CONTENIDO

HACKING ÉTICO Y TESTING INTELIGENTE PARA VALIDACIÓN DE INFRAESTRUCTURAS DE SEGURIDAD

El coste de la inseguridad y la indisponibilidad

El incremento continuo de las amenazas y las infracciones sobre la seguridad informática hacen que las organizaciones queden expuestas a robos de datos, pérdidas económicas, daños de imagen, indisponibilidad de los servicios e importantes problemas legales. Justificada la necesidad de evaluar y validar la infraestructura de seguridad, el presente artículo explica las buenas prácticas y medidas a llevar a cabo con el fin de asegurar a su empresa el nivel más alto de protección sin afectar al rendimiento de sus aplicaciones y servicios.

AYSCOM Celular de Servicios
José Ruiz

Septiembre de 2012

INTRODUCCIÓN

A menudo, aparecen en los medios de comunicación casos de empresas que han sufrido costosos tiempos de indisponibilidad, penalizaciones y demandas judiciales; como consecuencia de violaciones de su seguridad informática. El ataque a Sony Playstation le supuso a la compañía $171 millones en costes directos, $77 millones de registros robados y una estimación de $1 billón en costes de reparación y daño de imagen.

La Comisión Europea, en su Estrategia de *Ciberseguridad*, está valorando que las prácticas de gestión de riesgo sean de obligado cumplimiento, para los sistemas de información y redes que sean críticos en la provisión de servicios económicos y sociales clave como: finanzas, energía, transporte y salud; y en el funcionamiento de Internet como por ejemplo: comercio electrónico y redes sociales. Actualmente, solo los operadores de telecomunicaciones y los proveedores de servicios de Internet están obligados por las leyes europeas a adoptar prácticas de gestión de riesgos y reportar incidentes de seguridad.

Las amenazas a la seguridad informática, afectan directamente a aspectos empresariales que son clave para el desarrollo de cualquier negocio tales como: la credibilidad, pérdida de datos, reputación empresarial e incluso problemas legales.

- **Robo y salida no autorizada de datos.** Datos financieros, listas de clientes, propiedad intelectual, planes de desarrollo y marketing de producto.
- **Pérdida de tiempo.** Recuperación/reparación de datos, Chequeo completo del sistema.
- **Indisponibilidad e interrupción en los servicios.** Se suele traducir en una insatisfacción y pérdidas de clientes.

- **Exposición legal.** Una compañía se puede ver ante la ley por perder datos que están bajo su custodia.

¿Cuánto debería invertir una organización en asegurar un alto nivel de protección y continuidad de su actividad? A diferencia de un ROI típico, que determina la relación entre la cantidad invertida y lo que se recupera a cambio, cuando se trata de seguridad se compara lo que gasta en relación a la cantidad que se podría evitar perder. El alto coste que la inseguridad y la indisponibilidad de los servicios supone a las empresas justifica la necesidad de verificar y evaluar el cumplimiento de las directivas y políticas de seguridad.

Por otro lado, la simple instalación de una solución de seguridad no garantiza la protección contra un ataque, sino que incluso puede crear una falsa sensación de seguridad y además limitar el rendimiento de los servicios y aplicaciones del negocio. Las plataformas de seguridad, al igual que las amenazas, son cada vez más sofisticadas y diversas, y la clave para mantener un

nivel de protección efectivo está en ponerlas a prueba y validarlas de antemano antes de su despliegue e instalación.

Utilizando el banco de pruebas apropiado, con capacidad para recrear un entorno realista (actualizado) de carga y amenazas, se puede conocer el verdadero nivel de protección al que aspira una infraestructura de seguridad de red, así como el impacto que tendrá sobre el rendimiento de las aplicaciones y los servicios considerados legítimos.

RIESGOS Y AMENAZAS A LA SEGURIDAD

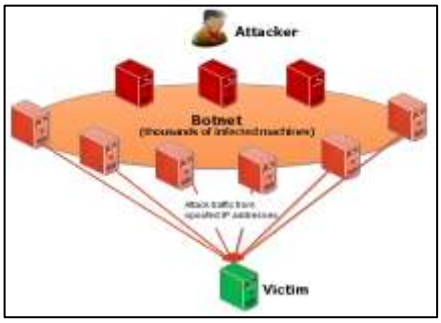
En los últimos años, impulsado por el incremento exponencial de los servicios y aplicaciones móviles y *cloud*, se ha incrementado de forma alarmante el número de amenazas sobre la seguridad informática e Internet.

