Aplicación de Fuerza Bruta con Diccionario de Datos, para vulnerar contraseñas débiles en archivos comprimidos Zip

Edgar Mendoza Fernández
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
emendozaf16@gmail.com

***Resumen*—El presente trabajo muestra la vulnerabilidad en los archivos comprimidos con extensión ZIP, realizando ataques de control de autenticación, específicamente en la cadena de las contraseñas; la técnica utilizada es fuerza bruta con diccionario de datos, desarrollando una aplicación en Python para las pruebas correspondientes.**

Palabras clave: Fuerza bruta, diccionario, ataque, vulneración, contraseña, zip.

I. INTRODUCCIÓN

La protección de la confidencialidad es una tarea difícil de mantener, es por eso que en el campo de la autenticación generalmente alguno de estos tres factores o una combinación de estos, algo que se conoce, algo que se es y algo que se tiene, refiriéndose en su orden por ejemplo un *password*, una huella o un token; para la presente investigación nos concentraremos en el primero (*password*) que hoy en día es el más común.

Los archivos Zip comprimen datos ahorrando tiempo y espacio, además hacen que la descarga de software y transferencia de archivos adjuntos en correo electrónico sea más rápida sumado a eso la seguridad que se le da a información confidencial que pueda enviarse aplicando una contraseña a sus archivos, hace que esta herramienta adquiera una importancia al momento de cifrarlo.

Además que se ve muy seguido en sistemas que requieren de una autenticación a través de unas credenciales por parte del usuario, como id y *password* hacer el uso para acceso a un sistema de un usuario y contraseña para poder acceder a un recurso [1] ya que esta se considera una medida de control básica y al no estar bien estructurada se convierte en una vulnerabilidad en el caso de que este sea el único control en el que se confía.

Usando la técnica denominada fuerza bruta se intentará identificar una cadena desconocida, probando con todas combinaciones posibles de un diccionario de datos; su eficacia radica en que el diccionario tomado como entrada al algoritmo contenga todas las letras, números y/o símbolos que conforman la cadena que se busca.

El Centro Nacional de Ciberseguridad de Reino Unido (NCSC, por sus siglas en inglés) analizó bases de datos públicas de cuentas filtradas para estudiar las palabras, frases o cadenas de caracteres que los usuarios a lo largo del mundo más utilizan a la hora de elaborar sus contraseñas. Uno de los principales datos que mostró el análisis es *que 23.2 millones de cuentas filtradas utilizaban 123456 como contraseña* [2], esto refleja la baja concientización que los usuarios tienen en cuanto al riesgo que se exponen al hacer uso de contraseñas débiles y las consecuencias que esto puede tener para la privacidad y el cuidado de la información personal.

II. MÉTODOS

Es importante que conozcamos cómo funciona la técnica de ataque de Fuerza Bruta con Diccionario de Datos, y de esta manera comprobar que es cuestión de tiempo y de recursos llegar a vulnerar los métodos de autenticación simple "Contraseñas".

Es a través de herramientas, que son cada vez más automatizadas, facilitan la tarea a personas mal intencionadas en el acceso de información confidencial. Una de las técnicas más usadas es el llamado "Ataque por Fuerza bruta" y se basa en la combinación de letras de un abecedario, números y símbolos especiales variando la longitud de la cadena hasta dar con la cadena desconocida, es un ataque sencillo en su concepción y certero de prueba y error.

Las etapas que hacen parte de este ataque se podrían resumir en: Identificación del objetivo, identificación de los valores de entrada, generación de datos aleatorios, monitoreo de las excepciones y por ultimo determinar la explotabilidad del objetivo [1]; a continuación, se muestra una implementación en *Python* de un algoritmo que busca por fuerza bruta una cadena desconocida con la ayuda de un diccionario de datos.

Ataque de diccionario.- Un ataque de diccionario es una técnica de violación de contraseñas, en la cual se prueban consecutivamente palabras de un diccionario para validar una clave correcta, para este tipo de ataques se cuenta con listados de claves o *passwords*; los cuales son archivos de texto que se pueden descargar de Internet o de algún repositorio, existen muchos sitios o repositorios donde se publican listados de claves, incluso de algunos que sirvieron para vulnerar sitios web

Para referenciar este artículo (IEEE):

[N] E. Mendoza, «Aplicación de Fuerza Bruta con Diccionario de Datos, para vulnerar contraseñas débiles en Archivos Comprimidos Zip», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 23-25, 2020.

los cuales sufrieron ataques en sus servidores y los datos de sus usuarios quedaron expuestos [3].

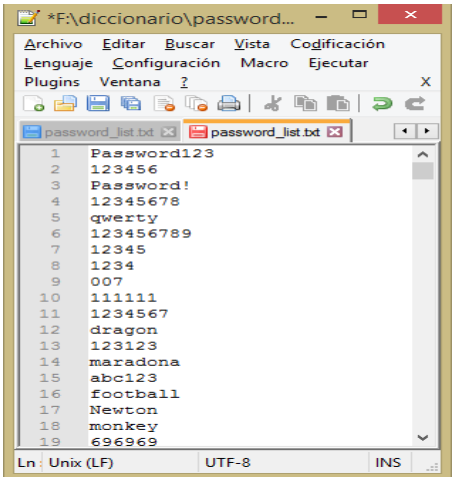

Fig. 1. Diccionario de palabras más utilizadas según varias publicaciones. Fuente: propia

Este ataque es muy similar al ataque por fuerza bruta, la diferencia radica en que esta prueba con una serie de palabras probables en lugar de generar combinaciones [4], generalmente las más utilizadas o las que tengan relación con la víctima. Si la cadena utilizada está en el diccionario se consigue reducir sustancialmente el tiempo necesario para encontrarla; además la utilización de palabras existentes y comunes como "secreto", "admin" o "1234" facilita este tipo de ataques.

