**Refuérzate contra ataques cibernéticos de fuerza bruta**

Los nombres de usuario y las contraseñas son uno de los controles de seguridad más comunes e importantes que existen en uso en la actualidad. Son como la cerradura de la puerta que las organizaciones utilizan para restringir el acceso a sus redes, servicios y datos. Sin embargo, un problema importante al confiar en las credenciales de inicio de sesión como una línea de defensa crítica es que son vulnerables a que las roben o adivinen los atacantes.

En un video, aprendiste que los **ataques de fuerza bruta** son un proceso de prueba y error para descubrir información privada. En esta lectura, aprenderás sobre las muchas tácticas y herramientas que utilizan los agentes de amenaza para realizar ataques de fuerza bruta. También aprenderás estrategias de prevención que las organizaciones pueden utilizar para defenderse de ellos.

**Una cuestión de ensayo y error**

Una forma de abrir una cerradura es probar la mayor cantidad de combinaciones posibles. A veces, los agentes de amenaza utilizan tácticas similares para obtener acceso a una aplicación o una red.

Los atacantes utilizan diversas tácticas para ingresar en un sistema:

* En los *ataques de fuerza bruta simples*, los atacantes adivinan las credenciales de inicio de sesión de un usuario. Pueden hacerlo ingresando cualquier combinación de nombres de usuario y contraseñas que se les ocurra hasta que encuentren la que funcione.
* La de los *ataques de diccionario* es una técnica similar, excepto que en estos casos los atacantes utilizan una lista de credenciales de uso común para acceder a un sistema. Esta lista se asemeja a hacer coincidir una definición con una palabra en un diccionario.
* Los *ataques de fuerza bruta inversa* son similares a los ataques de diccionario, excepto que comienzan con una sola credencial y se prueba en varios sistemas hasta que se encuentra una coincidencia.
* El *relleno de credenciales* es una táctica en la que los atacantes usan credenciales de inicio de sesión robadas en violaciones de datos anteriores para acceder a cuentas de usuario en otra organización. Un tipo especializado de relleno de credenciales se llama *pasar el hash*. Estos ataques reutilizan credenciales hash robadas y sin salting para, de esta manera, engañar a un sistema de autenticación para que cree una nueva sesión de usuario autenticada en la red.

**Nota:** Además de las credenciales de acceso, la información cifrada a veces puede forzarse mediante una técnica conocida como *búsqueda exhaustiva de claves*.

Cada uno de estos métodos implica mucho trabajo para intentar adivinar. Forzar de forma bruta tu entrada en un sistema puede ser un proceso tedioso y lento, en especial cuando se realiza de forma manual. Es por eso que los agentes de amenaza a menudo utilizan herramientas para llevar a cabo sus ataques.

**Herramientas del oficio**

Se pueden utilizar muchísimas combinaciones para crear un solo conjunto de credenciales de inicio de sesión. La cantidad de caracteres, letras y números que se pueden mezclar es inmensa. Cuando se hace de forma manual, podría llevarle años a alguien probar todas las combinaciones posibles.

En lugar de dedicarle tiempo a esto, los atacantes suelen recurrir a software para que adivine por ellos. Estas son algunas herramientas comunes para utilizar en ataques de fuerza bruta:

* Aircrack-ng
* Hashcat
* John the Ripper
* Ophcrack
* THC Hydra

A veces, los profesionales de seguridad utilizan estas herramientas para probar y analizar sus propios sistemas. Cada uno de ellos sirve para diferentes propósitos. Por ejemplo, puedes utilizar Aircrack-ng para probar una red Wi-Fi en busca de vulnerabilidades a los ataques de fuerza bruta.

**Medidas de prevención**

Las organizaciones se defienden contra los ataques de fuerza bruta mediante una combinación de controles técnicos y administrativos. Cada uno hace que la ruptura de los sistemas de defensa a través de la fuerza bruta sea menos probable:

* Hashing y salting
* Autenticación de múltiples factores, o multifactor, (MFA)
* CAPTCHA
* Políticas de contraseñas

Las tecnologías como la autenticación de múltiples factores (MFA) refuerzan cada intento de inicio de sesión al requerir una segunda o tercera forma de identificación. Otras herramientas importantes son CAPTCHA y las políticas de contraseñas efectivas.

**Hashing y salting**

El **hashing** convierte la información en un valor único que luego se puede usar para determinar su integridad. El **salting** es una protección adicional que se utiliza para reforzar las funciones hash. Se trata de una técnica que consiste en agregar caracteres aleatorios a los datos, como contraseñas. Esto aumenta la longitud y la complejidad de los valores hash, lo que los hace más difíciles de usar y menos susceptibles a  ataques de diccionario.