Denominamos vulnerabilidades a aquellos puntos débiles de las aplicaciones y software que permiten que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de los sistemas informáticos. Más del 40% del total de vulnerabilidades se producen en las webs.

El malware, abreviatura de software malicioso, es un código de programación diseñado para interrumpir o denegar la operación, reunir información que implica a la pérdida de la intimidad o la explotación, obtener acceso no autorizado a los recursos del sistema y otros tipos de comportamiento abusivos. El Malware incluye virus, gusanos, troyanos, *spyware, adware* deshonesto*, scareware, crimeware*, la mayoría de los *rootkits* y otros programas maliciosos y no deseados.

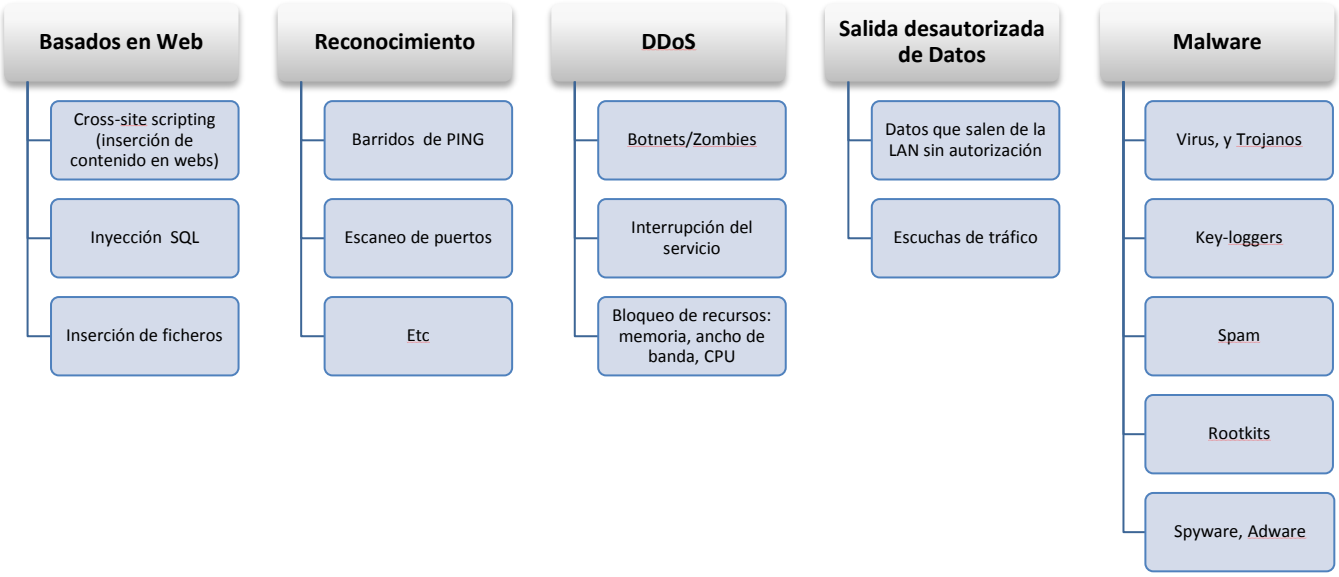
Hoy en día, el desarrollo de malware ha pasado de ser un hobby a ser un negocio muy lucrativo para los delincuentes. Mostrar publicidad selectiva (*Spyware, Adware y Hijacking*), robar información personal (Keyloggers y Stealers), realizar llamadas telefónicas (Dialers), etc.

Un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés *Denial of Service*), consiste en provocar que un servicio o recurso sea inaccesible a los usuarios legítimos. Cuando el ataque DoS es iniciado desde distintos puntos de conexión o hosts sincronizados, el ataque es llamado DDoS (de las siglas en inglés *Distributed Denial of Service*). La forma más común de realizar un DDoS es a través de una botnet (redes de robots informáticos), siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.



¿Qué motiva e impulsa la generación de ataques DDoS? Principalmente se trata de motivos económicos (DDoS como servicio, *blackmail*, etc), aunque también es habitual por venganza y ataques personales con los que se bloquean sitios webs de la competencia, motivos políticos o simplemente por diversión dada la facilidad de implementación de este tipo de ataques.

