Introducción a la piratería ética

- **Introducción**
- **Topología de laboratorio**
- **Ejercicio 1 - Aprenda sobre piratería ética**
- **revisión**

Introducción

Hackeo ético
Caja gris
Caja blanca
Caja negra
Ética

Bienvenido al Laboratorio de **Introducción a la** Práctica de **Hacking Ético**. En este módulo, se le proporcionará la información necesaria para desarrollar su conocimiento.

Los resultados del aprendizaje

En este módulo, completará los siguientes ejercicios:

- Ejercicio 1 - Aprenda sobre piratería ética

Después de completar este laboratorio, tendrá más conocimiento de:

- Hackeo ético
- La necesidad de piratería ética
- La metodología de piratería ética
- El aspecto ético de la piratería ética
- Tipos de actores de amenazas
- La diferencia entre Black Box vs. White Box vs. Gray Box Hacking
- Ataques de la vida real

Objetivos del examen

Los siguientes objetivos del examen están cubiertos en este laboratorio:

- **5.2** Metodologías de evaluación de seguridad de la información
- **7.1** Ética de la seguridad de la información

Nota: *Nuestro enfoque principal es cubrir los aspectos prácticos y prácticos de los objetivos del examen. Recomendamos consultar el material del curso o un motor de búsqueda para investigar temas teóricos con más detalle.*

Duración del laboratorio

Tomará aproximadamente **30 minutos** completar este laboratorio.

Ayuda y apoyo

Para obtener más información sobre el uso de Practice Labs, consulte nuestra página de **Ayuda y Soporte** . También puede elevar un ticket de soporte técnico desde esta página.

Haga clic en **Siguiente** para ver la topología de laboratorio utilizada en este módulo.

Topología de laboratorio

Este laboratorio contiene materiales de apoyo para Certified Ethical Hacker v10.

Haga clic en **Siguiente** para continuar con el primer ejercicio.

Ejercicio 1 - Aprenda sobre piratería ética

La piratería ética (también conocida como prueba de penetración) es un ciberataque simulado para explotar las vulnerabilidades en una red y los sistemas. Localiza las vulnerabilidades, luego intenta explotarlas. Una persona que realiza piratería ética puede intentar una violación de aplicaciones, protocolos, interfaces de programación de aplicaciones (API), servidores, firewalls y cualquier otra cosa que pueda explotarse en una red. La intención principal es descubrir las vulnerabilidades ante un atacante desde el exterior, luego explotarlas para simular el daño que podría causar.

En este ejercicio, aprenderá sobre los fundamentos básicos del pirateo ético.

Los resultados del aprendizaje

Después de completar este ejercicio, tendrá más conocimiento de:

- Hackeo ético
- La necesidad de piratería ética
- La metodología de piratería ética
- El aspecto ético de la piratería ética
- Tipos de actores de amenazas
- La diferencia entre Black Box vs. White Box vs. Gray Box Hacking
- Ataques de la vida real

Tarea 1: piratería ética

La diferencia fundamental entre la piratería y la piratería ética son los permisos. La piratería es cuando una fuente no autorizada accede a una computadora o red, generalmente por razones maliciosas. El pirateo ético es permitido por una persona u organización para explorar la posibilidad de vulnerabilidades dentro de un sistema o una red. La persona que realiza piratería ética se conoce como pirata informático ético, que puede ser contratada o empleada por una organización para ayudarla a fortalecer su seguridad. Los hackers éticos trabajan dentro de los límites legales, asegurando que los datos a los que tienen acceso no sean explotados ni divulgados a terceros (a menos que lo indique la organización).

Una vez que descubre las vulnerabilidades, el pirata informático ético ayudará a la organización con sugerencias sobre cómo repararlas y, por lo tanto, evitar ataques. Por ejemplo, su organización ha desarrollado una nueva aplicación web para una escuela. Se le ha pedido que pruebe la aplicación web y localice vulnerabilidades. Cuando prueba (piratea) la aplicación, descubre que es propensa a los ataques de inyección SQL. Si no ha pirateado esta aplicación y encontró la vulnerabilidad que corregir, entonces un pirata informático podría haberla llevado a cabo, lo que podría comprometer los datos.

