Las herramientas de los dioses

4 de abril de 2018 by **Antonio Villalón** **12 Comments**

Hoy en SAW no vamos a hablar de seguridad sino de religión. De la religión verdadera, de la buena: de Unix. Y de sus dioses: Kernighan, Ritchie, Thompson… podríamos citar unos cuantos. Y de las herramientas que, en los años setenta, estos dioses nos enviaron a los pobres mortales, como el maná caído del cielo para el pueblo elegido. Y es que estos dioses crearon un sistema operativo de verdad, con unas herramientas técnicamente maravillosas y una filosofía muy sencilla: capacidades simples que combinadas hacen tareas complejas. La perfección. La vida es Unix ejecutando un script. Han pasado más de cuarenta años y nosotros, pobres mortales que éramos el pueblo elegido, ¿qué hemos hecho en este tiempo? Tratar de deshonrar ese legado divino con capas artificiales e inútiles ("de abstracción", las llaman, para tratar de darles sentido) que introducen dos problemas innecesarios en cualquier entorno tecnológico "moderno": complejidad, y por tanto probabilidad de error, y lentitud. Sirva de ejemplo el ejecutable "true", al hilo de la historia que hace poco comentaba Rob Pike en Twitter:

```
$ >mytrue;chmod +x mytrue
$ ./mytrue
$ echo $?
0
$
```

Un programa cuya única finalidad es devolver siempre 0. Un ejecutable vacío. VACÍO. No puede haber algo más simple y que funcione, desde hace cuarenta años… pues bien, aquí entramos los mortales. Año 2018:

```
$ ls -l /usr/bin/true
-rwxr-xr-x 1 root wheel 17760 29 abr 2017 /usr/bin/true
$ file /usr/bin/true
/usr/bin/true: Mach-O 64-bit executable x86_64
$ otool -L /usr/bin/true
/usr/bin/true:
/usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1238.0.0)
$ /usr/bin/true
$ echo $?
0
$
```

Por supuesto, este es solo un ejemplo, y no de los graves, sobre cómo nos gusta complicarnos. Como dijo un profeta hace años, "*Those who do not understand Unix are condemned to reinvent it, poorly.*". Me imagino el *brainstorming* inicial en un grupo que luego acaba sacando a la luz determinadas tecnologías:

– Tíos, vamos a hacer unas herramientas para manejar grandes conjuntos de datos que ahora están en ficheros planos.
– Pero, si ya tenemos awk, sed, grep…
– Funcionan demasiado bien y la gente no contrata mantenimiento. Escuchad, las llamaremos "bases de datos".
– ¿Bases de datos? Irás de coña, ¿no?
– No, no, lo tengo todo atado: hacen que el fichero por debajo sólo se pueda procesar con nuestro programa metiendo varias capas de abstracción, pero realmente también están manejando archivos de texto, como hasta ahora…
– Jajajaja, ¡qué cabrón! ¡No hay huevos, Larry!
– Sujetadme la cerveza.

```
#define SELECT grep
#define ALTER sed
```

English

SUSCRÍBETE A SAW

¡OK!

PÁGINAS

Acerca de
Aviso Legal
Herramientas "self-made"
Licencia de uso
Los autores
Política de privacidad
Políticas de uso

BUSCAR

Search this website …

SECURITY ON AIR

Por Security On Air
Episodio 3 - Vacaciones ciberseguras

3

Descargar APP

CATEGORIAS

Ciberseguridad industrial (57)
Continuidad de Negocio (13)
Cumplimiento (66)
Eventos (5)
Formación y concienciación (4)
General (1.482)
Gestión (42)
Herramientas (18)
I+D (6)
Inteligencia (37)
IoT (14)
Noticias (53)
Seg. Desarrollo (11)

```
#define DELETE cut
#define DROP ">"
int make_program_look_bigger[1000000];
```

