CEH – Hacker Ético Certificado

El CEH (Certified Ethical Hacker) es la certificación desarrollada, independientemente de los fabricantes tecnológicos, por el EC-Council (International Council of Electronic Commerce Consultants). Es una de las **más reconocidas internacionalmente** en el campo del Hacking Ético y la Auditoría de Sistemas Informáticos.

2.1.2 Proceso de prueba de penetración – puntos esenciales

El trabajo de un probador de penetración es extremadamente importante. Las computadoras y las redes están constantemente bajo ataque. Para combatir a estos piratas informáticos, las organizaciones contratan probadores de penetración.

Las pruebas de penetración son la práctica de encontrar vulnerabilidades y riesgos con el propósito de proteger una computadora o un sistema de red. Los términos pruebas de penetración y piratería ética a menudo se usan indistintamente. Sin embargo, la piratería ética es un término general que incluye todos los métodos de piratería. Las pruebas de penetración son parte de la piratería ética.

Esta lección cubre los siguientes temas:

- Equipo rojo contra equipo azul

- Metodología de piratería ética
- Ciclo de vida de las pruebas de penetración
- Marcos de prueba de penetración
- Tipos de pruebas de penetración

Equipo rojo vs. Equipo azul

Los especialistas en seguridad ofensiva se conocen como el equipo rojo o hackers éticos. Los especialistas en seguridad defensiva se conocen como el equipo azul.

Metodología de Ethical Hacking

Hay cinco fases en la metodología de piratería ética:

Fase	Descripción
Realización de reconocimiento	En esta fase, el pirata informático comienza a recopilar información sobre el objetivo. Esto puede incluir la recopilación de información disponible públicamente, el uso de técnicas de ingeniería social o incluso el buceo en basureros.
Escaneo y enumeración	El escaneo es una extensión natural del reconocimiento. El pirata informático utiliza varias herramientas para recopilar información detallada sobre la red, los sistemas informáticos, los sistemas en vivo, los puertos abiertos y otras funciones. La extracción de información como nombres de usuario, nombres de computadoras, recursos de red, recursos compartidos y servicios se conoce como enumeración. La enumeración es parte del paso de exploración.
Estableciendo acceso	En esta fase, el pirata informático utiliza toda la información recopilada a través del reconocimiento y el escaneo para explotar las vulnerabilidades encontradas y obtener acceso.
Mantener el acceso	Una vez que el hacker ha obtenido acceso, puede usar puertas traseras, rootkits o troyanos para establecer un acceso permanente al sistema.
Borrar pistas	El último paso en el proceso de piratería es limpiar pistas. El pirata informático sobrescribe los archivos de registro para ocultar el hecho de que alguna vez estuvieron allí.

Ciclo de vida de las pruebas de penetración

Otra metodología es el ciclo de vida de las pruebas de penetración. El ciclo de vida de las pruebas de penetración es casi idéntico al proceso de piratería ética. Los pasos son:

1. Realización de reconocimiento
2. Escaneo y enumeración
3. Estableciendo acceso

4. Mantener el acceso
5. Reportando

La única diferencia es el enfoque en la documentación de la prueba de penetración. Es importante un informe detallado de las pruebas realizadas y todo lo que se descubrió.

Marcos de prueba de penetración

Se han desarrollado múltiples marcos de prueba de penetración y se utilizan en situaciones apropiadas.

Marco de referencia	Descripción
Proyecto de seguridad de aplicaciones web abiertas (OWASP)	Describe técnicas para probar las aplicaciones web y los problemas de seguridad de servicios web más comunes.
Manual de metodología de pruebas de seguridad de código abierto (OSSTMM)	Intenta crear un método aceptado para una prueba de seguridad exhaustiva.
Publicación especial 800-115 del Instituto Nacional de Estándares y Tecnología (NIST SP 800-115)	Es una guía de los aspectos técnicos básicos de la realización de evaluaciones de seguridad de la información.

Tipos de pruebas de penetración

La siguiente tabla identifica los diferentes tipos de pruebas de penetración:

Tipo	Descripción
Caja negra	El hacker ético no tiene información sobre el objetivo o la red. Este tipo de prueba simula mejor un ataque externo e ignora las amenazas internas.
caja blanca	El hacker ético tiene pleno conocimiento del objetivo o la red. Esta prueba permite una prueba completa y exhaustiva, pero no es muy realista.
Caja gris	El hacker ético recibe información parcial del objetivo o la red, como configuraciones de IP o listas de correos electrónicos. Esta prueba simula una amenaza interna.