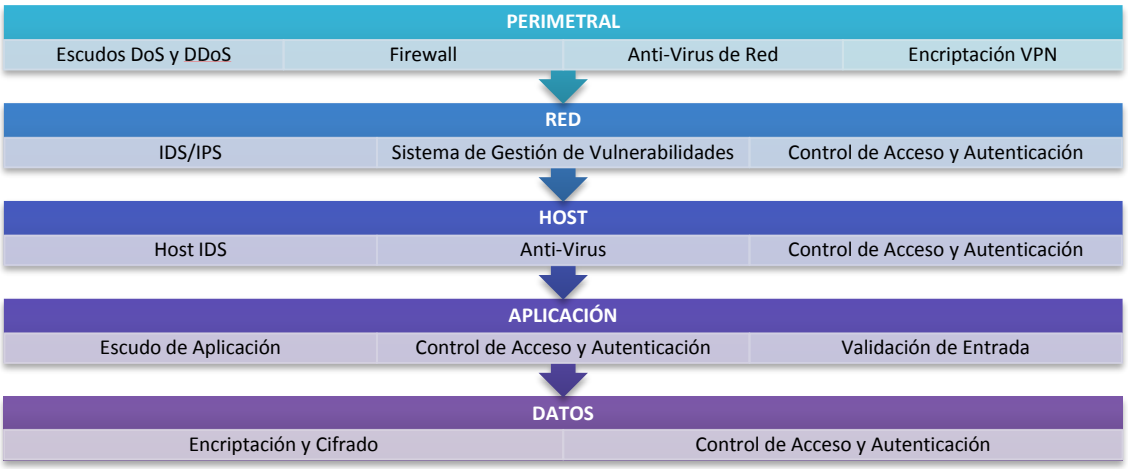
Una posible clasificación general de los ataques y amenazas más comunes se muestra a continuación.



DISPOSITIVOS Y SISTEMAS DE PROTECCIÓN

Para definir e implementar una infraestructura de seguridad, lo primero que se ha de tener en cuenta es qué es lo que se pretende proteger (la red interna de las sedes de una empresa, un servicio de *cloud*, un centro de datos en internet, la entrada a la red de un operador móvil, etc) y cuáles son las expectativas ponderadas que se tienen sobre la misma (protección, precisión en la detección para evitar bloqueos de tráfico legítimo, rendimiento, eficiencia de operación y gestión de la plataforma, etc).

El enfoque por capas y niveles representa una buena práctica para afrontar y reducir el riesgo sobre la seguridad de red y sistemas de información. Se trata de clasificar en cinco niveles las responsabilidades que los distintos procedimientos y sistemas de protección tienen sobre la seguridad global.



No obstante, la evolución de algunos fabricantes de sistemas de seguridad ha sido la de intentar integrar en un solo dispositivo distintas capacidades y mecanismos de protección. Los llamados Firewalls de Nueva Generación (NGFW, de las siglas en *Next Generation FireWall*) ofrecen las funcionalidades de un Firewall tradicional, pero además, incorporan capacidades de identificación de aplicaciones, usuarios y contenido (como las de cualquier dispositivo DPI, *Deep Packet Inspection*) de forma que puedan integrar en un solo dispositivo funciones identificación y prevención de intrusos, antivirus, etc.

Del mismo modo, un sistema de Gestión Unificada de Amenazas (UTM, del inglés *Unified Threat Management*) es un Firewall que engloba una serie de funcionalidades añadidas en una misma máquina como pueden ser las Antispam, Antiphishing, Antispyware, Filtro de contenidos, Antivirus, Detección y Prevención de Intrusos (IDS/IPS), etc.

Actualmente existe un gran debate entre fabricantes que piensan que es más ventajoso para las organizaciones tener todos los mecanismos de protección integrados en un solo dispositivo y los que defienden el modelo por capas y la especialización en un solo dispositivo de cada servicio de protección. Entre las posibles ventajas y desventajas de cada opción se suelen exponer la sencillez y menor coste de una gestión unificada y en contraposición la creación de cuellos de botella.

El propósito principal de este documento no es el de profundizar en detalle en el funcionamiento de los distintos dispositivos y sistemas de protección, si no el de exponer la metodología a seguir para obtener una serie de métricas que reflejen los verdaderos niveles de seguridad y rendimiento ofrecidos por dichos sistemas y dispositivos.

TESTING DE LA INFRAESTRUCTURA DE SEGURIDAD

Debido a la alta responsabilidad que los dispositivos y sistemas que componen la infraestructura de seguridad tienen sobre el nivel de protección ofrecido y el impacto sobre el rendimiento de los servicios, se hace indispensable una exhaustiva evaluación y validación de los mismos durante la fase de *benchmarking* competitivo y selección de fabricantes,

previamente al despliegue y periódicamente durante la fase de producción y explotación de los sistemas.