– Eres el puto amo, Larry. ¿Qué va a ser lo próximo, chicos? ¿Un lenguaje de programación que pueda convertir esta Sun 3500 en un 8086, con alguna excusa? ¿Qué se os ocurriría?
– Podemos meter un sleep en las líneas pares de nuestro código C y decimos que es independiente de plataforma.
– Jajajajajaja, no colará… Espera, ¿qué haces, James?
– Sujetadme la cerveza…

Evidentemente, situaciones como las anteriores se producen porque aunque sabemos que Unix es la religión verdadera, Kernighan, Ritchie y demás son sus dioses y algunos otros son sus profetas, aún así hay entre nosotros ateos (los llamaremos así para no ser crueles, aunque el nombre técnico es *Human Malware*), perfiles aparentemente técnicos que no han querido, sabido o podido ver la luz verdadera; los perfiles no técnicos están disculpados, porque Unix no ha iluminado sus vidas aún. Todos conocemos a algún ateo: son los que siempre buscan soluciones complejas a problemas triviales. Preguntadle a cualquier creyente cómo realizar una operación sobre, pongamos, un log, y con una línea de awk lo resolverá. Preguntadle a un ateo y definirá una estructura en base de datos, parseará el log con un programa en Java que tira de varias librerías bajadas de github para convertirlo en un XML, para luego insertarlo en la base de datos de antes, y montará un comité para determinar aspectos críticos, como elegir los tonos pastel para la interfaz gráfica o analizar la ubicación de los botones en una aplicación web que conecta vía API contra un servidor en cloud que a su vez aplica técnicas de machine learning sobre el puto log. ¿Y esto para qué? Para sacar las líneas que contienen la cadena "foo". Ojo, en el tercer campo, ahí es nada.

Dentro de esa familia que estamos denominando amablemente "ateos" podemos diferenciar varios tipos característicos; son los siguientes:

– **Proceseitor**. Lo arregla todo con comités, procesos, procedimientos, controles, controles de los controles, seguimientos periódicos y derivados. Realmente esta subespecie no es un ateo, sino que es peor: está intentando convertir gente a otra religión, ITIL, considerada como secta destructiva en muchos entornos. Debe considerarse a proceseitor como ALTAMENTE PELIGROSO y, en caso de encontrase con uno, se recomienda no acercarse a él y avisar inmediatamente a las autoridades; también podemos cambiarles alguna de sus obras de cabecera, como *Coaching for IT Strategists: a fist fucking approach*, por un ejemplar de *The Magic Garden Explained* o *The Design of the Unix Operating System*, lo que conseguirá una combustión espontánea en cuanto comiencen la lectura.

– **Visual developer**. Programador que no sabe usar punteros y por tanto reniega de C; el scripting no es una alternativa porque "son ñapas". Ante un problema ("especificación de requisitos" le llaman) analiza durante días la situación, hace comparativas entre varias tecnologías, monta unos entornos de desarrollo para realizar *benchmarkings* y, en seis meses, determina que va a desplegar diez capas de abstracción para empoderar al usuario en su relación con la tecnología y evitar así el tratamiento personalizado del dato. Ríete tú de ISO/OSI. Por supuesto el programa nunca funcionará, pero será por culpa de una especificación de requisitos incorrecta; en estos casos, invitar al ateo leer e interiorizar las Sagradas Escrituras, *The C Programming Language* y *The Unix Programming Environment*, puede ser útil, aunque no tanto como un disparo en la rodilla.

– **Segurata**. Acaba de actualizar su LinkedIn para poner que es "*Senior Security Architect, Red Team Leader and Chief Strategist Hacker*" porque se ha leído un manual de metasploit mientras acaba el máster y ya va a tope, con su Kali Linux y sus menús; por supuesto, prefiere ese manual al *Computer Networks* o al *Modern Operating Systems* de Tanenbaum, porque Tanenbaum no es jaker y además usa troff, y eso no es cool… Al contrario que en el caso anterior, el disparo en la rodilla suele ser contraproducente, porque el ateo seguiría molestando y encima se pondría paranoico, activando en su vida el modo MOSSAD_CLAIMS_FOR_ME y siendo aún más pesado; es más efectivo modificar su /etc/hosts para apuntar www.sgae.es a www.fsb.ru, convencerlo para atacar a la SGAE por el tema del canon de los CD, que nunca pasa de moda, y dejar que la naturaleza siga su curso.

