D1

Un ataque de fuerza bruta es un intento de averiguar una contraseña o un nombre de usuario o la clave utilizada para cifrar un mensaje, mediante un enfoque de prueba y error, con la esperanza de acertar. Este es un antiguo método de ataque, pero sigue siendo efectivo y popular entre hackers. (<https://latam.kaspersky.com/resource-center/definitions/brute-force-attack> )

D2

-Los ataques de contraseña de fuerza bruta a menudo se llevan a cabo mediante scripts o bots que tienen como destino la página de inicio de sesión de un sitio web.

-son muy lentos, ya que es probable que deban pasar por cada una de las combinaciones posibles de caracteres antes de lograr su objetivo. (<https://www.cloudflare.com/es-es/learning/bots/brute-force-attack/>)

D3

-Cómo funcionan los ataques de fuerza bruta

Los ataques de fuerza bruta suelen utilizar herramientas automatizadas para adivinar varias combinaciones de nombres de usuario y contraseñas hasta que encuentran la entrada correcta. Cuanto más larga sea la contraseña, más tiempo tardará normalmente en encontrar la entrada correcta.

Según la longitud y la complejidad de la contraseña, averiguarla puede tardar desde unos pocos segundos hasta muchos años. De hecho, según IBM, algunos hackers atacan los mismos sistemas cada día durante meses e incluso años. (<https://latam.kaspersky.com/resource-center/definitions/brute-force-attack>)

Debido a esto los hackers han desarrollado herramientas para agilizar el trabajo. (<https://latam.kaspersky.com/resource-center/definitions/brute-force-attack>)

D4

El termino ATAQUE DE FUERZA BRUTA INVERSA -> se invierte la estrategia de ataque y se comienza con una contraseña conocida, como contraseñas filtradas disponibles en Internet, y con la búsqueda de millones de nombres de usuario hacen pruebas hasta encontrar una coincidencia.

En caso de INVERSA, se prueban muchos nombres de usuario contra una contraseña, al contrario de AFB.

D5

Entre las herramientas famosas que se utilizan para este tipo de acciones están

Brutus, Medusa, THC Hydra, Ncrack, Aircrack-ng y Rainbow. Muchos pueden encontrar una contraseña de diccionario en menos de un segundo.

Por lo que estas herramientas debilitan muchos protocolos informáticos, por ejemplo:

FTP (File Transfer Protocol) -> Un cliente FTP es una aplicación que se conecta a un servidor FTP para acceder a los archivos o hacer transferencias de archivos.

MySQL-> es un motor de datos.

SMTP -> Simple Mail Transfer Protocol por sus siglas en inglés; reglas de comunicación que utilizan los servidores de correo electrónico para enviar y recibir e-mails.

Telnet

y permiten que los hackers descifren módems inalámbricos, identifiquen contraseñas poco seguras, descifren contraseñas de almacenamientos cifrados,

- traduzcan palabras a escritura leetspeak, en la que palabras como “don'thackme” se convierten en “d0n7H4cKm3”, por ejemplo, y que ejecuten todas las combinaciones posibles de caracteres y efectúen ataques por diccionario.

D6

También mencionar que el procesamiento de la **GPU -> tipo de procesador**

**que maneja y acelera la representación de gráficos** permite descifrar contraseñas casi 250 veces más rápido que con solo una CPU.

Para tener una idea, una contraseña de seis caracteres que incluye números tiene aproximadamente 2 mil millones de combinaciones posibles. Tratar de descifrarla con una CPU potente que prueba 30 contraseñas por segundo tarda más de dos años. Sumar solo una tarjeta GPU potente le permite al mismo equipo probar 7100 contraseñas por segundo y descifrarla en 3,5 días.

D7

Pasos para que los especialistas en TI reduzcan la posibilidad de sufrir un ataque de fuerza bruta

-Contraseñas de sus sistemas estén cifradas con el mayor índice de cifrado posible

-Requerir autenticación de dos pasos e instalar un sistema de detección de intrusiones para detectar ataques de fuerza bruta.

-Limitar la cantidad de intentos también reduce la posibilidad de sufrir ataques de fuerza bruta.