¿Cómo funciona CPHulk? Cuales son sus usos; cómo configurar

¿Cómo funciona CPHulk? Cuales son sus usos; cómo configurar. La seguridad es de gran importancia para el equipo de cPanel. No solo se aseguran de proporcionar todo lo que pueda mejorar la protección de sus clientes, sino que también brindan formas de mantener segura la información de los «clientes de los clientes» también.

Una de sus características interesantes para la seguridad web, de correo electrónico o del servidor es cPHulk. Esta función proporciona una gran protección contra los ataques de fuerza bruta y se ha convertido en parte de su suite de seguridad durante años, y ahora se ha vuelto aún más dominante con el lanzamiento de cPanel & WHM versión 70.

Ataques de fuerza bruta

Cuando queda bloqueado de una cuenta después de varios intentos fallidos de contraseña, esta es una medida de seguridad que se utiliza para garantizar que el software malintencionado no se introduzca con éxito en los datos de sus usuarios privados o clientes. En un ataque de fuerza bruta, un atacante intenta

acceder a una cuenta de usuario ingresando repetidamente contraseñas aleatorias. Si bien este método de piratería no es particularmente refinado, puede funcionar y funciona. Eso hace que protegerte a ti mismo sea aún más importante.

¿Cómo funciona este cPHulk?

cPHulk está involucrado como parte de todas las instalaciones de cPanel y WHM y se puede usar para monitorear y bloquear todos los intentos de inicio de sesión realizados en cPanel, WHM, FTP, correo electrónico y SSH. Ofrece a todos los administradores una variedad de métodos para combatir los ataques de fuerza bruta de forma automática o manual. cPHulk puede incluso usarse para bloquear direcciones IP maliciosas en su firewall.

El bloqueo de los inicios de sesión maliciosos se puede emitir en duraciones diferentes desde una prohibición temporal hasta un día o incluso una prohibición permanente. Este sistema cPHulk altamente configurable le permite un control total. E incluso puede especificar el número de intentos de inicio de sesión fallidos antes de que se bloquee una dirección IP. Y también le permite definir algunas acciones adicionales para realizar y desencadenar un bloqueo automático. También permite las **notificaciones a los administradores del servidor para cada evento específico que ocurrió**.

Cómo configurar cPHulk en su servidor para evitar problemas de carga

Internet es un lugar muy inseguro donde cada vez que su servidor puede ser atacado, si no está bien protegido. **Un ataque de fuerza bruta es uno de esos ataques que intenta iniciar sesión en su servidor mediante intentos repetidos de adivinación de contraseñas.**

Si bien la forma ideal de prevenir un ataque de fuerza bruta es deshabilitar totalmente el acceso a ese servicio, no es factible en un servidor de alojamiento web público que pueda obtener acceso desde cualquier parte del mundo.

Es prácticamente imposible permitir o denegar manualmente cada IP, desde el rango completo de direcciones IP. Ahí es cuando una herramienta de protección de fuerza bruta se vuelve relevante.

