**[TLP BLANCO]:** La información conlleva un riesgo mínimo o inexistente aplicables para publicación pública. Sujeto a las normas de protección intelectual, puede distribuirse sin restricciones.

# INCIDENTE BRUTE FORCE

## 1. INTRODUCCIÓN

Este tipo de ataque, conocido como de fuerza bruta, es un método de ensayo y error persistente, utilizado para obtener información de un usuario y su contraseña, clave o número de identificación personal, entre otros. Funciona mediante la generación de un gran número de intentos consecutivos para el valor de los datos deseados. Un ataque de este tipo agota todas las posibilidades sin preocuparse por cuales opciones tienen mayor probabilidad de funcionar.

En los términos del control de acceso, generalmente encontramos al atacante intentando ingresar mediante un gran número de pruebas. En algunos casos el atacante puede conocer nombres de usuario válidos y la contraseña es la única parte que se trata de adivinar.

Los ataques por fuerza bruta están muy extendidos debido a que mediante la configuración de un script se puede probar cientos o miles de servidores de forma automática.

## 2. RIESGO

En caso de que el ataque de fuerza bruta sea efectivo, se podría comprometer:

- Acceso a sistemas sin autorización, lo que permitirá al atacante acceder a la información que se tenga almacenada, la cantidad de datos que sea revisados o robados dependerá del nivel de acceso que se haya obtenido en el sistema

- Acceso a una aplicación o servicio de una persona en particular (correo, skype, cuenta de un foro, intranet,…) lo que permitirá al atacante usar directamente la identidad de la victima, incluso secuestrar el usuario digital con multiples intenciones de estafa, secuestro, robo, entre otros delitos.

## 3. DETECCION

La detección se la realiza a través de integrantes de la red de confianza del Centro de Respuesta a Incidentes informáticos EcuCERT, quienes mediante un log de registros

proporcionan entre otra información dirección IP, día, fecha, hora y puerto en que un sistema o aplicación presentó el incidente.

Existen distintos programas que analizan el fichero de log de accesos ssh (por defecto, /var/log/auth.log) para determinar las direcciones IP desde las que se realizan los ataques, y configurar automáticamente el servidor para rechazarlos.

Fail2ban es una aplicación escrita en Python para la prevención de intrusos en un sistema, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta; es uno de los más conocido en sistemas Linux y funciona en combinación con iptables para rechazar los accesos desde las IP atacantes al nivel del núcleo del sistema (kernel).

## 4. ACCIONES RECOMENDADAS

Establecer mecanismos que permitan el monitoreo del tráfico entrante y saliente en la infraestructura de un sistema a fin de identificar tráfico inusual que se genere o ingrese, con medidas de contención para bloqueo de las conexiones remotas que intentan accesos por ataque de fuerza bruta.

## 5. REFERENCIA


- http://www.seguridad.unam.mx/documento/?id=17
- http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion4(5).pdf
- https://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=6293
- http://www.kb.cert.org/vuls/id/723755