.

Quizá tenía razón...

Epílogo

Este epílogo complementa los anteriores capítulos con información que se encuentra en la red y que podría no estar disponible al lector.

En el Capítulo 13, el nombre de usuario que postea el comentario «Lost in de comentarios» es «lte5280».

En el Capítulo 17, dado que no sabemos si el lector dispone de la imagen, se la proporcionamos junto con lo que debería hacer para conseguir el archivo oculto.



Figura 20.1: Imagen de cabecera del Capítulo 17

Al lanzar en terminal:

```
$ steghide extract -sf tempixhead.jpg
```

Y entrar la contraseña (el nombre de usuario de la solución del capítulo 14) nos extrae el fichero "salvame.gpg"

```
wrote extracted data to "salvame.gpg".
```

Que, una vez descodificado con:

```
$ gpg salvame.gpg
```

nos devuelve el mensaje oculto:

```
Me retienen los Blue Pantallaz en la planta .exe, celda güin7.  
De 8 a las 20 horas, todos los días, he de tragarme vídeos con  
las virtudes de Puertas y Ventanas. Estoy a punto de hundirme  
con tanto next, next, next. Ya no sé distinguir un lanzador de  
un acceso directo. Por favor... sálvame.
```

Disculpen las molestias si no ha encontrado la fuente de la imagen.