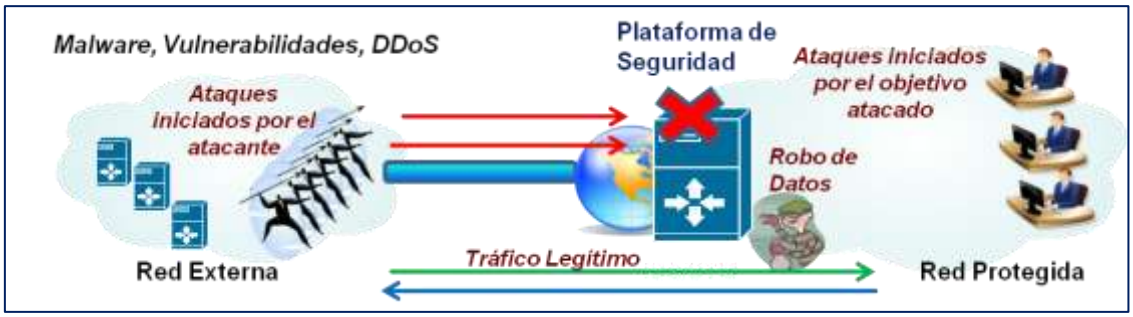
¿Cómo debe ser la plataforma de test?

Realizar pruebas inadecuadas puede resultar aún peor que no hacer nada en absoluto y podrían crear una falsa sensación de seguridad. Algunas de las prácticas inadecuadas (y no recomendadas) más conocidas se exponen a continuación:

- Hacer pruebas directamente sobre la red en producción aunque en horarios de baja actividad. En caso de encontrar algún problema el margen de acción es muy reducido y el coste mucho mayor que en el caso de haberlo verificado previamente al despliegue.
- Utilización de *scripts* propietarios. No suelen tener un plan de soporte y desarrollo adecuado, y además se ejecutan sobre máquinas sin los recursos suficientes que permitan recrear entornos y escenarios realistas.
- Uso de software gratuito y código abierto. Pueden llegar a ser útiles en resolución de problemas y en pruebas funcionales básicas, pero en ningún caso podrán ser utilizados para verificar el rendimiento y todas las características de los dispositivos evaluados.

¿Qué debe tener una plataforma de test que permita medir los verdaderos niveles de protección y rendimiento de una infraestructura de seguridad?

- Debe ofrecer un escenario de pruebas representativo de la realidad y simular un comportamiento realista de hasta cientos de miles de usuarios legítimos y atacantes simultáneos.
- Debe disponer de una amplia librería de vulnerabilidades y ataques. Además se debe actualizar periódicamente a medida que surjan nuevas amenazas mediante la suscripción a organizaciones como NIST, Mitre corp -CVE, etc.
- Debe poder generar ataques con y sin técnicas de evasión.
- Debe poder replicar los ataques DDoS conocidos a escala realista de Internet y a tasas máximas de línea.
- Debe contemplar casos de prueba basados en estándares y personalizables.



Adicionalmente, el proveedor de la plataforma de pruebas así como el auditor de la infraestructura de seguridad debe de ser independiente y agnóstico de cualquier fabricante de sistemas de seguridad para que la evaluación sea objetiva, y además debe contar con experiencia demostrable y contrastada en la industria de Test y Medida.

Métricas objetivo en infraestructuras de seguridad

Entre profesionales de la seguridad de la red es habitual hablar en términos de "Factor Trabajo", que es un concepto importante cuando se implementa una infraestructura de seguridad. Factor de Trabajo se define como el esfuerzo requerido por un intruso para comprometer la vulnerabilidad de los sistemas de protección, de forma que la seguridad de red quede expuesta a ser violada con éxito. Algunas métricas tales como la Efectividad de Bloqueo, Precisión en la Detección, Robustez, Rendimiento y Estabilidad definen el Factor de Trabajo de la infraestructura de protección y son expuestas a continuación.

- **Efectividad de bloqueo.** Define la capacidad de un dispositivo de seguridad para detectar y bloquear un ataque (vulnerabilidad, malware, DDoS, robo de datos, etc).

- **Precisión en la detección.** Define la capacidad del dispositivo para detectar correctamente el tráfico legítimo y evitar así los denominados falsos positivos (bloqueo de un servicio o usuario legítimo).

- **Robustez.** Respuesta del dispositivo ante ataques que usan técnicas de evasión (fragmentación IP, segmentación de flujo, ofuscación de URL, etc).

- **Rendimiento.** Métricas como el número máximo de conexiones, ancho de banda, o throughput, a nivel de aplicación (FTP, HTTP, etc) y tiempos de respuesta deben de ser verificadas con y sin la presencia de ataques y amenazas.