Lo que necesita ser protegido:

Mientras trabaja, un hacker ético debe preservar lo siguiente:

- **Confidencialidad**: debe salvaguardar la información que tiene y conoce. Es su responsabilidad asegurarse de que la información no caiga en las manos equivocadas. Puede proteger la información con los permisos y el cifrado adecuados. Si no se aplican, hay posibilidades de divulgación, lo que permite que una persona no autorizada acceda a la información.
- **Integridad**: mantenga la información en su forma original y no permita ninguna alteración no autorizada.
- **Disponibilidad**: Mantenga la información disponible para que las personas autorizadas la utilicen. Si esto no se hace, la información puede perderse.

Tarea 2 - La necesidad de piratería ética

Todos los sistemas en Internet se consideran en riesgo. Los atacantes están equipados con las últimas herramientas y técnicas para atacar sistemas que consideran vulnerables. Para poder proteger los sistemas de sus organizaciones, debe conocer los métodos utilizados por los piratas informáticos y los pasos que puede seguir para evitar sus ataques.

Hay algunas respuestas fundamentales que debes saber:

- **¿Qué buscar**? ¿Qué estás tratando de proteger?
- **Cómo proteger**: una vez que sepa qué necesita protección, ¿cómo va a hacer eso?

Es importante recordar que no se puede proteger todo. Si se desconoce una vulnerabilidad, no hay forma de protegerse contra ella. Aquí es donde entra en juego un hacker ético. Por ejemplo, un atacante puede descubrir y explotar una vulnerabilidad de día cero en su aplicación web. Esto es algo en lo que no habría pensado, pero el atacante estaba un paso por delante de usted. Un hacker ético podría haber descubierto esta vulnerabilidad de antemano.

Como hacker ético, necesitas:

- Comprenda y conozca los sistemas y procesos antes de comenzar cualquier actividad.
- Conozca las reglas de compromiso antes de comenzar cualquier actividad. Debes saber lo que hay que hacer.
- Obtenga permisos por escrito antes de proceder con cualquier tipo de piratería.
- Poder piratear los sistemas de la organización sin causar ningún daño.
- Descubra vulnerabilidades y ayude a la organización a repararlas.
- Use los mismos métodos y técnicas que cree que usaría un atacante para explotar un sistema, aplicación o vulnerabilidad.
- Asegúrese de NO compartir ninguna vulnerabilidad o información descubierta con nadie más que las autoridades designadas.
- Mantenga abierto el canal de comunicación con las autoridades respectivas para que sean conscientes de las vulnerabilidades.
- Presente sus hallazgos al final de la prueba o piratería y compártalos con el cliente.

Tarea 3: la metodología de piratería ética

El pirateo ético replica la metodología de un atacante, por lo que hay ciertos pasos que deben realizarse. Estos pasos incluyen:

> ***Nota**: Los pasos utilizados por una organización pueden variar.*

- Reconocimiento y huella - activa y pasiva
- Exploración
- Enumeración
- Hackear / Ganar Acceso
- Escalada de privilegios

- Mantener el acceso
- Cubriendo pistas
- Puerta trasera
- Informes

Reconocimiento y huella

El reconocimiento es recopilar información sobre el sistema o sistemas objetivo, lo cual es crítico en la piratería ética para identificar los objetivos de ataque. Con la cantidad y el tipo de información que recopila el atacante, pueden formar la estrategia para la piratería ética. La huella ayuda a recopilar información sobre el tamaño de la organización.

Ambas tareas tienen lugar juntas. Por ejemplo, cuando reúne información sobre una red, obtiene los detalles de los sistemas en la red y, al mismo tiempo, conoce la cantidad de sistemas allí.

Hay dos tipos de reconocimiento y huella:

Pasivo

El hacker ético puede usar varias herramientas para obtener información sin interactuar con el sistema. Es un método más seguro ya que no se expone mientras recopila la información. El hacker ético puede buscar información en varios lugares, como:

- Base de datos Whois
- El sitio web del objetivo
- Perfiles en redes sociales de empleados
- Resultados de búsqueda de Google
- Consultas DNS
- Blogs y foros públicos.

El hacker ético también puede usar varias herramientas para recopilar información pasivamente. Algunas de las herramientas clave son:

- QUIEN ES
- Social Media
- Shodan
- Google Hacking
- Consulta de DNS

- La cosechadora
- Reconocimiento
- Maltego

Por ejemplo, suponga que desea buscar www.practice-labs.com en el sitio web whois.domaintools.com. Observe la salida. Se muestra el resultado de practice-labs.com.

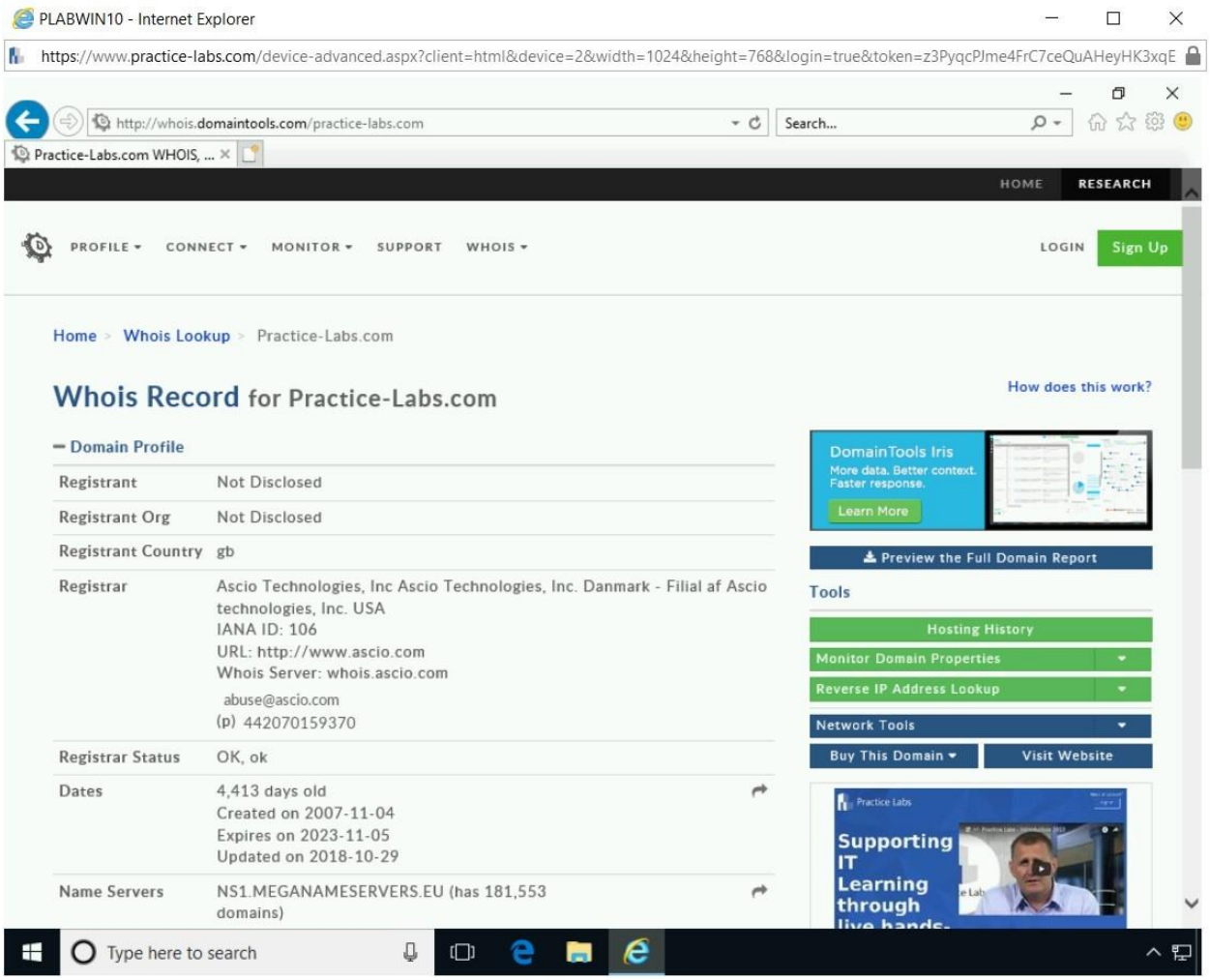

Figura 1.1: Captura de pantalla de Internet Explorer: muestra información sobre el sitio web buscado.

Activo

En el método de reconocimiento activo, el pirata informático ético se conecta con el sistema y recopila información. Aunque este método proporciona información más precisa en comparación con el método pasivo, el riesgo de ser notado y expuesto es mucho mayor. Un ejemplo de

reconocimiento activo es realizar un escaneo de puertos en un sistema. En un escaneo de puertos, el pirata informático ético se conecta con el sistema para obtener la información de puerto abierto.

