Red Teaming – Ethical Hacking

Borda Alaby Javier Alejandro
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
javierbor@gmail.com

RESUMEN

El término de Red Teaming es un proceso diseñado para detectar la red, vulnerabilidades y la seguridad mediante la adopción de una prueba. Este proceso también se conoce como "hacking ético", ya que su objetivo final es mejorar la seguridad.

Palabra Clave

Red Teaming, internet, sistema, seguridad, red, vulnerabilidad, conocimiento, servicios, programa, pensamiento, razonamiento.

1. INTRODUCCION

El término "hacker" fue utilizado inicialmente para entusiastas de la computación especializados que podrían "Hackear" su camino a través de problemas técnicos. Hoy en día, los hackers representan una de las principales amenazas contra nuestra infraestructura de información generando vulnerabilidades en el código y eludir las medidas de seguridad. Red Teaming es un proceso diseñado para detectar vulnerabilidades de la red, sistema este proceso también se conoce como "hacking ético" ya que su objetivo final es para mejorar la seguridad. Ethical Hacking es un "arte" en el sentido de que el "artista" debe poseer las habilidades y conocimientos de un potencial atacante (para imitar un ataque) y los recursos para mitigar las vulnerabilidades utilizadas por los atacantes.
El propósito es discutir el papel global de la Red Teaming en la evaluación de un sistema y la seguridad de la red, tratar de justificar la necesidad de tales métodos para proporcionar un conocimiento exacto de la situación para la seguridad de red / sistema.
.

2. ANTECEDENTES

"La seguridad de la información es un modo de pensar de examinar las amenazas de la red y vulnerabilidadesy gestionar el riesgo adecuadamente "-. Eric Maiwald
.
El Computer Security Institute (CSI) informó que el 90% de los encuestados (principalmente grandes corporaciones y agencias gubernamentales) detectaron violaciones de seguridad informática dentro de los últimos doce meses. 80% de estas compañías reconocen la pérdida mensurable financiero como consecuencia de estas infracciones.

La Seguridad sería un proceso fácil si todo lo que tenía hacer es instalar un software, firewall y antivirus, pero la realidad es que la seguridad de información requiere un enfoque de múltiples capas de Información viendo que los ataques vienen de todos los ángulos y con diferentes intenciones.
Las empresas ya no sólo corren el riesgo de ser atacados (hackeados), pero también son legalmente responsables de sus "recursos" que permitan ser utilizado por los hackers para atacar a otras empresas (responsabilidad downstream).
Para ayudar en la gestión de este riesgo, hay muchos tipos de profesionales. Dos de los campos de cultivo de estos profesionales son equipos rojos y azules equipos. Rojo Teaming es el proceso de análisis de vulnerabilidades en un sistema dado o red mediante el modelado de las acciones de un adversario. Trabajar en equipo azul tiene los mismos objetivos que el equipo rojo, pero funciona como un defensor que trabaja con los responsables del funcionamiento de la red o sistema para mitigar el riesgo. Ambos enfoques sólo identificar vulnerabilidades conocidas en los sistemas y no aborda los requisitos para una infraestructura de seguridad global.

Con el fin de proporcionar servicios completos de seguridad en la información, una organización debería optar como mínimo las siguientes directivas de seguridad:
Política de información, Política de seguridad, Administración del sistema, procedimientos, Procedimientos de respuesta a incidentes, Gestión de la configuración, Metodología de diseño, Planes de recuperación de desastres
Para apoyar estas políticas, la estructura organizativa para la seguridad de la información de una empresa u organización también necesita ser definido. Está a menudo conduce a la designación de un oficial de seguridad y directores de seguridad (para los sitios, divisiones o departamentos) para gestionar las políticas y prácticas de seguridad.

3. Sistemas de información de seguridad - INFOSEC

Las vulnerabilidades se identifican más rápido que las políticas pueden modificarse o cambios necesarios puede ser completamente a prueba (antes de implementación). Sin embargo, las medidas generales de seguridad se pueden adoptar para gestionar los riesgos desconocidos o no identificados.Por ejemplo, los planes de recuperación de desastres a menudo son documentos complicados debido a la amplia gama de posibles "desastres" que abarcan.
Los riesgos pueden ser minimizarse si los procedimientos adecuados estén en su lugar cuando los eventos no planificados ocurren. El desarrollo de un Plan de Respuesta a Incidentes del Equipo de Respuesta.
Guías de la organización sobre la manera de reaccionar cuando un evento de seguridad se lleva a cabo. El principal propósito de estos procedimientos es planear lo no planificado.
La mayoría de los profesionales de la seguridad se centran en la identificación de las vulnerabilidades específicas de sistemas en lugar de implementar medidas de seguridad para las amenazas universales. Pasado devastadores para muchas empresas debido a que no tienen una respuesta planificada después de darse cuenta de sus redes estaban siendo atacados. Seguridad de la información pueden ayudar a sus clientes a desarrollar estos procedimientos y proporcionar seguridad de la información preventiva las medidas para proteger contra futuros ataques.