– **DevOps**. Administra máquinas Ubuntu y se ha comprado una Raspberry, así que lo debemos considerar devops, porque cree que es un BOFH de verdad pero de vez en cuando se le escapan palabros como XML o agile. Acude regularmente a encuentros endogámicos donde algunos devops explican a otros devops cosas de devops, con dockers y tal, y cuenta la leyenda que una vez uno de ellos recompiló un núcleo Linux y no se lo contó a los demás. *A Quarter Century of Unix History* puede ser un buen detalle con estos ateos, para que sean conscientes de que muchas cosas no las

Seg. Física (32)
Seguridad TI (174)

AUTHORS

Manuel Benet (206)
Antonio Villalón (165)
Maite Moreno (71)
José Rosell (59)
Roberto Amado (55)
Joaquín Moreno (54)
José Miguel Holguín (54)
Jose L. Villalón (49)
José Vila (43)
Nelo Belda (43)
Antonio Huerta (38)
Fernando Seco (38)
Antonio Sanz (36)
Samuel Segarra (35)
Miguel A. Juan (34)
Rafael Páez (33)
David Lladró (30)
Óscar Navarro (27)
Damià Soler (27)
Pablo M. (26)
Adrián Capdevila (25)
José L. Chica (24)
Marc Salinas (21)
Joel Sevilleja (21)
Joan Soriano (21)
Juan Manuel Sanz (20)
Alberto Olmos (18)
José S. (17)
David Cutanda (16)
Raúl Rodríguez (15)
Marcos Sánchez (15)
Alberto Rivas Sr. (14)
David Monteagudo (13)
Borja Merino (13)
Manuel Iranzo (13)
José Manuel Fernández (11)
Marina Brocca (11)
Alberto Segovia (11)
María Ángeles Arqueros (11)
José González (11)

ARCHIVOS

Archivos

Elegir mes

ASOCIACIONES

Hack Hispano

han descubierto ellos, como también puede serlo un teclado sin intro, que nunca viene mal en estos casos. Y si además nos lo queremos pasar bien, tampoco está mal meterles el evil.sh en su .bash_profile.

– **El usuario**. Aunque se considera a sí mismo un perfil técnico porque una vez consiguió salir de vi y se hizo youtuber e instagramer a la vez, realmente sus conocimientos no son muy amplios y debemos considerarlo un usuario. De vez en cuando dice frases como "*Nosotros, los técnicos*" o "*Aquí todos venimos de la parte técnica*", que te suenan como cuando los gibraltareños dicen "*Nozotro lo ingleze*". Ante este tipo particular de ateo no podemos recomendar ninguna lectura, sólo comprensión y paciencia, y también hablarles despacito para que no hagan swap; por otro lado, es fácil -y divertido, hay que decirlo- entretenerlos con algunos palabros sabiamente combinados para que no molesten, como "*Es que en el red team estamos trabajando con una VPN a través de USB que envía paquetes TCP a dispositivos IoT*". Ale, a procesar, campeón.

¿Qué hacemos con esta gente? Guardad el AK-47, por favor, que os veo venir y no debemos legislar en caliente. La situación es compleja, principalmente porque los ateos no tienen depredadores naturales y, sobre todo en los últimos años, se han dedicado a reproducirse de manera exponencial; si os cruzáis con uno podéis regalarle condones para frenar su tendencia reproductiva, pero un consejo: jamás os hagáis los héroes, que esta gente ya no tiene nada que perder, como los administradores de Lotus Notes, y pueden incluso ponerse agresivos. Por ejemplo, a proceseitor le molestan especialmente cosas como que alguien se salte el paso 3, punto 3.8, apartado 3.8.A, párrafo 3.8.A.c, línea 3.8.A.c.XVI, del procedimiento "*Gestión de recursos informáticos corporativos en plena sinergia con el negocio*", que dice que todo renice debe ser aprobado mediante un burofax con el sello oficial, firmado por el *IT Manager* y dirigido al *Business Strategist* de la organización. Se pone nervioso, le da vueltas la cabeza y empieza a hablar en ITIL.