2.1.3 Preguntas de prácticas

1. Las pruebas de penetración son la práctica de encontrar vulnerabilidades y riesgos con el propósito de proteger un ordenador o una red. ¿Las pruebas de penetración están comprendidas en cuales de estos?

A. Escaneo de red

B. Equipo azul

C. Hacking ético

D. Equipo rojo

2. Heather está realizando una prueba de penetración. Ella ya ha reunido mucha información valiosa sobre su objetivo. Heather ha utilizado algunas herramientas de hackeo para determinar que, en su red objetivo, una computadora llamada Production Workstation tiene el puerto 445 abierto. ¿Qué paso en la metodología de hacking ético está realizando Heather?

A. Acceder
B. Mantener el acceso
C. Reconocimiento
D. Escaneo y enumeración

3. ¿Cuál de los siguientes es el tercer paso en la metodología de piratería ética?

A. Escaneo y enumeración
B. Obtener acceso
C. Reconocimiento
D. Limpiar el rastro

4. Miguel está realizando una prueba de penetración en la aplicación basada en web de su cliente. ¿Qué marcos de prueba de penetración debe utilizar Miguel?

A. ISO/IEC 27001
B. OSSTMM
C. NIST SP 800-115
D. OWASP

5. El ciclo de vida de las pruebas de penetración es una metodología común utilizada al realizar una prueba de penetración. Esta metodología es casi idéntica a la metodología de piratería ética. ¿Cuál de las siguientes es la diferencia clave entre estas metodologías?

2.2.2 Datos tipo actor de amenazas

Un actor de amenazas es una persona u organización que representa una amenaza para la seguridad de una organización. Esto puede ser una amenaza interna o externa. Algunas amenazas ni siquiera son maliciosas; pueden ser causados por negligencia interna.

En esta lección se tratan los siguientes temas:

- Tipos de actores de amenazas
- Amenaza persistente avanzada

- Modelado de amenazas

Tipos de actores de amenazas

Los actores de amenazas generalmente caen en diferentes categorías basadas en sus habilidades y motivación.

Tipo	Descripción
Sombrero blanco	Este es un hacker experto que utiliza sus habilidades y conocimientos sólo con fines defensivos. Un hacker sombrero blanco sólo interactuará con un sistema al que tienen permiso explícito para acceder. Estos son los hackers éticos.
Sombrero negro	Este hacker también es muy hábil, pero utiliza sus conocimientos y habilidades con fines ilegales o maliciosos. Un sombrero negro también se conoce como una galleta. Son muy poco éticos.
Sombrero gris	El hacker sombrero gris cae en el medio del sombrero blanco y los hackers sombrero negro. El sombrero gris puede cruzar la línea de lo que es ético, pero por lo general tiene buenas intenciones y no está siendo malicioso como un hacker sombrero negro.
Hacker suicida	Un hacker que sólo está preocupado por derribar su objetivo por una causa. Este hacker no tiene ninguna preocupación con ser atrapado o ir a la cárcel- su única preocupación es su causa.
Terrorista cibernético	Este hacker está motivado por creencias religiosas o políticas y quiere causar una interrupción severa o miedo generalizado.
Hacker patrocinado por el Estado	Un hacker que trabaja para un gobierno e intenta obtener información secreta pirateando otros gobiernos.
Hacktivista	Un hacker cuyo propósito principal es protestar y obtener sus puntos de vista y opiniones por ahí. Los hacktivistas a menudo desfiguran sitios web o utilizan ataques de denegación de servicio.
Guión infantil	Esta persona es extremadamente no calificada y utiliza herramientas y scripts que los hackers reales han desarrollado.

Amenaza persistente avanzada

Independientemente de la motivación y el conjunto de habilidades del hacker, un objetivo para muchos hackers es ejecutar lo que se conoce como una amenaza persistente avanzada (APT). Un APT es un ataque sigiloso que obtiene acceso a una red o sistema informático y permanece oculto durante un

período prolongado de tiempo. Esto significa que el hacker puede seguir volviendo sin ser detectado durante bastante tiempo.

Modelado de amenazas

El modelado de amenazas es el proceso de analizar la seguridad de la organización y determinar los agujeros de seguridad. Una vez que se arma un modelo de amenaza, la organización puede comenzar a proteger sus sistemas y datos.

2.3.3 Datos de selección de objetivos

Antes de comenzar una prueba de penetración, hay muchos detalles que deben ser resueltos. Estos detalles incluyen el tipo de prueba que se está realizando y cualquier limitación de prueba. Después de que se hayan reunido los planes iniciales y los detalles de una prueba de penetración, hay algunos detalles adicionales que deben considerarse. Estos incluyen realizar una evaluación de riesgos, determinar la tolerancia, programar la prueba e identificar las excepciones de seguridad que se pueden aplicar al probador de penetración.

