



Examen de vulnerabilidades

"Ethical hacking", el nuevo método para prevenir fraudes informáticos

Cada vez más empresas usan esta técnica que consiste en usar los mismos procedimientos que los hackers para probar la resistencia de los sistemas informáticos

→ principales noticias 1 de 8



"Ethical Hacking" es la técnica cada vez empleada en el mundo de la seguridad informática de las empresas y organismos públicos para prevenir fraudes y ataques de hackers.

En otras palabras se trata de "provocar" los sistemas de una empresa con simulacros los más pegados a la realidad posible empleando las mismas armas que usa el enemigo para vulnerar, explotar o ingresar. Se lo conoce también el ethical hacking como "Penetration Testing" o "Intrusion Testing".

SERVICIOS

Agregar a mis artículos	0
Imprimir	
Enviar a un amigo.	
Aumentar/Reducir tipografía	



El ingeniero **Pablo Masoero**, Presidente Baicom Networks S.A., empresa especializada en seguridad informática, explica cómo se emplea este recurso y a qué tipo de empresa le conviene instrumentarlo.

Una técnica de auditoría

Se podría decir que como método es el más conveniente, pues aunque el atacante tiene tiempo ilimitado para probar y atacar, y el auditor no, con este recurso se hacen pruebas exhaustivas de todos los sistemas con absoluta libertad.

Actividades

Existen tres actividades fuertes:

- **"Security Assessment"**: es un método de auditoría de seguridad no intrusiva, o sea se buscan fallas pero no se explotan, pero al no tratar de ingresar al sistema, no podemos estar seguros ciento por ciento que un atacante no sería capaz de realizarlo.
- **"Penetration Testing"**: con este método se busca ingresar de la manera que se pueda dentro de un sistema. Una vez obtenida la muestra de ingreso, se terminan los testeos, ya que quedó demostrado que el sistema era penetrable.
- **"Ethical Hacking"**: se busca ingresar dentro de un sistema de todas las maneras posibles, para alcanzar a determinar la totalidad de las maneras posibles por medio de las cuales un atacante podría entrar al sistema.

Lo más importante de todo esto es el término "Ethical", que se refiere a lo ético de la actividad, dado que la información que se maneja es sensible, y es de vital importancia tener en claro quién va a poder acceder a esa información y quien no.

En seguridad hay un punto en el cual se usa un modelo similar al "trust", es decir, uno tiene que tener confianza en la empresa que esta realizando estos trabajos por dos motivos excluyentes.

El primero es porque el "Ethical Hacking" depende 99% del recurso humano que se dedica a esa tarea, pues

PUBLICIDAD

PUBLICIDAD

FRÁVEGA
PRIMEROS SIEMPRE
AL PRECIO QUE BUSCAS

no existe para que esto sea realmente válido, ningún software que automatice la tarea.

El segundo motivo se debe a que dependiendo de quien tenga acceso a esa información en primer lugar (la idea es que no sea un atacante), podría llegar a lucrar con la misma.

Chicos malos y buenos

Aquí, es donde nacen los términos de "Blackhats" (se refiere a los "chicos malos") y "Whitehats" (remite a los "chicos buenos").

El procedimiento básicamente se resume en:

- **"Footprinting"** (poder reunir información de distintos lugares).
- **"Scanning"** (poder examinar quien esta presente en esa red).
- **"Enumeration"** (poder enumerar cuales son los servicios que se prestan).
- **"Hacking/Exploiting"** (poder explotar las vulnerabilidades encontradas).
- **"Vulnerability Research"** (investigación de nuevas vulnerabilidades)

Para empresas medianas y grandes

En general, las empresas que mas solicitan este tipo de servicios son empresas medianas y grandes y cuanto mas presencia internacional tienen, más consumidores de este tipo de servicios son, ya que el mercado internacional esta más conciente de los riesgos que realmente existen.

Las fallas mas insólitas comienzan por la mala configuración de los sistemas, seguido de la trivialidad de los passwords y concluyendo en las vulnerabilidades detectadas de la plataforma. Estos hitos nombrados aisladamente parecen no tener conexión con la vida de un CEO. Justamente lo que hay que entender es qué pasa si se vulnera ese sistema con la operación de la empresa. Esto va mucho más allá de la tecnología en sí misma.

Cuando las empresas reciben los informes del análisis en general quedan muy sorprendidas, ya que no tenían en claro cuanta información que ellos consideraban privada en realidad era pública.

La realidad es que hoy, la gran mayoría de las empresa basan su operación de "core" en algún punto en tecnología, lo cual sirve como parámetro para poder medir cuán seguros deberían estar en una empresa en la que su información es manejada por quien o quienes la propia empresa determine.

Situación del mercado

La situación de seguridad en el mercado es:

- Se producen aproximadamente 200 incidentes de gravedad en Seguridad Informática publicados en el mundo diariamente.
- El 90% de las empresas del mundo son víctimas de algún tipo de ataque informático.
- El 70% de los ataques provienen desde Internet.
- Se espera haber detectado para el 2005 alrededor de 500 nuevas vulnerabilidades.
- En el 2004 los ataques provocaron pérdidas que oscilan entre 40.000 y 50.000M de dólares.

Todo esto puede sonar muy paranoico, pero destaquemos que las empresas hoy deben tener en cuenta como factor de riesgo claro a los posibles incidentes de seguridad, al espionaje informático, entre otros.

No hay que asustarse sino que ser precavido y tratar de tener las cosas lo más ordenadas y seguras posible.

Capacitación de usuarios

La seguridad absoluta es una utopía, pero es fundamental la capacitación y concientización de los usuarios de los sistemas, los periódicos Security Assessment y Penetration Test de las redes y servicios prestados (realizados por un tercero sin intereses en la organización) y las correspondientes adecuaciones que se necesitan para elevar el nivel de seguridad.

La seguridad desarrollada "in house" tiene muy poco efecto, en primer lugar porque la seguridad informática es un nicho tan específico que debe contar con gente muy especializada en el tema y que se esté actualizando constantemente. En segundo lugar, si la persona que realiza las distintas pruebas y recomendaciones tuviera intereses con la empresa o con algún empleado de la misma, estos informes (que en definitiva son los que van a darnos la herramienta para proteger nuestro negocio) van a carecer de efectividad.

En la empresa Baicom todos los colaboradores firman un código de ética y a su vez son controlados por auditores externos, de manera que se pueda garantizar a nuestros clientes la total confidencialidad de su información.

Con esto nace la figura del MSSP "Managed Security Service Provider", que básicamente es una empresa de servicios de seguridad que se dedica a operar la seguridad de distintas empresas, teniendo un know how & expertise muy fuerte en el área.

Ing. Pablo Masoero

Presidente Baicom Networks S.A.

Volver ↩

📌 Suscribirse para recibir
Alertas y Primicias

✉ Enviar esta nota
a un colega

Subir ↗

[QUIENES SOMOS](#) • [RECOMENDAR ESTE PORTAL](#) • [PAGINA DE INICIO](#) • [CONTACTENOS](#)

[POLITICAS DE PRIVACIDAD](#) • [TERMINOS Y CONDICIONES DE USO](#)

Copyright © 2004 Emprendimientos Corporativos S.A. Todos los derechos reservados