En SAW no tenemos la solución mágica para hacer frente al colectivo de ateos que pululan en las organizaciones; algunos ingenuos piensan que se pueden recuperar con iniciativas sencillas, por ejemplo con campañas donde se use el hashtag #AdoptaUnAteo (#AdoptALuser) para enviarles indirectas simpáticas que traten de marcarles el buen camino, del tipo "*biff también avisa de nuevos mensajes… desde hace 40 años y sin soniditos ridículos, imbécil #AdoptaUnAteo*", "*Menos stackoverflow y más RTFM #AdoptaUnAteo*" o "*No abras ficheros CSV con Excel, hijo de puta! #AdoptaUnAteo*". Pero nosotros sabemos que esto no funcionará: ni devolverá al ateo al camino verdadero ni tampoco conseguiremos que convierta el agua en vino. Por eso miramos a la Historia: ¿qué se ha hecho de siempre con la gente que abandona la religión verdadera? Dos cosas: exorcismos y sacrificios humanos. Punto.

Si vamos a exorcizar ateos, por ejemplo poseídos por systemd, debemos ir con cuidado; desde SAW recomendamos que un exorcismo lo ejecuten sólo profesionales, porque si sale mal nos confiamos, creemos haberlo recuperado y un día nos encontramos al falso creyente diciendo en un foro que ifconfig está *deprecated*. Cuando se dé cuenta de que vamos a exorcizarlo, el ateo tratará de confundirnos para hacernos creer que ha visto la luz verdadera; puede decir cosas en idiomas desconocidos, fruto de la posesión, del tipo "*Powered by Solaris…*" o "*alias nano='rm -f'*", pero no nos dejemos engañar: al acercarle el Essential System Administration, su solo contacto le producirá quemaduras, comenzará a girar la cabeza 180 grados, a escupir espuma por la boca y a soltar blasfemias como "*Has visto lo que ha hecho la cerda de tu hija*", "*Tómame, tómame*" o "*Yo soy el Maligno y capturo SIGKILL*". Cuidado. Aquí es cuando el exorcista, un profesional, arrojará varios SIGTERM contra el PID del ateo y pronunciará unas palabras sagradas para liberar su alma:

Te exorcizamos Espíritu Inmundo, quienquiera que seas, Java, XML o Word. En el nombre de Unix seas arrojado de las almas de la religión verdadera. No oses oscurecer a los elegidos a quienes pretendes hacerte semejante; te lo ordena Brian, te lo ordena Dennis, te lo ordena Rob, que se hicieron carne y habitaron entre nosotros. Que los descendientes de MULTICS se apiaden de ti, que la pureza de un buen script limpie tu alma, que uses goto cuando tengas que usarlo. Unix es la senda y yo soy su pastor, así está escrito en mi GECOS. Hosanna, K&R, limpiad esta alma.

En este momento el ateo debe mostrar signos de reconversión, por ejemplo desinstalando la máquina virtual de Java o recitando de memoria la página man de getpwent(3). Si no es así ya debemos rociarlo de SIGKILL o, directamente, ejecutar un shutdown, que es el último recurso del exorcista antes de pasar a mayores: si el exorcismo no funciona ya sólo nos queda el sacrificio humano. Por ejemplo, en SAW, desde el fallecimiento de Ritchie hace más de siete años, mensualmente sacrificamos en su honor a un ateo en la hoguera, a la antigua, con encanto; lo hemos puesto en el cron y así no falla, que si no luego se reencarnan en consultores ISO y la liamos. Pero no penséis que es un simple kill -9, no: antes de quemarlo lo abrimos en canal con un CD

