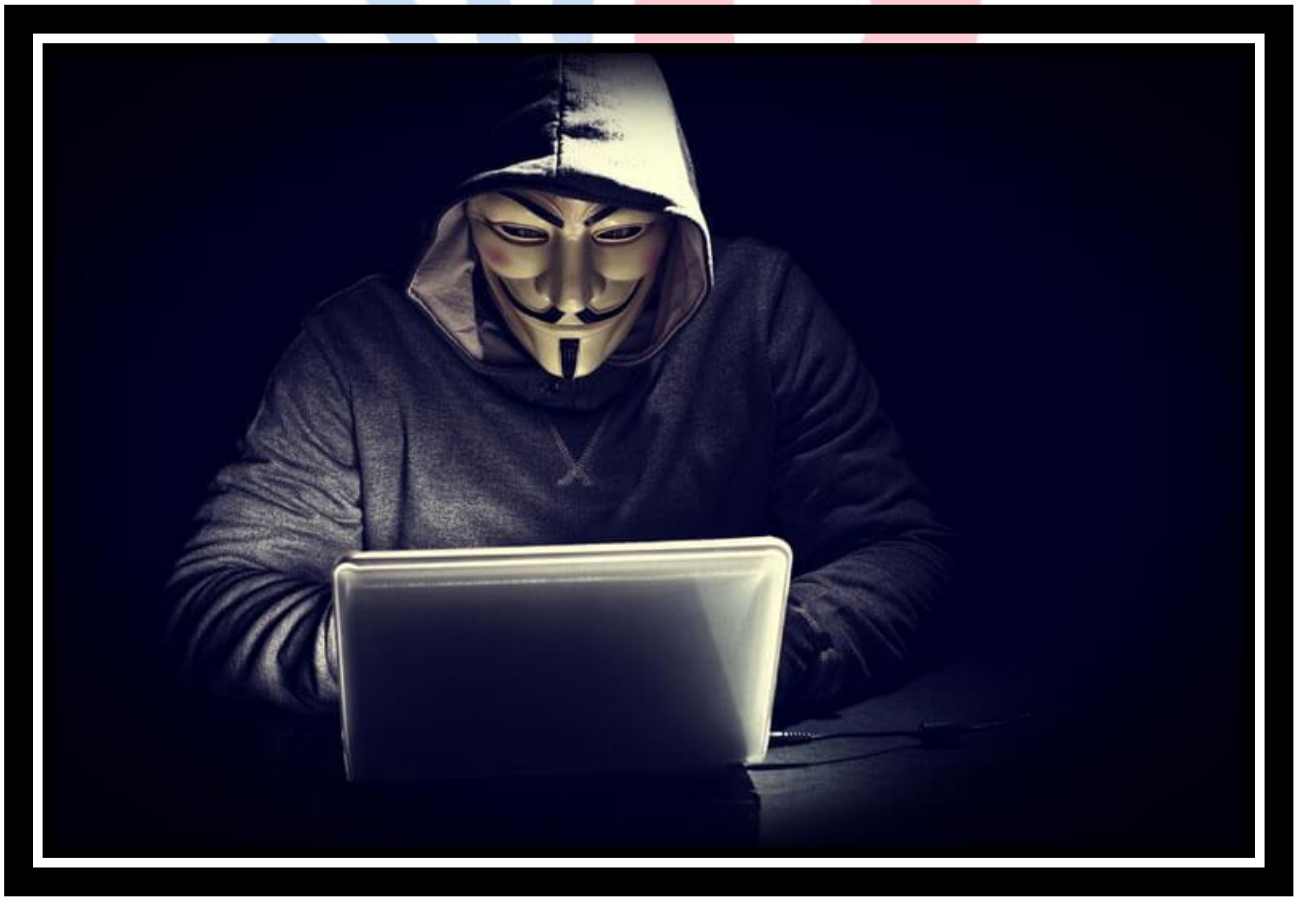
HACKERS

Y

CIBERSEGURIDAD



Formando profesionales

SUMARIO

INTRODUCCIÓN

El término hacker tiene diferentes significados. Según el diccionario de los hackers (The Jargon File) es "todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo", que considera que poner la información al alcance de todos constituye un extraordinario bien. El Diccionario de la lengua española de la RAE, en su segunda acepción, establece que es una "persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora". De acuerdo con Eric S. Raymond el motivo principal que tienen estas personas para crear software en su tiempo libre, y después distribuirlos de manera gratuita, es el de ser reconocidos por sus iguales. El término hacker nace en la segunda mitad del siglo XX y su origen está ligado con los clubs y laboratorios del MIT.

Comúnmente el término es asociado a todo aquel experto de las tecnologías de comunicación e información que utiliza sus conocimientos técnicos en computación y programación para superar un problema, normalmente asociado a la seguridad. Habitualmente se les llama así a técnicos e ingenieros informáticos con conocimientos en seguridad y con la capacidad

de detectar errores o fallos en sistemas informáticos para luego informar de los fallos a los desarrolladores del software que hayan visto que es vulnerable o, directamente, a todo el público.

En español, se recomienda diferenciar claramente entre hacker y ciberdelincuente, ya que, si bien ambos son expertos en colarse en sistemas, el segundo lo hace con propósitos ilícitos.

CONTROVERSIA

En la actualidad, se usa de forma corriente para referirse mayormente a los criminales informáticos ("piratas informáticos" lo define la RAE en su primera acepción), debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. Según Helen Nissenbaum, que los hackers sean mal vistos ayuda al gobierno y a los poderes privados con dos cosas:

1) a definir lo que es normal en el mundo computacional haciendo creer que un buen ciudadano es todo lo que el hacker no es; 2) a justificar la seguridad, la vigilancia y el castigo.

A los criminales se le pueden sumar los llamados *script kiddies*, gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre cómo funcionan. Este uso parcialmente incorrecto se ha vuelto tan predominante que, en general, un gran segmento de la población no es consciente de que existen diferentes significados.

Mientras que los hackers aficionados reconocen los diferentes tipos de hackers y los hackers de la seguridad informática aceptan todos los usos del término, los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como *crackers* (analogía de *safecracker*, que en español se traduce como "un ladrón de cajas fuertes").

Ambigüedad y debate

Los términos hacker y hack pueden tener connotaciones positivas y negativas. Los programadores informáticos suelen usar las palabras hacking y hacker para expresar admiración por el trabajo de un desarrollador cualificado, pero también se puede utilizar en un sentido negativo (delincuentes informáticos) para describir una solución rápida pero poco elegante a un problema. Algunos desaprueban el uso del hacking como un sinónimo de cracker, en marcado contraste con el resto del mundo, en el que la palabra hacker se utiliza normalmente para describir a alguien que se infiltra en un sistema informático con el fin de eludir o desactivar las medidas de seguridad.

Bruce Schneier define a un hacker como aquel que es creativo, aquel que descarta la sabiduría convencional y hace algo más en su lugar. Alguien que ve un conjunto de reglas y se pregunta qué sucederá si no las sigue. En definitiva, es alguien que experimenta con las limitaciones de los sistemas por curiosidad intelectual.

Richard Feynman, quien trabajó en el Proyecto Manhattan, es considerado por Bruce Schneier como un hacker en la muy estricta definición del término. Schneier va mucho más allá: a Galileo y a M. Curie también los considera como tales. Sin embargo, a Aristóteles no y lo ilustra de una manera muy pragmática:

> "Aristóteles tenía alguna prueba teórica de que las mujeres tenían menos dientes que los hombres. Un hacker simplemente habría contado los dientes de su esposa. Un buen hacker habría contado los dientes de su esposa sin que ella lo supiera, mientras ella estaba dormida. Un buen hacker malo podría eliminar algunos de ellos, solo para demostrar un punto."

ACTIVISMO

Desde el año 2002-2003, se ha ido configurando una perspectiva más amplia del hacker, pero con una orientación a su integración con el hacktivismo. Aparecen espacios autónomos denominados *hacklab* o *hackerspace* y los *hackmeeting* como instancias de diálogo de hackers. Desde esta perspectiva, se

entiende al hacker como una persona que es parte de una conciencia colectiva que promueve la libertad del conocimiento y la justicia social.

Se entiende, por tanto, el hacktivismo (fusión de *hack* y activismo) como el empleo de las destrezas técnicas más diversas, en pro de fines sociales, ecológicos, humanitarios o de cualquier otra índole con repercusión o tendente a la defensa de los derechos humanos.

Así, el hacktivismo debe ser entendido no desde un prisma reduccionista como equivalente siempre al desarrollo de actividades subversivas. Se encuentran ramificaciones del hacktivismo en la liberación de conocimiento (como puede ser la misma Wikipedia, con la que comenzó toda una revolución en el modo de crear y compartir el conocimiento humano más allá de barreras académicas o comerciales), o en la liberación de información clasificada que se considera que debe estar, por definición, a disposición de la sociedad (casos de WikiLeaks o las filtraciones de Snowden sobre las actividades militares y casos de espionaje gubernamentales).

Por tanto, el fenómeno hacker tiene un importante componente de aperturismo y liberación de conocimientos e información que, a través del activismo de estos especialistas, buscan informar a la sociedad en general.

En este caso, los roles de un hacker pueden entenderse desde distintos aspectos:

- Poner a disposición del dominio público el manejo técnico y destrezas alcanzadas personal o grupalmente.
- Crear nuevos sistemas, herramientas y aplicaciones técnicas y tecnológicas para ponerlas a disposición del dominio público.
- Realizar acciones de hacktivismo tecnológico con el fin de liberar espacios y defender el conocimiento común y abierto.

Se reitera que no se debe confundir el concepto "hacker" con el de "ciberdelincuente".

CLASIFICACIÓN DE LOS HACKERS: LOS SOMBREROS

El origen del término parece provenir de las antiguas películas de vaqueros donde el personaje bueno utilizaba un sombrero blanco y el malo un sombrero negro, lo cual era muy efectivo para recalcar la trama, incluso si el filme era en blanco y negro o a color. De allí, primordialmente, deriva la costumbre de clasificar a los hackers según sus intenciones o forma de actuar asignándoles un "color de sombrero".

Sin embargo, no es suficiente para decir que alguien es "sombrero blanco" o "sombrero negro". El comportamiento de los hackers muchas veces escapa al control de la ley porque lo que hacen es inusual. Un ejemplo de ello lo explica Paul Graham refiriéndose a un conocido suyo que fue detenido por el FBI debido a que recientemente se había legislado sobre la irrupción en ordenadores. Las técnicas de investigación no funcionaron porque estaban basadas en causas frecuentes: dinero, venganza, drogas o sexo o una combinación de algunas y/o todas ellas. La curiosidad intelectual no era un concepto para el que estaban preparados los agentes policiales del FBI.

Hacker de sombrero blanco:

Un hacker de sombrero blanco (del inglés, *white hat*), vulneran la seguridad del sistema para conocer sus fallos y avisar de los mismos y repararlos, suelen trabajar para compañías en el área de seguridad informática para proteger el sistema ante cualquier alerta.

Hacker de sombrero negro:

Por el contrario, los hackers de sombrero negro (del inglés, *black hat*), también conocidos como crackers o ciberdelincuentes, muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas o creando virus, entre otras muchas cosas utilizando sus destrezas en métodos hacking. Rompen la seguridad informática, buscando la forma de entrar a programas y obtener información o generar virus en el equipo o cuenta ingresada. No se rigen por ninguna ética o moral ni tampoco les importa quebrantar las leyes.

