HACKING ÉTICO

AUTOR: RICARDO CASTILLO

NOVIEMBRE: 2020

San Marcos

Introducción

La protección de los sistemas y redes actuales requiere una comprensión amplia de las estrategias de ataque y un conocimiento profundo de las tácticas, herramientas y motivaciones del pirata informático. El creciente uso de metodologías de ataque de ingeniería social exige que cada probador sea consciente de la organización y los hábitos de sus usuarios de TI (personal).

Los Hackers Éticos son expertos que se especializan en las pruebas de penetración de sistemas informáticos y de software con el fin de evaluar, fortalecer y mejorar la seguridad.

Este tipo de pirata informático a menudo se denomina como hacker de 'sombrero blanco' (White hat), con el fin de diferenciarlos de los piratas informáticos criminales, que se conocen como hackers de 'sombrero negro'.

A continuación, se detallan los conceptos relacionados con esta práctica con el objetivo de brindar la información relevante del quehacer y habilidades con las que debe contar un Hacker ético.

Contenido

¿Qué es Hacking ético?

El hacking ético es la práctica que consiste en utilizar las habilidades en sistemas informáticos y de red para ayudar a las organizaciones a probar sus mecanismos y procedimientos de seguridad con tal de identificar debilidades y/o vulnerabilidades.
Las pruebas de un hacking ético se realizan con el conocimiento de los administradores y/o propietarios de los activos a probar, sin la intención de causar daños. Todos los hallazgos detectados se reportan para su subsanación.
Los hackers éticos utilizan las mismas herramientas, trucos y técnicas que los atacantes para descubrir vulnerabilidades que pueden ser explotadas por estos. Uno de los métodos que utilizan son los pentest o pruebas de intrusión.

Realización de Hacking Ético

Para la realización de un hacking ético es necesario lo siguiente:

- Contrato o acuerdo firmado por el cliente o la organización donde se autoriza a realizar las pruebas.

- Acuerdo de confidencialidad de la información (NDA: “Non-Disclosure Agreement”) durante y después de la realización de las pruebas.

- Realizar las pruebas sin sobrepasar los límites acordados con el cliente o organización (alcance).

- Analizar los resultados obtenidos de las pruebas y realizar el informe final.

- Presentar los hallazgos al cliente u organización.

Durante el proceso se intentará responder a:

- ¿Qué información pueden obtener los atacantes del sistema objetivo?

- ¿Qué puede hacer un intruso con la información obtenida acerca del sistema objetivo?
- ¿Se registran los intentos de acceso o los accesos de los atacantes?

Se ejecutarán las siguientes tareas:

- Asegurar que los activos de información están adecuadamente protegidos, actualizados y parcheados.

- Servir de base para la elaboración de planes de acción preventivos y correctivos para la Seguridad de la Información: cuánto esfuerzo, tiempo y dinero se necesitan para una adecuada protección.

- Comprobar que los mecanismos y procedimientos de seguridad cumplen con los estándares y regulaciones de aplicación.

Fases del hacking ético

1. Reconocimiento: fase inicial donde se recopila información acerca de la organización objetivo de las pruebas y se planifican (por ejemplo, los puntos débiles).

2. Escaneo de la red para obtener información específica de los sistemas (sistemas operativos, versiones de software, puertos, etc.). Se suelen utilizar escaneos de puertos con herramientas, como Nmap.

3. Ganar acceso a los sistemas: es la fase donde se consigue el control sobre el sistema, aplicación o máquina. Se usan técnicas como crackeo de contraseñas o secuestro de sesiones.

4. Escalado de privilegios/mantener el acceso: es la fase en la que se conserva el acceso y se obtienen privilegios administrativos en el sistema mediante puertas traseras, rootkits, troyanos, etc.

5. Borrar las evidencias: es el punto en la que se intenta borrar o cubrir las pistas acerca de las actividades realizadas en las pruebas.

Formación Profesional

Las habilidades de un hacker ético son una combinación de habilidades técnicas y personales tales como:

Técnicas:

1. Amplio conocimiento de los principales sistemas operativos.
2. Conocimientos detallados de red: arquitectura, hardware, software, etc.
3. Conocimientos amplios sobre seguridad.
4. Gran conocimiento acerca de los distintos ataques.

Personales:

1. Capacidad de aprender continuamente.
2. Resolución de problemas.
3. Habilidades de comunicación.
4. Concienciación sobre cumplimientos legales, estándares y buenas prácticas.

Conclusiones y recomendaciones

En conclusión, el hacking ético permite mejorar la seguridad informática de instituciones y empresas, asimismo permite adelantarse a posibles ciberataques. Es un mecanismo fiable para detectar vulnerabilidades e implementar así sistemas que mejoren la seguridad. De esta manera los profesionales en Hacking ético manejan un profundo conocimiento de cómo penetrar en la seguridad de una infraestructura en línea para encontrar vulnerabilidades, que en manos de criminales se implementan comúnmente buscar algún provecho poco moral.

Referencias bibliográficas

- Revista Unir (2020) ¿Qué es el hacking ético y cómo se realiza? Recuperado de: https://www.unir.net/ingenieria/revista/hacking-etico/
- Tecología para los negocios. (2020). Qué es el hacking ético. https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica