

INTRODUCCION A LA SEGURIDAD DE LA INFORMACION



INSTITUTO TECNOLÓGICO DE MORELIA
Mapa Conceptual Comunicaciones Telegráficas

Carlos Sebastian Madrigal Rodriguez
18121699

Ingeniería en Tecnologías de la Información y la Comunicación
Prof. Antolino Hernández Anastacio
Departamento de Sistemas

Sábado 13 de Marzo del año 2021

1.- Realizar una búsqueda e investigación acerca del ataque de fuerza bruta y uso de diccionario de datos, respondiendo a:

- **¿Cómo se hace o en que consiste el ataque de fuerza bruta?**

Un ataque de fuerza bruta utiliza prueba y error para adivinar la información de inicio de sesión, las claves de cifrado o encontrar una página web oculta. Los hackers trabajan a través de todas las combinaciones posibles con la esperanza de adivinar correctamente. Estos ataques son realizados por "fuerza bruta", lo que significa que utilizan intentos excesivos de fuerza para tratar de "forzar" su camino en sus cuentas privadas.

Este es un viejo método de ataque, pero todavía es eficaz y popular entre los hackers. Porque dependiendo de la longitud y complejidad de la contraseña, romperla puede tardar de unos segundos a muchos años.

- **Herramientas o software que hay para hacer este ataque.**

Aircrack-ng: Se puede utilizar en Windows, Linux, iOS y Android. Utiliza un diccionario de contraseñas ampliamente utilizadas para violar redes inalámbricas.

John the Ripper: Se ejecuta en 15 plataformas diferentes, incluyendo Unix, Windows y OpenVMS. Intenta todas las combinaciones posibles utilizando un diccionario de posibles contraseñas.

LOphtCrack: una herramienta para descifrar contraseñas de Windows. Utiliza tablas arco iris, diccionarios y algoritmos multiprocesador.

Hashcat: funciona en Windows, Linux y Mac OS. Puede realizar ataques simples de fuerza bruta, basados en reglas e híbridos.

DaveGrohl: una herramienta de código abierto para descifrar Mac OS. Se puede distribuir en varios equipos.

Ncrack: una herramienta para descifrar la autenticación de red. Se puede utilizar en Windows, Linux y BSD.

Rainbow Crack: Herramienta de forzamiento bruta utilizada para el agrietamiento de contraseñas. Genera tablas arco iris para su uso mientras realiza el ataque. De esta manera, es diferente de otras herramientas convencionales de forzamiento bruta. Las tablas arco iris se calculan previamente. Ayuda a reducir el tiempo en la realización del ataque.

THC Hydra: es conocido por su capacidad para descifrar contraseñas de autenticaciones de red mediante la realización de ataques de fuerza bruta. Realiza ataques de diccionario contra más de 30 protocolos, incluyendo Telnet, FTP, HTTP, HTTPS, SMB y más. Está disponible para varias plataformas, incluyendo Linux, Windows / Cygwin, Solaris 11, FreeBSD 8.1, OpenBSD, OSX y QNX / Blackberry.

Wfuzz Es una herramienta de creación de contraseñas de la aplicación web como Brutus que intenta descifrar contraseñas a través de un ataque de adivinanzas de fuerza bruta. También se puede utilizar para encontrar recursos ocultos como directorios, servlets y

scripts. Wfuzz también puede identificar vulnerabilidades de inyección dentro de una aplicación como inyección SQL, inyección XSS e inyección LDAP.

Medusa: Es una herramienta de agrietamiento de contraseñas en línea similar a THC Hydra. Afirma ser una herramienta rápida paralela, modular e indiciada para forzar brutos. Es compatible con HTTP, FTP, CVS, AFP, IMAP, MS SQL, MYSQL, NCP, NNTP, POP3, PostgreSQL, pcAnywhere, rlogin, SMB, rsh, SMTP, SNMP, SSH, SVN, VNC, VmAuthd y Telnet. Es una herramienta de línea de comandos, por lo que es necesario utilizar algún nivel de conocimiento de línea de comandos para utilizarla. La velocidad de agrietamiento de contraseñas depende de la conectividad de red. En un sistema local, puede probar 2.000 contraseñas por minuto. También admite ataques paralelos. Además de una lista de contraseñas para probar, también es posible definir una lista de nombres de usuario o direcciones de correo electrónico para probar durante un ataque.

OphCrack Es una herramienta gratuita de agrietamiento de contraseñas basada en tablas arco iris para Windows. Es la herramienta de agrietamiento de contraseñas de Windows más popular, pero también se puede utilizar en sistemas Linux y Mac. Rompe los hashes LM y NTLM. Para romper Windows XP, Vista y Windows 7, también hay mesas arco iris gratuitas disponibles.

Wifislax: es una popular herramienta de hacking de redes Wi-Fi, en donde puedes encontrar una suite completa de herramientas y ganar conocimiento integral al respecto.

- **Recomendaciones o sugerencias para evitar el ataque de fuerza bruta a los sistemas informáticos.**

Bloqueos de cuentas después de intentos fallidos: La implementación de un bloqueo de cuenta después de varios intentos de inicio de sesión sin éxito es ineficaz, ya que hace que su servidor sea presa fácil para los ataques de denegación de servicio. Sin embargo, si se realiza con retrasos progresivos, este método se vuelve mucho más eficaz.