3.1 El Papel de la Red Teaming en Infosec

Red Teaming es sólo un componente de la evaluación de la red y del sistema general de seguridad. Como se ha indicado anteriormente, seguridad de la información es una forma de pensar y un arduo proceso. Esto se debe en parte a la dinámica de la industria, pero también debido en parte al desarrollo de nuevos exploits y vulnerabilidades código. Mantenerse al día con estas vulnerabilidades es un trabajo de tiempo completo.

Proporcionar conocimiento realizando capacitaciones para la empresa para proteger información sensible a través de la cooperación y la participación de los empleados.
Basado en la Evaluación, para diseño una postura de seguridad la creación de políticas para gestionar de forma más eficaz el riesgo para el sistema y red. Evaluar el estado actual mediante la evaluación de riesgo mediante métodos de seguridad y medidas políticas. Identificar y aplicar la herramienta técnica y física controles necesario gestionar el riesgo.

Para determinar el riesgo, vulnerabilidades y amenazas deben ser identificadas. El equipo de Red utiliza herramientas para sondear para vulnerabilidades y puede proyectar las posibles amenazas basado en el alcance de la evaluaciónsolicitada por el cliente. Sin embargo, el enfoque de Red Teaming es más a fondo de lo que la mayoría de los posibles atacantes siguen, porque los intenta burlar la seguridad sólo necesita encontrar una sola vulnerabilidad, mientras que profesionales de la seguridad que encontrar todas las vulnerabilidades posibles para un sistema dado con el fin de evaluar el riesgo asociado. Los atacantes típicamente sólo atacan a una sola vulnerabilidad para un exploit específico, para hacerlo de otra manera aumentaría la posibilidad
Para la detección (cuanto más tiempo pasaba y probaron las vulnerabilidades, la más probable es la acciones atacante se notará). Sin embargo, Red Teaming deben someterse a prueba para todos tipos de ataques (acceso, modificación, denegación de servicio, y el repudio) a proporcionar una evaluación de seguridad completa. Una evaluación completa del equipo rojo debe proporcionar una precisa situación el conocimiento de la posición de seguridad de un sistema dado / red. Pero la identificación de riesgos a través de Red Teaming y otros métodos no pueden proporcionar seguridad de la información
Solo, la empresa / organización debe continuar con el proceso en Infosec. Para gestionar adecuadamente el riesgo y proporcionar protección de seguridad.

4. Herramientas y métodos de trabajo en equipo RED

4.1 Análisis de Riesgos

Un método sistemático de identificación de los activos de un proceso de datos sistema, las amenazas a esos bienes y la vulnerabilidad del sistema ante esas amenazas.

4.2 Evaluación

Una evaluación del equipo rojo evalúa distintas áreas de la seguridad en una de varias capas enfoque. Cada área de seguridad define cómo el objetivo (sistema / red) será evaluado. Siguiendo el concepto de defensa en profundidad, El objetivo debe ser probados en cada capa de la posible intrusión / ataque. El enfoque por capas de Defensa en profundidad:

Este concepto de seguridad en capas contempla la ejecución de controles de seguridad en cada capa. Una vulnerabilidad identificada menos una capa puede estar protegido en otro capa de minimizar el riesgo asociado de la vulnerabilidad. Las pruebas del equipo Red cumplimiento de las políticas de los controles de seguridad en cada capa. Y el control es sometido de una manera específica para el área de seguridad al que se aplica. La siguiente tabla se muestra las áreas de evaluación de vulnerabilidad de prueba.

5. El Proceso de Red Teaming

Normalmente, los equipos rojos son entidades de terceros contratados para realizar una investigación imparcial evaluación de la red o sistema. El cliente establece el alcance de la proyectar para especificar el área de la información a ser evaluada. Antes de que el equipo rojo pueda proceder, varias consideraciones legales deben ser abordadas. El equipo debe tener el permiso explícito y directo para realizar la prueba por parte del cliente. Esta También debe incluir una renuncia a las repercusiones en caso de un desastre debería ocurrir en el proceso de pruebas. El equipo rojo es responsable de suministrar al cliente un plan detallado, así como una lista de métodos y herramientas que se utilizado durante la evaluación. Cualquier prueba realizada fuera del ámbito declarado por el cliente, puede ser considerada como un ataque injustificado por el Equipo Rojo. El cliente mantiene todos los derechos de propiedad e información de datos y en ningún momento caso de que el equipo rojo a propósito desestabilizar la confidencialidad o disponibilidad de esa información.
Jessica Lowery en su artículo de "Pruebas de Penetración: The Hacker de terceros", discute muchas de las razones para externalizar las evaluaciones de seguridad. Más importante aún, la externalización demuestra una evaluación imparcial de una compañía