Hay varias herramientas que se pueden utilizar en el reconocimiento activo. Nmap es una de las herramientas más buscadas para esto. Supongamos que usted, como pirata informático ético, desea escanear la red 192.168.0.0/24 y ver cuántos hosts están utilizando un escaneo de ping. Puedes usar el siguiente comando:

```
nmap -sP 192.168.0.0/24
```

***Nota** : el parámetro -sP se usa para el escaneo de ping. Cuando usa CIDR / 24, Nmap escaneará las 256 direcciones IP en la red.*

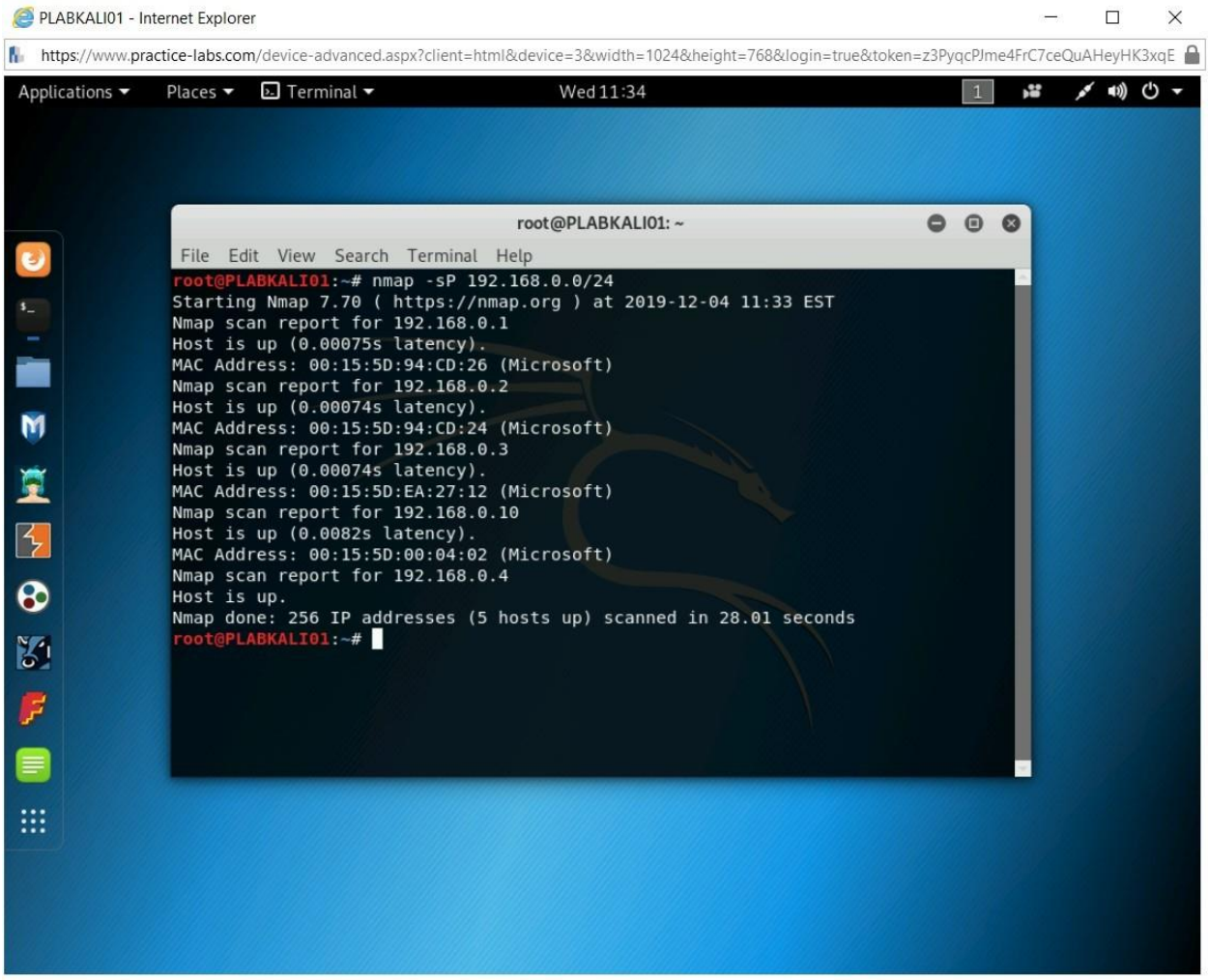

Figura 1.2 Captura de pantalla de Kali Linux: muestra el resultado del comando nmap -sP.

El comando nmap que se muestra arriba hace ping a 256 hosts en la red y regresa con una lista de los hosts que están activos en ese momento.

Escaneo y enumeración

Después de haber explorado la red e identificado los sistemas en vivo en ella, puede continuar con el escaneo y la enumeración. Esto es crítico para la explotación o para obtener acceso.

La enumeración también se considera parte del reconocimiento activo. Con la enumeración, puede encontrar muchos detalles sobre un dispositivo, servidor o servicio.

La enumeración se puede utilizar para buscar información, como:

- Información del sistema operativo, como la versión
- Información de DNS
- Información SNMP
- Usuarios y grupos
- Hashes de contraseñas y contraseñas
- Nombres de host
- Información del dominio
- Ejecución de servicios y procesos

El escaneo encuentra vulnerabilidades que pueden ser explotadas. Por ejemplo, puede usar Nikto para escanear una aplicación web y encontrar vulnerabilidades. Veamos el ejemplo en el que ejecuta el siguiente comando:

```
nikto -host http://192.168.0.10
```

***Nota** : Puede alojar una aplicación web vulnerable y asignarle una dirección IP. Luego, puede usar el comando anterior, reemplazando la dirección IP con la dirección IP de la aplicación web.*

Los resultados muestran las diversas vulnerabilidades descubiertas.

Use esta página para practicas:

http://hackme.org/GB/GB.html

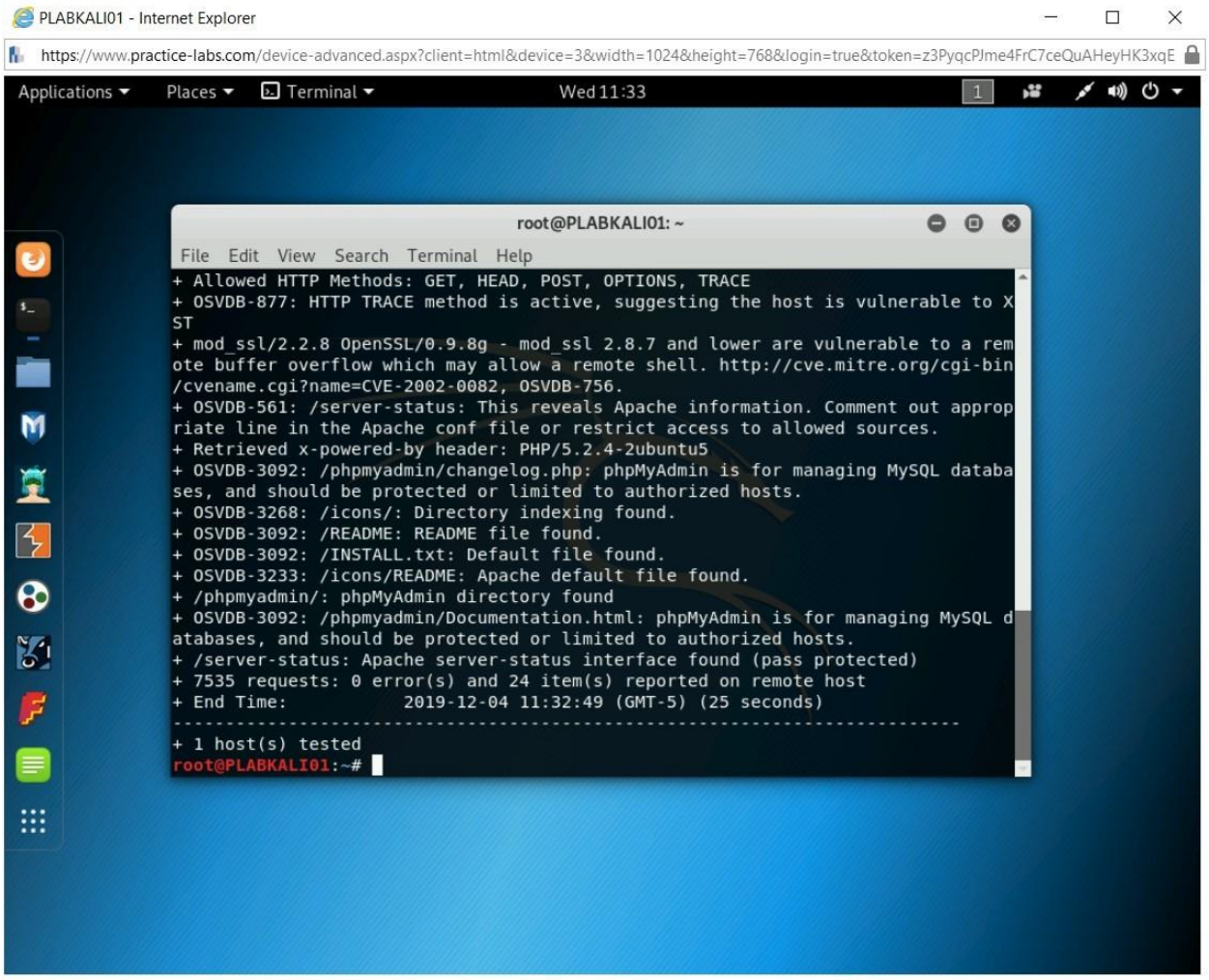

Figura 1.3 Captura de pantalla de PLABKALI01: mostrando la salida del comando nikto.

Ganar acceso (explotación)

Al elegir un ataque para usar para obtener acceso al sistema, se debe tener en cuenta el entorno y la situación. Algunas técnicas de ataque comunes utilizadas en las pruebas de penetración son:

- **Ingeniería social**: este ataque establece la base para todos los demás ataques. Un atacante puede usar diferentes métodos, como el phishing, para desencadenar el ataque.
- **Ataques a aplicaciones web**: pueden incluir ataques como inyección SQL, XSS y XSRF. Estos son aplicables si está realizando una prueba de penetración en una aplicación web.

- **Secuestro de sesión**: esto es útil cuando tiene sesiones sin cifrar. Un atacante puede realizar un secuestro de sesión o un ataque de hombre en el medio.
- **Descifrado de contraseñas**: esto implica cierto nivel de acceso al servidor o sistema, luego se utilizan varias herramientas para descifrar las contraseñas.

Una red privada es más segura que la red pública, que es visible para todos. Al entrar en una red privada, el atacante debe encontrar varios métodos para conectarse. Por ejemplo, el atacante puede usar ingeniería social e implementar malware compartiendo una unidad USB infectada con un usuario.

Si utiliza un método técnico, como un ataque a una aplicación web, primero debe ubicar un servidor web y ver si tiene una aplicación web ejecutándose. Entonces podría explotar la aplicación web.

En otros casos, puede utilizar un método de ingeniería social, como enviar un correo electrónico a un usuario, pretendiendo ser de su banco. El correo electrónico puede tener una URL en la que el usuario debe hacer clic. Una vez que acceden a la URL, se navega a los usuarios a un sitio web que parece ser el sitio web del banco. Luego podría implementar malware en su sistema.

Mantener el acceso

Supongamos que ha explotado una vulnerabilidad en el sistema operativo Windows y ha obtenido acceso al sistema. No hay garantía de que pueda mantener el acceso. En tales situaciones, debe hacer algo que le permita mantener el acceso si se repara la vulnerabilidad.

Por ejemplo, puede crear una nueva cuenta de usuario con acceso administrativo. Esto le permitirá conectarse con el sistema explotado de forma remota. Alternativamente, instala una puerta trasera o rootkit.

Cubriendo pistas

En cualquier forma de piratería, es probable que dejes rastros en el sistema, lo que posiblemente te detenga o te atrape. Por ejemplo, si crea una cuenta de usuario, se capturará en los archivos de registro. Uno de los métodos

clave utilizados para cubrir pistas es borrar los archivos de registro. Sin embargo, cuando se borran los registros, se crea una nueva entrada en los archivos de registro, mencionando que los registros se han eliminado.

Informes

Debe informar sus hallazgos a la organización o persona que ha solicitado la prueba de piratería ética. El informe incluye vulnerabilidades, exposición de datos confidenciales, su acceso a los sistemas confidenciales y cómo mitigar las amenazas que pudo presentar.