- **Estabilidad.** Define la capacidad de la infraestructura para mantener los niveles de protección y rendimiento estables en el tiempo ante cambios en las configuraciones y políticas de protección y ante actualizaciones de software y bases de firmas.

Metodología de Testing

1. **Definir y priorizar los requerimientos.** Se debe hacer una ponderación en base a lo que se espera de la infraestructura de seguridad y tenerlo presente desde el principio. Hacerse las siguientes preguntas puede ayudar a definirlos.
    - ¿Qué rendimiento objetivo debería soportar la infraestructura?
    - ¿Cuáles son los requisitos de Latencia de Transacción?
    - ¿Cómo de importante es la seguridad de las transacciones en comparación con su velocidad?
    - ¿Qué servicios y aplicaciones son las más sensibles, requiriendo los más altos niveles de seguridad?
2. Crear un **escenario realista de carga y definir el plan de pruebas:**
    - Definir los rangos de direccionamiento IP y el número de usuarios a simular.
    - Definir el tráfico legítimo. Se configuran los servicios y aplicaciones más críticos para la organización (HTTP, mail, FTP, etc).
    - Selección de las amenazas a reproducir. Se hace un estudio de las aplicaciones y protocolos más usados y críticos para la organización (Microsoft, Oracle, Apple, etc).
    - En el caso de pruebas de DDoS, se define la red de atacantes y el servidor objetivo, los tipos de amenazas DoS y la tasa a la que se generarán.
    - Definir las técnicas de evasión para las pruebas de robustez.
3. Definir las **variables de rendimiento objetivo** para las pruebas: Ancho de banda por aplicación, conexiones concurrentes, ataques concurrentes, etc.
4. Establecer los **ejes de tiempos de ejecución**.
5. Configurar uniformemente, con **políticas para máxima protección y con las bases de firmas actualizadas** todos los dispositivos a evaluar. Mantener las mismas configuraciones (las que realmente tendrán los dispositivos cuando sean puestos en producción) durante todo el plan de pruebas.
6. Ejecución de **pruebas de rendimiento**. Sin ataques.
7. **Análisis de efectividad**. Simulación de los ataques sin tráfico legítimo. Estudio y clasificación del comportamiento por severidad, año de publicación, fabricante y aplicación.
8. **Pruebas de precisión en la detección**.
9. **Pruebas de robustez**. Uso de técnicas de evasión.
10. **Escalado en complejidad.** Mezcla de tráfico legítimo y amenazas.
11. **Recurrencia y comprobación de estabilidad** en tiempo.
12. **Análisis de Resultados**

CONCLUSIONES

Los proveedores de sistemas de seguridad, compresiblemente, intentarán presentar sus soluciones de la mejor forma posible. Es responsabilidad de cada organización el asegurarse en

cualquier proceso de compra que la solución se adapta a sus necesidades verificando que se cumple lo ofertado por el proveedor.

Resulta tentador simplificar el proceso de verificación y el entorno de pruebas usando herramientas que no son capaces de recrear un escenario realista, pero está demostrado que esta mentalidad le puede suponer a las organizaciones un alto coste y aumentar la probabilidad de acabar en los titulares por una incidencia de seguridad.

Los beneficios del análisis de antemano y periódico de la solución de seguridad son sustanciales. En la mayoría de los casos el servicio de validación y evaluación no supone ni un 5% del presupuesto destinado a la infraestructura de seguridad y de entrada se consiguen rebajas en los precios de adquisición mucho mayores. El retorno de la inversión global se maximiza porque los sistemas funcionan mejor, son más fiables y requieren menos mantenimiento.

- Sistemas más seguros, precisos, robustos y fiables.
- Reducir los niveles de riesgo, evitando problemas cuya solución es conocida de antemano.
- Reducción del tiempo de comercialización.
- Mayor disponibilidad de los servicios.
- Menor exposición legal.
- Mejor reputación y conservación de la marca de identidad.
- Optimización de la configuración de las plataformas, facilitando su administración
- Reducir la complejidad de las reglas, eliminando políticas innecesarias que deterioren el rendimiento
- Evitar pérdidas económicas.

AYSCOM Celular de Servicios S.L.

c/ Manuel Tovar 36, oficina 1º izq

28034 – Madrid – SPAIN

www.ayscom.com

Teléfono: (+34) 91 376 82 25

Fax: (+34) 91 376 80 56

Contacto: ayscom@ayscom.com / jose_ruiz@ayscom.com