En esta lección se tratan los siguientes temas:

- Planificación de pruebas de penetración
- Excepciones de seguridad
- evaluación de riesgos
- Determinar la tolerancia
- Fluencia de alcance

Planificación de pruebas de penetración

detalle	descripción
cómo	Uno de los primeros elementos a tener en cuenta es el tipo de prueba a realizar, interno o externo. Una prueba interna se centra en los sistemas que residen detrás del firewall. Esto probablemente sería una prueba de caja blanca. Una prueba externa se centra en sistemas que existen fuera del firewall, como un servidor web. Esto sería, más que probable, una prueba de caja negra.
Quién	Determine si el probador de penetración puede usar ataques de ingeniería social dirigidos a los usuarios. Es de conocimiento común que los usuarios son generalmente el eslabón más débil en cualquier sistema de seguridad. A menudo, una prueba de penetración puede dirigirse a los usuarios para obtener acceso. También debe pre-determinar quién sabrá cuándo se está llevando a cabo la prueba.
Qué	La organización y el probador de penetración deben ponerse de acuerdo sobre qué sistemas se centrarán. El probador de penetración necesita saber

	exactamente qué sistemas se están probando y, como no pueden dirigirse a ningún área que no esté especificada por la documentación. Por ejemplo, la organización puede tener un sitio web que no desea que se dirija o pruebe. Algunos otros sistemas que deben examinarse incluyen redes inalámbricas y aplicaciones.
cuando	Programar la prueba es muy importante. ¿La prueba debe realizarse durante el horario comercial? Si es así, esto puede resultar en una interrupción de los procedimientos comerciales normales. Ejecutar las pruebas cuando el negocio está cerrado (durante los fines de semana, días festivos o horas posteriores) puede ser mejor, pero podría limitar la prueba.
Dónde	Por último, ¿se ejecutará la prueba in situ o de forma remota? Una prueba in situ permite mejores resultados de las pruebas, pero puede ser más costosa que una prueba remota.

Excepciones de seguridad

Una excepción de seguridad es cualquier desviación de los protocolos de seguridad operativos estándar. El tipo de prueba (cuadro blanco, cuadro negro, cuadro gris) determinará qué excepciones de seguridad, si las hubiera, se dará a la prueba de penetración.

evaluación de riesgos

El propósito de una evaluación de riesgos es identificar áreas de vulnerabilidad dentro de la red de la organización. La evaluación de riesgos debe examinar todas las áreas, incluidos los datos de alto valor, los sistemas de red, las aplicaciones web, la información en línea y la seguridad física (sistemas operativos y servidores web). A menudo, la prueba de penetración se realiza como parte de una evaluación de riesgos.

Una vez determinadas las vulnerabilidades, la organización debe clasificarlas y averiguar cómo controlar cada riesgo. Existen cuatro métodos comunes para hacer frente al riesgo:

1. Evitación: siempre que puedas evitar un riesgo, deberías hacerlo. Esto significa realizar solo las acciones necesarias, como recopilar solo los datos de usuario relevantes.
2. Transferencia: el proceso de trasladar el riesgo a otra entidad, como un tercero.
3. Mitigación: esta técnica también se conoce como reducción del riesgo. Cuando no se puede evitar ni transferir el riesgo, se deben tomar medidas para reducir el daño que puede ocurrir.
4. Aceptación: a veces el costo de mitigar un riesgo supera los efectos potencialmente dañinos del riesgo. En tales casos, la organización simplemente aceptará el riesgo.

Determinar la tolerancia

Una vez realizada la evaluación del riesgo y identificadas las áreas vulnerables, la organización debe decidir su nivel de tolerancia en la realización de una prueba de penetración. Puede haber áreas de operación que absolutamente no pueden ser derribadas o afectadas durante la prueba. Las áreas de riesgo que se pueden tolerar deben colocarse en el ámbito de trabajo, y es posible que sea necesario colocar áreas críticas fuera del alcance de la prueba.

Fluir de alcance

En la gestión de proyectos, uno de los problemas más peligrosos es el rastreo del alcance. Esto es cuando el cliente comienza a pedir pequeñas desviaciones del alcance del trabajo. Esto puede hacer que el proyecto se salga de la pista y aumente el tiempo y los recursos necesarios para completarlo. Cuando se solicita un cambio en el ámbito de trabajo, se debe rellenar y acordar una orden de cambio. Una vez hecho esto, se pueden completar las tareas adicionales.

[Ir al inicio de página]