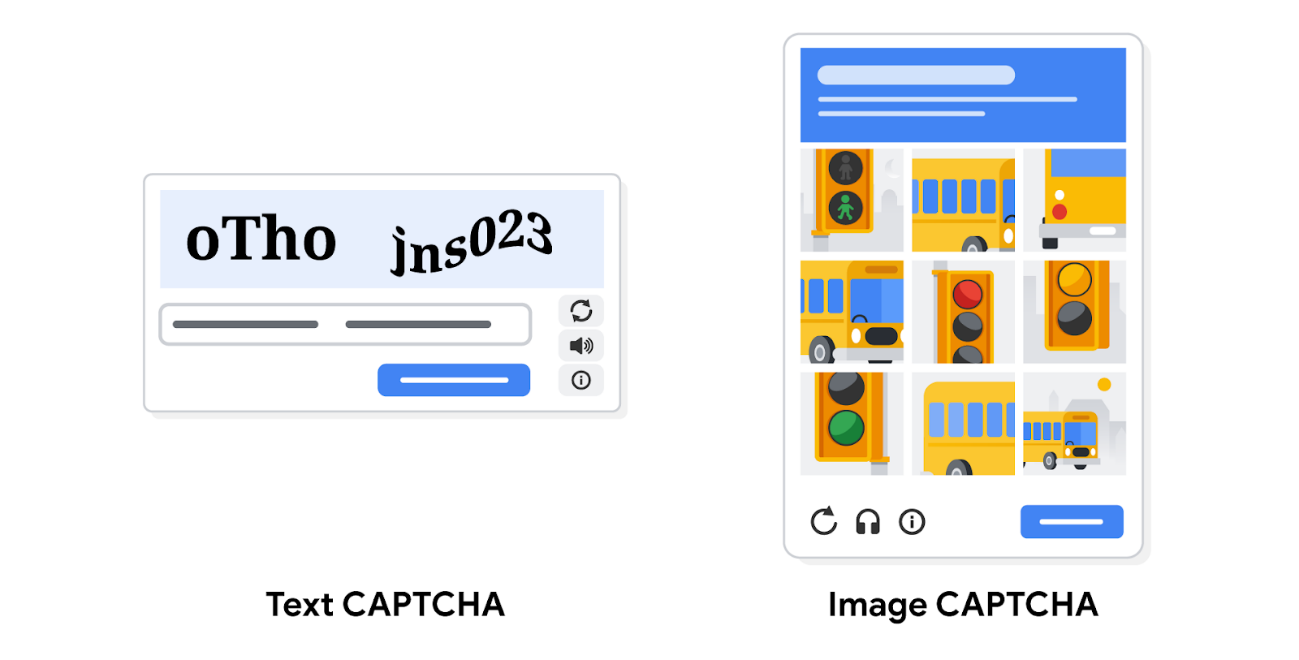
**Autenticación de múltiples factores (MFA)**

La **autenticación de múltiples factores, o multifactor,** (MFA) es una medida de seguridad que exige que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red. Se trata de una estrategia de protección de la información por capas. La MFA limita las posibilidades de ataques de fuerza bruta porque, aunque una credencial se viera comprometida, es poco probable que usuarios no autorizados cumplan con cada requisito de autenticación.

**CAPTCHA**

CAPTCHA significa prueba de turing pública y automatizada para diferenciar entre máquinas y humanos. Se trata de un sistema de autenticación, mediante respuesta a un desafío. CAPTCHA pide a los usuarios que realicen una prueba simple para demostrar que son humanos y no un software que está intentando forzar una contraseña.

Estos son algunos ejemplos comunes de CAPTCHA:



Existen dos tipos de pruebas de CAPTCHA. Uno desordena y distorsiona una secuencia de letras o números generada aleatoriamente y pide a los usuarios que los ingresen en una caja de texto. Otra prueba pide a los usuarios que relacionen imágenes con una palabra generada aleatoriamente. Es probable que hayas tenido que superar una prueba de CAPTCHA al acceder a un servicio web que contiene información confidencial, como una cuenta bancaria en línea.

**Política de contraseñas**

Las organizaciones utilizan estos controles de gestión para estandarizar las prácticas recomendadas de contraseñas en toda su empresa. Por ejemplo, una de estas políticas podría requerir que los usuarios creen contraseñas que tengan al menos ocho caracteres e incluyan una letra, un número y un símbolo. Otros requisitos comunes pueden incluir políticas de bloqueo de contraseñas. Por ejemplo, un bloqueo de contraseña puede limitar el número de intentos de inicio de sesión antes de que se suspenda el acceso a una cuenta y requerir que los usuarios creen contraseñas nuevas y únicas después de un determinado período de tiempo.

El propósito de cada uno de estos requisitos es crear la mayor cantidad de combinaciones de contraseñas posible. Esto extiende la cantidad de tiempo que tarda un atacante en encontrar una que funcione. La [Publicación especial 800-63B del Instituto Nacional de Estándares y Tecnología (NIST)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf) proporciona orientación detallada que las organizaciones pueden consultar al crear sus propias políticas de contraseñas.

**Conclusiones clave**

Los ataques de fuerza bruta son formas simples pero confiables de obtener acceso no autorizado a los sistemas. En general, cuanto más fuerte sea una contraseña, más resistente será a ser descifrada. Como profesional de la seguridad, puede que debas utilizar las herramientas descritas, para probar la seguridad de los sistemas de tu organización. Reconocer las tácticas y herramientas utilizadas para llevar a cabo un ataque de fuerza bruta es el primer paso para detener a los atacantes.