Hacker de sombrero gris:

Los hackers de sombrero gris (del inglés, *grey hat*) son aquellos que poseen un conocimiento similar al hacker de sombrero negro y con este conocimiento penetran sistemas y buscan problemas, cobrando luego por su servicio para reparar daños. Se mueven por su propio interés, pero se mueven a medio camino entre los hackers éticos (sombrero blanco) y los ciberdelincuentes (sombrero negro).

Supuestamente, cualquier hacker debería comprender y aprender todas las formas existentes de hackeo. Lo cual causa una doble moral para aquellos que son de sombrero blanco: por un lado, existe la ética a la cual han sido fieles y por ello prestan servicios profesionales a miles de empresas en el mundo asegurando su infraestructura; por otro, conocer y usar métodos propios de los *black hat* que incluyen ataques de denegación de servicio e ingeniería social agresiva entre otros.

ÉTICA HACKER

En 1984, Steven Levy publicó el libro titulado *Hackers: heroes of the computer revolution*, (en español, "Los hackers: los héroes de la revolución informática") en donde se plantea por primera vez la idea de la ética hacker, y donde se proclama y se promueve una ética de libre acceso a la información y al código fuente del software. Levy se basó en entrevistas para poder identificar los seis principios básicos relacionados con las creencias y las operaciones de los hackers.

De acuerdo con Levy los seis fundamentos del hacker son:

1. El acceso a los ordenadores (y cualquier cosa que pueda enseñar algo acerca de la forma en que funciona el mundo), debe ser ilimitado y total.
2. Toda la información debería ser libre.
3. La desconfianza en la autoridad, promover la descentralización.
4. Los hackers deben ser juzgados por su capacidad, no por criterios como títulos, edad, raza, sexo o posición.

5. Se puede crear arte y belleza en un ordenador.
6. Los ordenadores pueden cambiar la vida para mejor.

Sin embargo, la ética hacker genera controversia, y hay personas, como el estudiante de derecho Patrick S. Ryan, que critican los principios recién enumerados de la ética hacker, considerando que allí "hay muy poca ética", y catalogando esos enunciados como "un grito de batalla -que- no pone límites a los hackers". Sin embargo, para otras personas, como por ejemplo Linus Torvalds, estos principios éticos están de acuerdo al trabajo cotidiano del hacker, que es "interesante, emocionante, y algo que se disfruta", adjetivos que en ocasiones son usados por los mismos hackers para describir sus respectivos trabajos, lo que también limita la restricción que se proclama sobre la libertad de usar la información.

Finalmente, en la sociedad actual, se considera que la ética general que rige las normas sea la que posea el hacker ético, por lo que se usa como sinónimo de hacker de sombrero blanco.

KALI LINUX: UNA HERRAMIENTA BÁSICA PARA UN HACKER

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Fue desarrollada por Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, que crearon la distribución a partir de la reescritura de BackTrack, que se podría denominar la antecesora de Kali Linux.

Kali Linux trae preinstalados más de 600 programas incluyendo *Nmap* (un escáner de puertos), *Wireshark* (un sniffer), *John the Ripper* (un crackeador de passwords) y la suite *Aircrack-ng* (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

Kali es desarrollado en un entorno seguro; el equipo de Kali está compuesto por un grupo pequeño de personas de confianza quienes son los que tienen permitido modificar paquetes e interactuar con los repositorios oficiales. Todos los paquetes de Kali están firmados por cada desarrollador que

lo compiló y publicó. A su vez, los encargados de mantener los repositorios también firman posteriormente los paquetes utilizando GNU Privacy Guard.

Todo esto conlleva que Kali sea considerada una herramienta básica para cualquier hacker ético, pero a su vez, al ser libre y gratuita, también puede ser usada por cualquier persona, independientemente de sus intenciones.