Ataques por fuerza bruta (Brute Force)

El término “fuerza bruta” relacionado con incidentes de seguridad informática está asociado a los intentos por conseguir averiguar una o varias contraseñas. Estas pueden estar vinculadas a accesos a servicios online o a ficheros y mensajes cifrados. En cualquier caso, el atacante va probando diversas combinaciones hasta dar con la correcta. Para ello se apoya en el uso de software, hardware, así como también en algoritmos y diccionarios de palabras.

En función de la longitud y complejidad de la contraseña, descifrarla puede llevar desde unos segundos hasta varios años. De hecho, apunta a que algunos hackers tienen los mismos sistemas como objetivo a diario durante meses e, incluso, años.

En cuanto al hardware que se utiliza, cuanta más potencia se tenga más combinaciones por segundo se podrán evaluar, mientras que en lo que respecta el software, existen programas que son utilizados desde hace tiempo para aplicar la fuerza bruta en el descifrado de contraseña.

GPU acelera los ataques de fuerza bruta

La combinación de la CPU y la unidad de procesamiento de gráficos (GPU) acelera la potencia informática, puesto que añade al procesamiento miles de núcleos informáticos de la GPU para que el sistema pueda gestionar varias tareas de forma simultánea. El procesamiento de GPU se utiliza para aplicaciones de análisis, ingeniería y otras aplicaciones que hacen un uso intensivo de la informática y puede descifrar las contraseñas unas 250 veces más rápido que una CPU independiente.

Con un ejemplo, una contraseña de seis caracteres que incluye números tiene aproximadamente 2000 millones de combinaciones posibles. Para descifrarla con una CPU potente que pruebe 30 contraseñas por segundo, sería necesario más de dos años. Añadiendo una sola tarjeta GPU potente, el mismo equipo puede probar 7100 contraseñas por segundo y descifrarla en 3,5 días.

Cómo pueden los usuarios fortalecer las contraseñas

Si es posible, los usuarios deben elegir contraseñas de 10 caracteres que incluyan números o símbolos. De esta manera se crean 171.3 trillones (1.71 x 1020) de posibilidades. Con un procesador de GPU que pruebe 10,3 mil millones de hashes por segundo, descifrar la contraseña llevaría aproximadamente 526 años, aunque un superordenador podría descifrarla en varias semanas.

Aun así, no todos los sitios aceptan contraseñas tan largas, lo que implica que los usuarios deben elegir frases de contraseña complejas en lugar de palabras independientes. Es importante evitar las contraseñas más comunes y cambiarlas con frecuencia.

¿Cómo podemos calcular la complejidad de una contraseña?

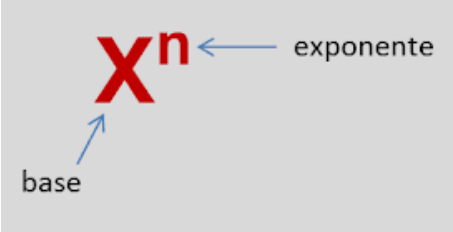
Cuando se crea una contraseña, normalmente se dispone de los siguientes caracteres:

Números (10 diferentes: 0-9)

Letras (52 diferentes: A-Z y a-z)

Caracteres especiales (32 diferentes).

La complejidad de una contraseña (número de combinaciones posibles) se calcula mediante la siguiente fórmula:



X → es la suma de todos los posibles caracteres.

n → es la longitud de la contraseña.

El resultado es el número de posibles contraseñas por lo tanto, a mayor sea el resultado más segura será nuestra contraseña.

Ejemplos:

Letras minúsculas (27) + números (10) con una longitud de 5 dígitos

(27+10)^5= 69343957 posibles contraseñas

Letras minúsculas (27) + letras mayúsculas (27) con una longitud de 4 a 5 dígitos

((27+27) ^ 4) + ((27+27) ^ 5) = 467668080 posibles contraseñas

Brute Force Atack: es una técnica que permite probar todas las combinaciones posibles hasta encontrar la palabra o texto legible que fue cifrado.

Un Ataque de fuerza bruta consta de siguientes elementos vitales:

- ✓ Un Charset o alfabeto utilizado para obtener todas las posibles combinaciones.
- ✓ Una longitud de palabra, la cual nos determina todas las posibles combinaciones.
- ✓ Palabra cifrada, la cual va a ser usada para romper el ciclo de iteraciones en caso de encontrar la palabra legible.
- ✓ Algoritmo o función de cifrado, ya que sin esta no es posible hacer el brute force.

Combinaciones por Fuerza Bruta

Fórmula:

$$\text{Combinaciones posibles} = \text{Número de caracteres posibles}^{\text{Longitud de la contraseña}}$$

Consigna en Clase: Resolver el siguiente ejercicio, mediante fuerza bruta.

- Longitud de dígitos de la contraseña → 2
- Cantidad de posibles caracteres utilizados → Solamente números (10)
- Cantidad de segundos por combinación → 1

Resultado:

10^2 = 100 combinaciones * 1 segundos = 100 segundos.