**Ataque por Fuerza Bruta**

***¿Qué es un ataque de fuerza bruta?***

Un ataque de fuerza bruta ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema.

El principal objetivo de este ataque es intentar romper todas las combinaciones posibles de nombre usuario y contraseña, estos ataques buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil a la información que está protegida.

Como protegerse del ataque:

* Bloquee el número de intentos fallidos al introducir el usuario y la contraseña.
* Utilice una contraseña segura de más de 8 caracteres realizando combinación de mayúsculas, minúsculas, letras y números.
* Evite un nombre de usuario como admin, administrador.
* Usa CAPTCHA.
* Limita los inicios de sesión a una dirección IP especificada o rango.
* Emplear autenticación de 2 factores (2FA).

**Tipos de ataques de fuerza bruta**

En esencia, la fuerza bruta es el acto de probar muchas combinaciones posibles, pero hay muchas variantes de este ataque para aumentar su tasa de éxito. Aquí están los más comunes:

**Estándar**

Un ataque estándar de fuerza bruta puede usar diferentes métodos, como iterar a través de todas las contraseñas posibles, una a la vez. Esto se usa comúnmente en archivos locales, donde no hay límites para la cantidad de intentos que tiene, ya que otros ataques suelen ser más exitosos a escala.

**De diccionario**

Este ataque de diccionario utiliza una lista de palabras y contraseñas comunes en lugar de ir al azar, creando un “diccionario” de posibles contraseñas e iterando a través de ellas. Usar una buena lista de contraseñas puede ayudar a mejorar las tasas de éxito de los atacantes, pero estos ataques a menudo requieren una gran cantidad de intentos contra posibles objetivos.

**De arco iris**

Estos ataques de arco iris parten del valor hash para reproducir los pasos de la cadena hasta obtener la contraseña. Sin embargo, muchas veces el valor no se encuentra en la tabla; por lo que se recrea al reducir el valor con la misma función con la cual se creó la cadena.

Este procedimiento se repite hasta conseguir el valor resumen en un punto final. Ahora bien, eso no significa que se ha encontrado la contraseña, sino la cadena de caracteres que terminará revelando el texto plano que compone la contraseña.

Se les llaman Tablas Arcoiris porque se asigna un color distinto a cada reducción para evitar confusiones. Al final son tantas las reducciones con sus respectivos colores, que termina por parecer un arcoiris.

[**Yolanda González**](https://protecciondatos-lopd.com/empresas/author/dpto-juridico-063/)

**19 junio, 2020**

**Artículo**

**Qué son ataques de fuerza bruta y cómo protegerse.**

[**https://protecciondatos-lopd.com/empresas/ataques-fuerza-bruta/**](https://protecciondatos-lopd.com/empresas/ataques-fuerza-bruta/)