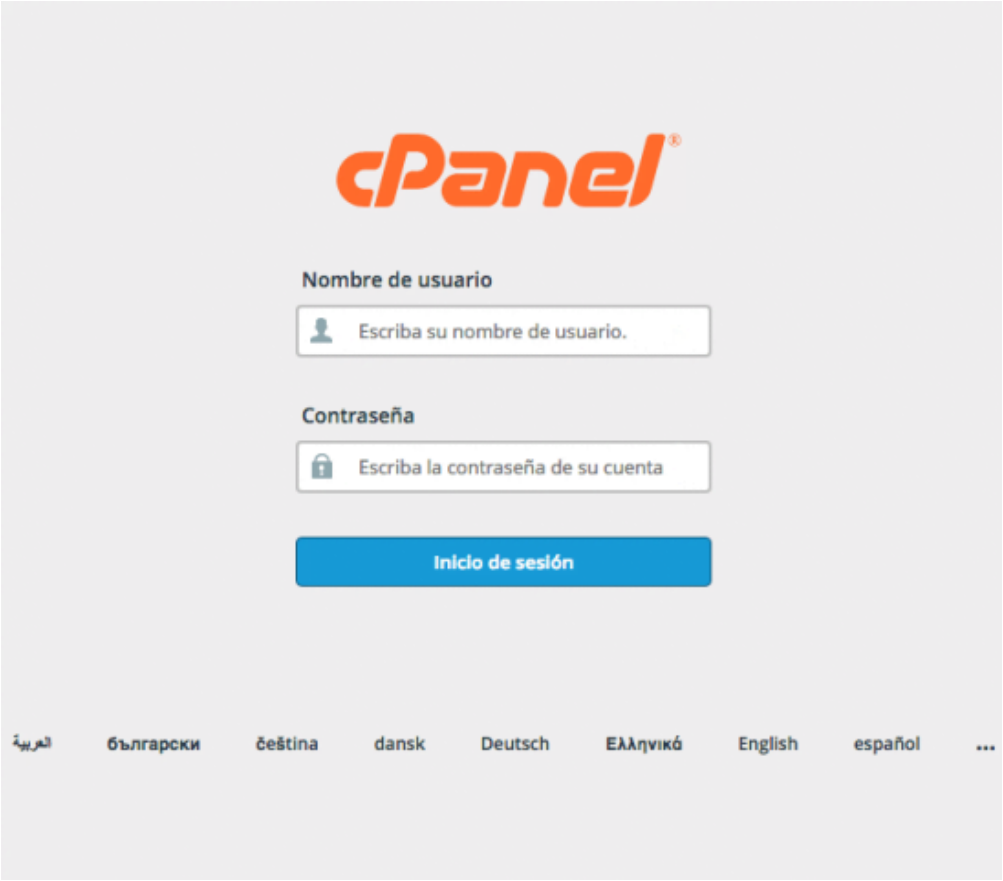
Una experiencia

Cuando se sospecha de un ataque, desactiva los intentos de inicio de sesión de esa dirección IP al servidor. La IP bloqueada puede acceder al sitio, pero al intentar iniciar sesión, se mostrará un error
cPHulk puede bloquear 1. Las direcciones IP desde las cuales se notaron demasiados intentos de inicio de sesión fallidos a los servicios en el servidor y **2. Una cuenta** que está siendo abusada activamente por intentos de inicio de sesión fallidos.

cPHulk se puede habilitar en los servidores de cPanel usando la opción ‘WHM -> Security Center -> cPHulk Brute Force Protection’. cPHulk tiene ciertos ajustes de configuración, lo

que determina la efectividad de la protección.

Si no se configura con los parámetros correctos, estos ajustes pueden hacer que la protección sea ineficaz para prevenir los ataques o pueden hacer que los usuarios válidos se bloqueen innecesariamente.



Recientemente fuimos contactados por un servidor web cuyo servidor estaba respondiendo muy lento. Nuestro experto experto en servidores examinó el servidor y descubrió que la carga del servidor era muy alta.

En una investigación adicional, nuestra tecnología pudo ver que el servidor estaba bajo ataque de fuerza bruta, pero la configuración de cPHulk en el servidor era ineficiente para bloquear este ataque.

Hoy, veremos los principales parámetros en la herramienta cPHulk y cuál es el propósito de cada uno de ellos.
La configuración de cPHulk en el archivo de configuración se ajusta específicamente a cada requisito de servidor y nivel de seguridad requerido. **Las siguientes configuraciones se pueden configurar para decidir cómo cPHulk maneja los ataques**.

- Período de protección de fuerza bruta basado en IP en minutos: el tiempo durante el cual se bloquea una dirección IP en el servidor. Esto no debe establecerse en un valor bajo, sino al menos durante un par de horas o más en el caso de una amenaza.
- Período de protección de fuerza bruta en minutos: determina la duración de los fallos de inicio de sesión, en los que una dirección IP califica para un bloqueo. Esto no debe ser un valor alto, sino que debe configurarse en pocos minutos para evitar una carga del servidor.
- Máximo de fallos por cuenta: restricción específica de la cuenta dónde una vez que una cuenta alcanza este límite, se bloqueará la totalidad de la cuenta para futuros intentos de inicio de sesión.
- Máximo de fallos por IP: el número de fallos de inicio de sesión que califican para un bloqueo de IP. Una vez que una dirección IP alcance este límite, a esa dirección se le denegarán más intentos de inicio de sesión. Este valor no debe establecerse demasiado alto o demasiado bajo, ya que el primero puede hacer que el servidor sea susceptible de ser atacado y este último puede bloquear usuarios válidos.
- Máximo de fallas por IP antes de que la IP se bloquee por un período de dos semanas: esta es una configuración para un bloqueo a largo plazo para IP sospechosas. Una vez que una dirección IP alcance este límite, se bloqueará durante dos semanas. Enviar una notificación cuando el inicio de sesión de root sea correcto cuando la IP no esté en la lista blanca: esta configuración ayuda a saber si alguien más establece una sesión de inicio de sesión de root válida en su servidor y toma una acción inmediata.

La configuración predeterminada en los servidores de cPanel a menudo es inadecuada para una protección infalible, y muchos servidores web tienden a pasar por alto eso, y los servidores

terminan siendo atacados.

En este servidor en particular, la configuración de «fallas máximas por IP» se estableció en un valor alto (20), lo que impidió que las IPs atacantes fueran bloqueadas por el cPHulk, lo que provocó que el servidor fuera atacado.

Después de cambiar la configuración a valores efectivos, las direcciones IP comenzaron a bloquearse y, por lo tanto, salvaron al servidor de un ataque y volvieron estable la carga y los sitios web más receptivos.

Además, también optimizamos el servidor web para un rendimiento óptimo y aseguramos el servidor en 360 grados para evitar vulnerabilidades o vulnerabilidades en él.

Conclusión


(Tomado de internet)

cPHulk actúa como un **antivirus en cPanel** y lo ayuda a trabajar con facilidad y también lo protege a usted y a las cuentas de sus clientes para que no se bloqueen. Incluso lo protege de ser hackeado. Si es nuevo en cPanel y desea que sus cuentas estén protegidas, puede confiar en esta función llamada cPHulk.

Leer también: Usar cPHulk Contra Ataques De Fuerza Bruta En Servidor Desde WHM; cómo activar cPHulk, para que se usa