Los hackers cuentan con unos conocimientos que, en un entorno donde la ciberseguridad adquiere cada vez mayor relevancia, se han vuelto imprescindibles para las empresas. A pesar de que el término “hacker” se ha visto manchado por las malas prácticas, no todo es negativo en ese mundo. Existen expertos en esta área que usan sus habilidades y conocimientos para ayudar a organizaciones a poner a prueba sus mecanismos de seguridad, con el fin de identificar las debilidades o vulnerabilidades de un sistema. A esta práctica se le conoce como hacking ético.

¿Qué es el hacking ético?

Hace referencia al modo en que una persona, utiliza todos sus conocimientos sobre informática y ciberseguridad para hallar vulnerabilidades o fallas de seguridad dentro de un sistema. Los hackers de sombrero blanco son expertos en seguridad de la información que irrumpen en los sistemas informáticos por petición de sus clientes. Se considera ética esta variable porque existe un consentimiento previo por parte de la “víctima”, es decir, el cliente, para detectar las fallas.

El hecho de que estos profesionales entiendan cómo operan los atacantes suele darles una perspectiva más clara sobre cómo prevenir los diferentes ataques y ayudar a las empresas o personas que contratan sus servicios sin ninguna mala intención.

Muchas compañías grandes, como Facebook o Google, suelen ofrecer recompensas a los profesionales en hacking ético que descubren agujeros de seguridad dentro de sus servicios o redes sociales.

¿En qué consiste el hacking ético?

Consiste en atacar de una forma pasiva el entorno de seguridad que ha creado la empresa que solicita este tipo de servicio. El objetivo es que el especialista trate de ponerse en los zapatos de los individuos que, en algún momento, podrían intentar atacar los sistemas o los servidores de dicha empresa, donde ponen en marcha una serie de pruebas o test, llamados “test de penetración” con el fin de poder burlar la seguridad de las diferentes organizaciones para poner a prueba la efectividad de los sistemas de seguridad o demostrar sus debilidades. En caso de encontrar algún error o alguna vulnerabilidad, el hacker tiene que notificar a la empresa que lo contrató por medio de un informe completo y dar soluciones para mejorar la ciberseguridad de la organización en cuestión.

A diferencia de los hackers de sombrero negro, estos no hacen daño a las organizaciones, sino que se convierten en una pieza fundamental para ellas, ayudándolas a no ver comprometidos sus archivos o funcionamiento en general.

¿Qué es un test de penetración en hacking ético?

Es una metodología que consiste en planificar un ataque a una red o plataforma, sin importar su tamaño, para encontrar vulnerabilidades en ella.

Para conseguirlo, es necesario simular diferentes patrones de ataque empleando herramientas desarrolladas por métodos de ataque conocidos. Algunos de los componentes de un test de penetración son:

- Puertos de seguridad: cortafuegos, programas antivirus, filtros de paquetes, etc.
- Elementos de acoplamiento: puertos, conmutadores o routers.
- Servidores web, de base de datos, de archivos, etc.
- Equipos de telecomunicaciones.
- Aplicaciones web de todo tipo.
- Instalaciones de infraestructura: mecanismos de control de acceso.
- Conexiones inalámbricas: bluetooth, WLAN, etc.

Generalmente, los test de penetración se clasifican en:

- Pruebas de caja negra: los especialistas en hacking ético solo tienen a su disposición la dirección de la red, esto quiere decir que se realiza desde el punto de vista de las entradas y salidas que recibe o produce sin tomar en cuenta el funcionamiento interno.
- Pruebas de caja blanca: el punto de partida es un amplio conocimiento de los sistemas, como la IP, el software utilizado y los componentes de hardware, es decir, se llevan a cabo sobre las funciones internas.

El hacking brinda múltiples beneficios. Algunos de los principales son:

- Ahorrar dinero en la implementación de sistemas de seguridad eficientes.
- Impedir catástrofes públicas por ser víctima de algún ataque hacker fuerte.
- Organizar y mantener los sistemas de ciberseguridad para evitar filtraciones.
- Focalizar las inversiones en seguridad eficientemente y no malgastar en sistemas con fallas.
- Concientizar a todos los colaboradores sobre la importancia que supone poner en riesgo los sistemas por el mal uso de contraseñas poco seguras.

Hacking ético vs. hackeo

Las principales diferencias entre el hacking ético y el malicioso son su fundamento y las condiciones generales del hacking. El ético tiene como fin principal brindar protección a las infraestructuras digitales y los datos confidenciales de los ataques para mejorar la seguridad.

El hackeo, por el contrario, se centra especialmente en objetivos malintencionados y destructivos: infiltración y destrucción de sistemas de seguridad, entre muchos otros fines.

La mayoría de los ataques de hackeo van de la mano con acciones criminales, como extorsión, espionaje, parálisis sistemática de cierta estructura, etcétera. Sus intenciones siempre están enfocadas en dañar a su víctima directa o indirectamente.

Esta distinción puede parecer muy obvia, pero existen casos que se encuentran en el límite entre uno y otro. Por ejemplo, algunos hackers enfocados en el campo político pueden perseguir objetivos éticos, pero también destructivos.

Si se busca una distinción entre el hacking ético y el hackeo, desde una perspectiva técnica, se resume en que ambos utilizan los mismos conocimientos y las mismas técnicas y herramientas, pero el hacking ético no centra sus acciones en algún tipo de daño, sino más bien beneficios para quien contrata el servicio de este profesional.

El verdadero reto para un hacker ético es descubrir la vulnerabilidad y no explotarla.