Tarea 4: el aspecto ético del pirateo ético

Un hacker ético debe seguir los principios profesionales y el código de ética.

Por ejemplo, no debe usar la información y los datos de la organización para sus necesidades personales ni hacer un mal uso de ellos con intenciones maliciosas. Además, la información debe protegerse para que no caiga en las manos equivocadas como resultado de la prueba. Cualquier mal uso de sus datos o información podría dar lugar a acciones legales.

Otro aspecto crítico de la piratería ética son los permisos. Por ejemplo, debe tener permiso para hackear un servidor web que ejecuta una aplicación web. Si no tiene permiso, se considera piratería, no piratería ética.

> ***Nota** : El Código de Ética está disponible*
>
> *aquí: **https://www.eccouncil.org/code-of-ethics/***

Si tiene la certificación CEH y no se adhiere a la ética definida por EC-Council, puede perder su certificación.

Tarea 5 - Tipos de actores de amenazas

Como hacker ético, debe conocer los diferentes tipos de actores de amenazas, que son cualquier entidad detrás de una amenaza, lo cual es un peligro potencial para un activo. Un actor de amenaza se puede clasificar en gran medida en tres categorías:

- **Amenaza interna** (por ejemplo: un empleado deshonesto)

- **Amenaza externa** (por ejemplo, un grupo criminal)
- **Amenaza natural** (p. Ej., Huracán o tsunami)

Los actores de amenazas buscan vulnerabilidades para explotar. Cuando una vulnerabilidad o debilidad está presente en la red, el servidor o la aplicación, el actor de la amenaza está en riesgo.

Ejemplos de actores de amenazas.

Hackers

Hay tres tipos de piratas informáticos: sombrero negro, sombrero gris y sombrero blanco.

Los hackers de sombrero negro piratean los sistemas con intenciones maliciosas. También se conocen como galletas saladas.

Los hackers de sombrero blanco son hackers éticos o zapatillas de deporte. Generalmente son contratados o contratados por organizaciones para evaluar sus parámetros de seguridad.

Los hackers de sombrero gris son una combinación de hackers de sombrero blanco y sombrero negro. Entran en sistemas sin pedir permiso. Sus intenciones no son maliciosas; Quieren demostrar sus habilidades. Sus acciones aún se consideran ilegales, ya que no buscan permiso para realizar sus acciones.

Script Kiddies

Un script kiddie es alguien que no tiene la experiencia de un hacker y confía en herramientas listas para usar, ya que no pueden escribir su propio código. Debido a la falta de experiencia, sus ataques no son sofisticados.

Hacktivistas

Los hacktivistas son actores de amenazas que son hackers con una misión específica, que podría ser política o social. Uno de los ataques más comunes que usan es una Denegación de servicio distribuida (DDoS). Están decididos a cumplir su causa y pueden trabajar en grupos con hackers de ideas afines.

Estado-nación / Estado patrocinado

Estos actores de amenazas son entidades bien financiadas y bien organizadas que comprometen sus actividades con el respaldo de gobiernos o similares. Los atacantes patrocinados por el estado generalmente se centran en infiltrarse en organizaciones más grandes con la intención de robar grandes cantidades de datos confidenciales y de misión crítica.

Amenazas internas

Estos actores de amenazas son internos de una organización y pueden realizar actividades maliciosas de manera intencional o no. Algunas de las actividades que podrían realizar incluyen la entrega de información confidencial o confidencial a otros sin querer, o la venta de información a otro actor de amenazas que quiera abusar de ella.

Es muy difícil detectar una amenaza interna ya que la persona es parte del sistema. Tendrían acceso a los datos, junto con el conocimiento de las operaciones y procesos internos. Dado que están dentro de la red, sus acciones son difíciles de rastrear mediante herramientas como firewalls.

Tarea 6: la diferencia entre el cuadro negro frente al cuadro blanco frente al pirateo del cuadro gris

Como hacker ético, se le puede pedir que realice diferentes tipos de piratería o pruebas de penetración. La organización, después de decidir el alcance de la tarea, también puede pedirle que realice un cierto tipo de piratería o pruebas de penetración, que generalmente se clasifican en tres tipos:

- Caja negra
- Caja gris
- Caja blanca

Caja negra

Una prueba de caja negra también se conoce como prueba de penetración de conocimiento cero. En la prueba de recuadro negro, no tiene ninguna información sobre la red, excepto un rango de IP. Por lo general, es una entidad externa que necesita explotar la red o los sistemas al máximo. La

organización espera que recopile información por su cuenta, descubra vulnerabilidades y luego las explote. Una prueba de caja negra lleva más tiempo ya que no sabe nada sobre la red o sus sistemas. Sin embargo, es más efectivo porque puede proporcionar una evaluación precisa de la seguridad de la red, y simula de cerca un ataque de la vida real que podría ocurrir.

Caja blanca

La prueba de penetración de la caja blanca es completamente opuesta a la prueba de la caja negra. También se conoce como Full Knowledge Penetration Testing. Tiene toda la información necesaria para realizar pruebas de penetración. Por ejemplo, la organización compartiría la siguiente información:

- Diagramas de red
- Lista de sistemas con su dirección IP
- Rangos de IP
- Credenciales de usuario para iniciar sesión en los sistemas

La prueba de penetración de la caja blanca lleva menos tiempo que la prueba de la caja negra porque tiene la información requerida disponible. Sin embargo, es posible que no proporcione resultados precisos ya que no es la misma situación en la que se encontraría un atacante externo.

Caja gris

La prueba de caja gris es una combinación de caja negra y caja blanca. Para empezar, tiene información limitada, pero no tiene credenciales de usuario ni detalles de configuración. Por ejemplo, la organización puede compartir el nombre de la aplicación y su dirección IP, pero no proporciona la versión de la aplicación o los servicios que está ejecutando. Esto lo hace un poco más preciso que una prueba de caja blanca.

Tarea 7 - Ataques de la vida real

Como hacker ético, es útil comprender las mentes de los hackers. Uno de los mejores métodos para hacer esto es estudiar los principales ataques que ocurrieron en el pasado. Algunos de estos ataques principales incluyen:

Adobe

En octubre de 2013, Adobe reveló que había sido atacado. Aquí hay un breve resumen del ataque:

- Eliminación de la información personal de 2.9 millones de clientes por parte de los atacantes: credenciales de inicio de sesión, nombres, información de la tarjeta de crédito, incluidas las fechas de vencimiento
- Se accedió a identificaciones de clientes y contraseñas cifradas
- El código fuente fue robado para ColdFusion, Acrobat Reader y Photoshop

Sony

Sony había estado bajo grandes ataques dos veces.

El primer incidente ocurrió en abril de 2011, lo que llevó al cierre de Sony PlayStation, Sony Online Entertainment y Qriocity por un mes.

Aquí hay un breve resumen:

- Se filtró información personal de 77 millones de cuentas de usuario
- Miles de cuentas bancarias de usuarios se vieron comprometidas

La vulnerabilidad explotada fue la información no cifrada en la red de Sony, que fue secuestrada mediante ataques de inyección SQL.

Noviembre 2014

En el segundo gran ataque, Sony Pictures Entertainment fue el objetivo.

Aquí hay un breve resumen:

- El ataque se realizó usando un gusano
- El ataque fue realizado por un grupo de hackers llamado Guardians of Peace, que terminó robando más de 100 terabytes de datos de Sony
- Las vulnerabilidades explotadas fueron una mala gestión de la infraestructura y una configuración incorrecta

Estas son algunas otras grandes organizaciones que han sido pirateadas en los últimos años:

- Facebook
- Google+
- Cambridge Analytica
- Mi herencia
- Quora
- Timehop
- Cathay Pacific Airways
- T-Mobile
- British Airways
- Yahoo
- Marriott International
- eBay
- Uber

En el pasado, la Oficina Federal de Investigaciones (FBI) ha utilizado ex hackers para localizar a algunos de los hackers más inteligentes del mundo.

revisión

Bien hecho, ha completado el Laboratorio de **Introducción a la** Práctica de **Hacking Ético**.

Resumen

Has completado los siguientes ejercicios:

- Ejercicio 1 - Aprenda sobre piratería ética

Ahora debe tener un mayor conocimiento de:

- Hackeo ético
- La necesidad de piratería ética
- La metodología de piratería ética
- El aspecto ético de la piratería ética
- Tipos de actores de amenazas
- La diferencia entre Black Box vs. White Box vs. Gray Box Hacking
- Ataques de la vida real