<!DOCTYPE html>

Jorge Calvo

Eficacia y Eficiencia

Ataques de Fuerza Bruta

Sígueme en - LinkedIn Twitter Blog

Ataques de Fuerza Bruta

¿Que es un ataque de fuerza bruta?

- Un ataque de fuerza bruta (también conocido como craqueo de fuerza bruta) es el equivalente de un ciberataque a probar todas las teclas de su llavero y, finalmente, encontrar la correcta.
- Los ataques de fuerza bruta son simples y confiables. Los atacantes dejan que una computadora haga el trabajo, probando diferentes combinaciones de nombres de usuario y contraseñas, por ejemplo, hasta que encuentran una que funciona. Detectar y neutralizar un ataque de fuerza bruta en curso es el mejor contraataque: una vez que los atacantes tienen acceso a la red, son mucho más difíciles de atrapar.

Tipos de ataques

- El ataque de fuerza bruta más básico es un ataque de diccionario, donde el atacante trabaja a través de un diccionario de posibles contraseñas y las prueba todas. Los ataques de diccionario comienzan con algunas suposiciones sobre contraseñas comunes para tratar de adivinar de la lista del diccionario.
- El reciclaje de credenciales es otro tipo de ataque de fuerza bruta que reutiliza nombres de usuario y contraseñas de otras filtraciones de datos para intentar ingresar a otros sistemas.
- El ataque de fuerza bruta inversa utiliza una contraseña común como "contraseña" y, posteriormente, intenta forzar un nombre de usuario para que vaya con esa contraseña. Dado que la contraseña es una de las contraseñas más comunes en 2017, esta técnica es más exitosa de lo que cree.

Defensa de los ataques de Fuerza Bruta

- Aumentar la longitud de la contraseña: más caracteres equivalen a más tiempo para romper la fuerza bruta
- Aumente la complejidad de la contraseña: más opciones para cada personaje también aumentan el tiempo para el crack de fuerza bruta
- Limite los intentos de inicio de sesión: los ataques de fuerza bruta incrementan un contador de intentos de inicio de sesión fallidos en la mayoría de los servicios de directorio; una buena defensa contra los ataques de fuerza bruta es bloquear a los usuarios después de algunos intentos fallidos, anulando así un ataque de fuerza bruta en curso
- Implementar Captcha: Captcha es un sistema común para verificar que un humano es humano en sitios web y puede detener los ataques de fuerza bruta en curso.

- Utilice la autenticación de múltiples factores: la autenticación de múltiples factores agrega una segunda capa de seguridad a cada intento de inicio de sesión que requiera la intervención humana, lo que puede detener el éxito de un ataque de fuerza bruta

Ejemplo 1

Ataque de fuerza bruta sobre un código PIN de 4 números En este ejercicio realizamos la busqueda del número PIN usando la aleatoriedad del comando randint, generando números aleatorios entre 0 y 9999.

Desventajas

- Controlar que la longitud de nuestro número aleatorio, debe ser 4
- No controlamos los valores repétidos

Alternativa de Hackear PIN controlando valores repetidos

- Creamos una lista de números **únicos** entre 0 y 9999
- Buscamos en esa lista uno por uno desde el principio hasta que coincida con el PIN introducido por el usuario.
- Comprobamos tiempos con ambos programas
- ¿Merece la pena ordenar la lista?

Como crear esa lista

```
hack_l=random.sample(range(0,9999),9999)
print(hack_l[0:20]) #imprimimos los primeros 20 números para comprobar
```

In [ ]:
```
import random
import time

password= str(input("Introduce tu PIN de 4 digitos: "))
hack=random.sample(range(0,9999),9999)

for x in hack:
    x=str(x) #Conviertes el núemro aleatorio en formato texto
    if len(x)!=4: #Si veo que el numero generado tiene menos de 4 cifras, le añado ce
            if ("0"*(4 - len(x)) + x == password): #Multiplico el cero por el número 
              print("Tu PIN es " + x)
              break
    elif (x==password): #Si lo encuentra lo imprime
            print("Tu PIN es " + x)
            break

    else: continue #Si no coincide continuo

fin = time.time()

print("Tu programa ha tardado " + str(fin-inicio) + " segundos")
```