ISMS Fórum

BLOGS

Apuntes de Seguridad de la Informac
BITácora
Bruce Schneier
Chesco Romero
Dancho Danchev
Diablo Horn
Ha.ckers.org
Hack Players
Kriptópolis
Marketing Positivo
Paloma Llaneza
Pentester
Port 666
RootByte
Security by default
Security Clan House
Seguridad y Gestión
Sergio Hernando
Steve Bellovin
Taddong Security Blog
Tenable Security
The Invisible Things
Veracode Blog
Vlan7
Zero Day

ORGANISMOS

Club Francés de Seguridad de Siste
Información
CSIRT-CV
INCIBE

PUBLICACIONES

RFID Magazine
Security Focus

META

Acceder
RSS de las entradas
RSS de los comentarios
WordPress.org

Licencia de uso del contenido

donde están las fuentes de System V, nos comemos sus vísceras, bebemos su sangre y rezamos dos scriptnuestros para que aquellos dioses que se hicieron carne en los 70 vuelvan a poner cordura en este mundo 4.0 que nos rodea. Todo esto en honor a los creadores de maravillas como Unix, C o awk y, por qué no, también porque nos gusta.

DISCLAIMER: *Todo este post está basado en hechos ficticios y no refleja en ningún momento opiniones personales del autor, efectivamente y no. Cualquier parecido con la realidad es pura coincidencia.*

Comments

Nomex says:
4 de abril de 2018 at 10:46 am

Que bueno Toni, me has hecho volver unos cuantos años atrás. Todavía recuerdo tu frase "Esto con awk está hecho en dos patás" :)

Enrique says:
4 de abril de 2018 at 11:10 am

GENIAL!!!

evil.sh says:
4 de abril de 2018 at 11:58 am

:'-) :'-) :'-) :'-)

ivelgar says:
4 de abril de 2018 at 12:04 pm

Descomunal!!!!! Alabados sean los dioses!!!!

Jordi Murgó says:
4 de abril de 2018 at 2:31 pm

Hijo mio, eres digno de ser acptado en la secta de Tha Apostols.

– Savage.

segurata006 says:
4 de abril de 2018 at 3:10 pm

No conocía el evil.sh. Me he puesto a echar una ojeada al .sh y me he encontrado esto:

export EDITOR=/bin/rm;

Mayor troleada que jamás he visto

Pepe Rosell says:
4 de abril de 2018 at 7:21 pm

Es espectacular!!!!!

El tío tonet says:
4 de abril de 2018 at 8:28 pm

Jajajaja…. Me he hartado de reír…. Pero los de la CCI rusa son mejores. De vez en cuando viene bien… Jajajajaja…. Gracias Toni

Troyano says:
4 de abril de 2018 at 8:57 pm

Omfg que jartá a reír. Pero aun no he visto ningún costalero de Kernighan ni de Ritchie estas semanas ni azotes con el LART: Luser Attitude Readjustment Tool (http://b0.img.mobypicture.com/e89eb2739d317a3add03de4d2230566c_view.jpg)

Habra que mejorar eso

Javier Montero says:
4 de abril de 2018 at 9:00 pm

Muy interesante los libros/manuales/lo que sea mencionados en el articulo. Creo que ya tengo lectura para el resto del año.

Lourdes says:
4 de abril de 2018 at 11:37 pm

Jajajaja ¡¡Hace tiempo que no me reía tanto leyendo un artículo!! IMPECABLE en el.fondo y en la Forma. Enhorabuena Toni

anónimo says:
5 de abril de 2018 at 12:43 am

jajajaj, cuanta razón. ¿En qué momento los informáticos puros The Unix dejaron de transmitir sus conocimientos a los compañeros y se dedicaros a ascender como jefes de humo? ¿En qué momento permitieron que los comerciales les pasaran por encima vendiendo tecnología 2.0, 3.0 y ahora 4.0 y sacrificando así sus almas por dinero?
La reconquista de la pureza empieza por uno mismo!

Deja un comentario

Introduce aquí tu comentario...

Return to top of page