CÓPPOLA & GARCÍA

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 2900 1636 - F +598 2900 1636 ext 4

info@cyg.com.uy
www.cyg.com.uy

Test de intrusión (Penetration Test)

Introducción

Nos encontramos en una época en donde las empresas están sufriendo ataques informáticos cada vez en forma más asidua, basta con ver los informes anuales de amenazas y compararlos con los de años anteriores para poder apreciar la forma acelerada en la que están creciendo los ataques y las enormes pérdidas que esto ocasiona para las empresas, que van desde la perdida de datos críticos, robo de información confidencial, interrupción del servicio y perdida de fiabilidad entre otros.

Debido al permanente cambio y crecimiento de las empresas, la demanda de trabajo que suele tener el área de tecnología y la cantidad de nuevas implementaciones y cambios que deben realizar en un periodo breve suelen provocar brechas de seguridad y dejar cabos sueltos que un atacante puede aprovechar en beneficio propio o de la competencia y perjudicar a la empresa.

Nuestro servicio consiste en ponerse del lado del atacante (hacker) utilizando las mismas herramientas y métodos, para realizar ataques de tipo intrusivo con el objetivo de evaluar el estado de seguridad de los sistemas (firewall, sitios web, correo electrónico,

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 **2900 1636** - F +598 **2900 1636 ext 4**

info@cyg.com.uy
www.cyg.com.uy

dispositivos de red, etc.) y encontrar fallas o vulnerabilidades que pudieran ser utilizadas en perjuicio de la organización.

En caso de encontrar fallas, las mismas se reportan a la organización junto con las medidas que se deben tomar para proceder a solucionarlas y aumentar la fortaleza de la seguridad de la organización. En caso contrario, el reporte puede ser utilizado como un certificado de un estado de seguridad satisfactorio que luego puede ser presentado a auditorias u otras empresas con las cuales haya un intercambio informático o infraestructura compartida.

Para realizar dicha tarea contamos con personal altamente capacitado y certificado por EC-Council, entidad de carácter internacional encargada de certificar a los pentesters (ethical hackers).

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 **2900 1636** - F +598 **2900 1636 ext 4**

info@cyg.com.uy
www.cyg.com.uy

Retorno de la inversión

Lamentablemente en la actualidad muchas empresas no son conscientes de las pérdidas que un ataque de este tipo puede provocar, hasta que son víctimas de uno.

Esto generalmente se debe al desconocimiento de los métodos de un atacante experimentado, que llevan a subestimar al mismo y provocan una sensación de baja probabilidad de que un ataque de este tipo pudiese ocurrir en la organización.

El resultado son perdidas económicas muy altas , entre ellos costos asociados a: Interrupción de servicio o producción detenida, reparación de daños a equipos, software y reconstrucción de datos, compra de nuevos equipos, recambio de personal (especialmente funcionarios de cargo jerárquico alto, ya que cuando ocurre un evento de esta magnitud las organizaciones suelen buscar un responsable que generalmente termina siendo el gerente de sistemas y a veces personal IT en general), contratación de servicios tercerizados para reforzar seguridad y finalmente el test de penetración que si se hubiese hecho desde un principio hubiese evitado todos estos costos tan elevados.

Otro beneficio para la organización es el de obtener soluciones técnicas a problemas de seguridad sin costo asociado, ya que en el 99% de los casos las soluciones que se recomiendan constan de

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 **2900 1636** - F +598 **2900 1636 ext 4**

info@cyg.com.uy
www.cyg.com.uy

simples cambios en la configuración de los sistemas, modificación de parámetros y otros detalles técnicos en general que no insumen más costo que el tiempo que tarda el técnico en corregirlos y esto nos lleva a tener una infraestructura en seguridad integra y completa sin necesidad de adquirir costosos dispositivos de seguridad que generalmente llevan un mantenimiento anual elevado.

Por lo mencionado podemos asegurar que el retorno de la inversión está garantizado ya que además de prevenir daños evita costos que surgen en la medida que la empresa crece y aumentan sus necesidades en infraestructura.

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 2900 1636 - F +598 2900 1636 ext 4

info@cyg.com.uy
www.cyg.com.uy

Metodología del test de penetración

La metodología utilizada está basada en un test del tipo Black-Box, el cual consiste en que partiendo únicamente de la información pública de la empresa se intenta realizar una intrusión mediante los servicios externos.

Los métodos utilizados son los siguientes:

1. **Reconocimiento Pasivo**: Se utilizan técnicas de footprinting para obtener información sobre la empresa, tecnologías utilizadas y servicios publicados. El objetivo en esta etapa además de recopilar información para realizar el ataque es demostrar a la organización que tipo de información se puede obtener públicamente acerca de la empresa en sí, sus sistemas y tecnologías, ya que generalmente se obtiene información detallada que habitualmente subestimada.

2. **Reconocimiento Activo**: Se utilizan técnicas de escaneos de puerto, servicios y sistemas operativos para obtener información sobre dispositivos utilizados y que servicios/aplicaciones se encuentran. Llegado a este punto hacemos un mapa de red con los dispositivos y servicios detectados que luego vamos a adjuntar en el reporte para que

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 2900 1636 - F +598 2900 1636 ext 4

info@cyg.com.uy
www.cyg.com.uy

la organización sea consciente de la información con la que cuenta un atacante.

3. **Escaneo de Vulnerabilidades**: En base a la información obtenida anteriormente se procede a buscar vulnerabilidades en los sistemas detectados. Luego cada una de estas vulnerabilidades serán especificadas en el reporte detallando una explicación, gravedad de las mismas y posibles soluciones.

4. **Explotación de Vulnerabilidades**: Se procede a explotar las vulnerabilidades encontradas con el objetivo de obtener acceso y elevar privilegios en los sistemas objetivos y/o obtener información confidencial. El objetivo es que la organización conozca que metodología puede utilizar un atacante para penetrar las defensas, que datos puede obtener y que daño es capaz de hacer a la organización.

5. **Expansión del Acceso**: A partir de un sistema comprometido se intentan acceder a otros sistemas dentro de la red mediante técnicas de pivoting y nuevos escaneos internos. El objetivo en este paso es que una vez encontrada un brecha que nos permita estar dentro de un sistema vulnerable, evaluar qué posibilidades de acceder desde dicho

MONTEVIDEO
Rondeau 1643, Of. 101 - C.P. 11100
T +598 2900 1636 - F +598 2900 1636 ext 4

info@cyg.com.uy
www.cyg.com.uy

sistema hacía otros sistemas dentro de la red que generalmente son más críticos e importantes para la organización que el sistema vulnerado. De esto modo además de los sistemas de borde podemos evaluar la seguridad perimetral y relevar que importancia puede tener asegurar todos los sistemas de la red y no solo los más críticos.

6. **Mantenimiento de acceso**: Una vez obtenido el acceso a los sistemas o red en general se intenta crear una vía de acceso permanente, de modo de volver periódicamente a conectarse a dichos sistemas sin ser detectado y sin explotar las vulnerabilidades nuevamente. Desde modo podemos evaluar las facilidades que puede tener una atacante para entrar y salir de la organización una vez comprometido el sistema de modo de poder implementar políticas que dificulten esta tarea.

7. **Borrado de huellas**: Se intenta eliminar los registros para que no queden rastros de la intrusión. El objetivo en este paso es el de probar la capacidad de los sistemas para mantener logs y registros de accesos no autorizados.