III. Resultado

A. *Desarrollo de la Aplicación*

Podemos creer que los documentos comprimidos permiten *añadir seguridad a nuestros archivos*, ya que podemos añadir una contraseña a nuestro archivo comprimido "zip", una contraseña que "en teoría" es irrompible y permite que nuestro archivo comprimido sólo pueda ser abierto con una contraseña especial.

Acá se puede observar como una simple aplicación desarrollada en *python* (ataquefun.py), ayuda a vulnerar y determinar la contraseña de un archivo comprimido con extensión ".zip" revelando su clave.

B. *Descargo de responsabilidades*

(Disclaimer) La presente aplicación del algoritmo desarrollado muestra la vulnerabilidad existente en archivos con extensión zip, por lo cual este material debe usarse solo con propósitos académicos educativos, ni el autor, ni la revista se hace responsables del mal uso del cual se le pueda hacer a esta aplicación.

Para averiguar la contraseña del archivo comprimido, tendremos que usar la sintaxis de ataquefun.py, en el cual tendremos que colocar el nombre de nuestra función seguido de unos parámetros que debemos entender que significan. Aquí va un significado de los parámetros:

-l: especifica el archivo de diccionario con extensión .txt (el cual debe estar en la misma carpeta).

-f: especifica el archivo ZIP (el cual debe estar en la misma carpeta).

En este caso, se hará uso del archivo sa.zip, el cual es un archivo comprimido con clave **N3wt0n!**, una clave sencilla que se asignó como prueba para poder observar que no tarda demasiado y es fácil de determinar por método programado.

El comando que debemos escribir es:

ataquefun.py -l password_list.txt -f sa.zip.

Fig. 2. Código Fuente Python. Fuente: propia

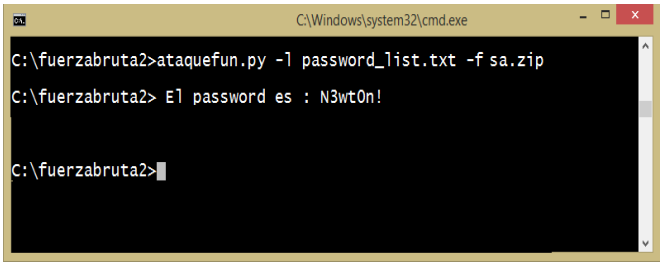

Fig. 3. Resultado de la aplicación. Fuente: propia

IV. Discusión

Se sabe que los métodos de cracking de contraseñas van evolucionando y haciendo cada vez más sencilla esta tarea, y a la vez la hace más complicada para el usuario, por lo que cada vez es más difícil construir una contraseña.

Existen varias recomendaciones de expertos y/o organizaciones que van desde el uso de contraseñas, con letras mayúsculas, minúsculas y números y/o caracteres especiales, para hacer más difícil la determinación de estos, pero en la actualidad se puede vulnerar ya este tipo de contraseñas justamente con esta técnica (ataque de fuerza bruta con

diccionario), a la fecha las recomendaciones en contraseñas promueven que sean frases largas unidas para incrementar la dificultad para determinarlas.

V. Conclusiones

Se pudo observar que realizar la vulneración de la contraseña de un archivo comprimido con extensión ".zip", no es compleja y se puede realizar haciendo uso de recurso bajos, simplemente una aplicación desarrollada en *python*, un diccionario de datos y el archivo con extensión ".zip" del cual se quiere determinar su contraseña.

La técnica de fuerza bruta, es una de las técnicas más antiguas para realizar un ataque que permite descubrir una contraseña desconocida, básicamente es ir probando las posibles cadenas que se encuentren en el diccionario y la combinación de estas las cuales serán un factor muy importante para el éxito.

Referencias

[1] V. López, «Papel de la explosión combinacional en ataques de fuerza bruta,» Investigación Innovación Ingeniería, vol. 1, nº 1, pp. 28-32, 2013.

[2] J. M. Harán, «Welivesecurity.com,» ESET, 22 Abril 2019. [En línea]. Available: https://www.welivesecurity.com/la-es/2019/04/22/millones-cuentas-filtradas-utilizaban-123456-contrasena/. [Último acceso: 24 enero 2020].

[3] A. Ciaurriz, «Seguridad Informática,» 21 noviembre 2016. [En línea]. Available: https://inforseguridad.wordpress.com/2016/11/21/ataques-de-diccionario-ataques-de-fuerza-bruta-programas-diccionarios/. [Último acceso: 25 enero 2020].

[4] W. Stallings, Fundamentos de la seguridad en redes, Prentice Hall, 2004.

Breve CV del autor

Edgar Mendoza Fernandez es Licenciado en Informática por la Universidad Mayor de San Andrés, NB/ISO 27001, NB/ISO/IEC 27032, Diplomado en Seguridad de la Información, Diplomado en Auditoría Informática. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática UMSA.
Miembro del comité editorial-científico de la Revista PGI – Ciencia, Innovación y Tecnología en Informática (2019-2020).
Miembro del grupo de investigación GI-FORSAI UMSA. Ejerce la docencia universitaria en la UMSA y en la Universidad Boliviana de Informática. Ganador 1er lugar Concurso de Investigación CCBOL 20.
Trabajó en la empresa Setel Ingeniería-Ututel SRL, y en AXS-Bolivia Data Center.
Email: emendozaf16@gmail.com. ORCID ID: https://orcid.org/0000-0001-8543-6214.