6. Metodología Red Teaming

El requisito más importante para el trabajo en equipo rojo es el consentimiento del cliente. Debido a que, por definición y por fin, el equipo rojo tiene un enfoque similar al atacante pruebas de seguridad, para iniciar una evaluación sin permiso explícito es legalmente percibido como un ataque injustificado en el sistema / red. Dicho esto, muchas evaluaciones equipo rojo se mantuvo a propósito de la red y el sistema de administradores como un medio de probar la respuesta a eventos de seguridad personal o para prueba IDS o PIR. El consentimiento debe provenir de los grupos de interés y de seguridad tomadores de decisiones. El asesor legal también puede estar involucrado en ambos lados para la definición de pruebas de alcance y el seguimiento del proceso y la confidencialidad.
El alcance de la evaluación Red Teaming puede ser muy general o muy específica la hora de definir lo que la evaluación incluirá o dirección. El ámbito de aplicación de la proyecto depende del tiempo o el costo de la evaluación y / o en el objetivo de la evaluación tal como se define por el cliente. Puede que no sea financieramente viable evaluar la seguridad de toda la red / sistema (debido al tiempo necesario para realizar la evaluación, el tamaño físico del sistema / red o el número de servicios que requieren una evaluación) de modo que el cliente puede limitar el alcance de la proyecto. Por ejemplo, si una compañía está llevando a cabo una evaluación del equipo rojo como parte de una auditoría de seguridad anual, sólo podrán optar por probar un segmento de la / red de seguridad del sistema (es decir, la seguridad en Internet, seguridad inalámbrica, social
Ingeniería, etc.) El alcance también ayudará a definir la profundidad de las pruebas y, en cierta medida, los resultados esperados. El cliente puede solicitar la verificación de integridad de datos sin comprobar disponibilidad y confidencialidad de prueba sin rendición de cuentas. De modo que los resultados de la evaluación del equipo rojo se adaptarán al cliente objetivo.

Red Teaming se confunde comúnmente como pruebas de penetración justo (pen-testing) cuando, en realidad, de la pluma de pruebas es un componente de la evaluación Red Teaming. Pen- prueba utiliza varios métodos y herramientas para acceder, obtener información o para causar daño a una red / sistema de sondeo en busca de vulnerabilidades conocidas. Pen-analizar Análisis de la ejecución mientras que Red Teaming diseño tests. Por descripción, pluma de pruebas es un análisis externo detallada de una red y sistemas asociados desde la perspectiva de un atacante potencial. Este método de pruebas de seguridad es útil en el proceso de Red Trabajar en equipo para la prueba de puertas traseras y sin parcheados- vulnerabilidades. Pero pen-testing no puede proporcionar un análisis de seguridad completa solo. Si un sistema / red es penetrado, la prueba demuestra que hay al menos una vulnerabilidad de la que se puede
utilizar para obtener acceso al sistema / red.

Y si la pluma de la prueba no tuvo éxito, la prueba sólo demuestra que la persona que realiza la pluma de la prueba no ha podido encontrar ningún hazañas en el sistema (que no garantiza que hay vulnerabilidades no están presentes).
Una buena regla del pulgar para las empresas a seguir en la planificación de Equipo Rojo evaluaciones es identificar las áreas más débiles o la "baja de frutas colgantes" y tienen estas áreas pruebas de vulnerabilidades. Como se dijo anteriormente, los hackers comiencen a una vulnerabilidad específica para acceder (en lugar de numerosos) para evitar la detección.
Por ejemplo, la SQL Slammer infame gusano utiliza una vulnerabilidad individual en Microsoft SQL Server para infectar miles de ordenadores conectados a Internet.
Así que cualquier base de datos utilizando SQL como backend podría ser un objetivo (por ejemplo, una baja altura fruta).
Hacking Ético deberá seguir estrictamente las directrices aprobadas previamente las pruebas que sean establecidos con el cliente.

El equipotambién debe documentar todos los pasos / procedimientos en las pruebas con el fin de volver sobre las acciones del equipo en caso de una incidente debido a las pruebas o para volver a probar / verificación de resultados, de ser necesario. A finalización del esfuerzo Red Teaming todos los resultados deberán presentarse a la cliente en un informe final detallando las vulnerabilidades descubiertas y cómo cada uno fue descubierto.

El informe también deberá hacer una evaluación de la nivel de riesgo global de la red / sistema, además del nivel de riesgo de cada uno vulnerabilidad. El informe final es tan importante como la propia prueba, ya que se dirige al cliente a tomar medidas de seguridad adicionales.

7. Referencias

[1] Disponible en: http://www.cert.org.mx
[2]Alejandro Reyes Plata - Ethical Hacking.*Processing system.* Disponible en:*www.atis.org*
[3] The Society for Competitive Intelligence Professionals. Disponible en: http://www.scip.org/ci/
[4] Cohen, Fred. “The 50 Ways Series”

.