Hacer que el usuario raíz sea inaccesible a través de SSH: Los intentos de fuerza bruta SSH a menudo se llevan a cabo en el usuario raíz de un servidor. Asegúrese de hacer que el usuario raíz sea inaccesible a través de SSH editando el archivo sshd_config. Establezca las opciones 'DenyUsers root' y 'PermitRootLogin no'.

Modificar el puerto predeterminado: La mayoría de los ataques SSH automatizados se intentan en el puerto predeterminado 22. Por lo tanto, correr sshd en un puerto diferente podría resultar ser una forma útil de lidiar con ataques de fuerza bruta. Para cambiar a un puerto no estándar, edite la línea de puerto en el archivo sshd_config.

Usar CAPTCHA: Todos nos acostumbramos a ver CAPTCHA en internet. A nadie le gusta tratar de dar sentido a algo que parece que ha sido garabateado por un niño de dos años, pero herramientas como CAPTCHA hacen que los robots automatizados sean ineficaces.

Limitar inicios de sesión a una dirección IP o rango especificados: Si solo permite el acceso desde una dirección IP o un rango designado, los atacantes de fuerza bruta tendrán que trabajar duro para superar ese obstáculo y obtener acceso con fuerza. Es

como colocar un perímetro de seguridad alrededor de sus datos más preciados, y a todos los que no se originan en la dirección IP correcta no se les permite el acceso.

Emplear autenticación de 2 factores (2FA): La autenticación de dos factores es considerada por muchos como la primera línea de defensa contra ataques de fuerza bruta. La implementación de una solución de este tipo reduce en gran medida el riesgo de una posible violación de datos.

Usar URL de inicio de sesión únicas: Cree direcciones URL de inicio de sesión únicas para diferentes grupos de usuarios. Esto no detendrá un ataque de fuerza bruta, pero la introducción de esa variable adicional hace que las cosas sean un poco más difíciles y consumen mucho tiempo para un atacante.

Supervise los registros del servidor: Asegúrese de analizar sus archivos de registro diligentemente. Los administradores saben que los archivos de registro son esenciales para mantener un sistema. Las aplicaciones de administración de registros, como Logwatch, pueden ayudarle a realizar comprobaciones diarias y pueden generar informes diarios automáticamente.

- **¿Qué es y como se utiliza un diccionario de datos?**

Un diccionario de datos es una colección de descripciones de los objetos o elementos de datos de un modelo de datos en beneficio de los programadores y otros que necesitan hacer referencia a ellos. A menudo, un diccionario de datos es un repositorio de metadatos centralizado.

Un ataque por diccionario: tiene un diccionario con palabras, que pueden ser contraseñas típicas, y las va probando todas. Para cada palabra, la cifra y la compara con el hash a descifrar. Si coinciden, es que la palabra era la correcta.

- **Relación del diccionario de datos con el ataque de fuerza bruta:**

Realmente no es un ataque de fuerza bruta que prueba todas las combinaciones posibles, pero los diccionarios son una de las principales herramientas para cualquier cibercriminal que ejecute los ataques de cracking de contraseñas. ¿En qué consisten? Son conjuntos de frases que se generan a partir de determinadas reglas. Por ejemplo, que las potenciales contraseñas sean series numéricas, alfanuméricas o que vayan incluyendo distintos caracteres especiales a medida que se vaya generando cada contraseña. Entre las herramientas disponibles, se encuentran los generadores de diccionario. Reiteramos el hecho de que estos programas pueden consumir muchísimos recursos de cómputo.

2.- Investigar sobre la herramienta de crack de contraseñas, basado en fuerza bruta, llamada "Jhon The Ripper". También responder a:

- John the Ripper es una herramienta de auditoría de seguridad de contraseñas de código abierto y recuperación de contraseñas disponible para muchos sistemas operativos. John the Ripper jumbo es compatible con cientos de tipos de hash y cifrado, incluyendo para:

contraseñas de usuario de sabores Unix (Linux, *BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "aplicaciones web" (por ejemplo, WordPress), groupware (por ejemplo, Notes/Domino) y servidores de bases de datos (SQL, LDAP, etc.); capturas de tráfico de red (autenticación de red de Windows, WiFi WPA-PSK, etc.); claves privadas cifradas (SSH, GnuPG, monederos criptomoneda, etc.), sistemas de archivos y discos (archivos macOS .dmg y "paquetes dispersos", Windows BitLocker, etc.), archivos (ZIP, RAR, 7z) y archivos de documentos (PDF, Microsoft Office, etc.)

- **¿En que plataformas se puede ejecutar?**

Se ejecuta en 15 plataformas diferentes, incluyendo Unix, Windows y OpenVMS.

- **¿Esta ya instalado en tu sistema de Linux?**

Si, por defecto en Kali Linux no viene instalado ya que se instala la versión mínima primero. Si se quiere obtener todas las mejores herramientas para pentesting y hackeo en general, se requiere instalar la versión completa de Kali Linux; Esto se puede obtener con los siguientes comandos:

sudo apt-get update -y	-> Actualiza el índice de paquetes de Linux.
sudo apt-get upgrade -y	-> Actualiza la lista de paquetes disponibles.
sudo apt-get install kali-linux-default	-> Versión completa de Kali.

- **Instrucción para instalarlo en Linux (CentOS o Debian)**

Debian: apt-get install -y john

CentOS:

Se puede bajar el archivo de instalación .rpm e instalarlo:

wget http://pkgs.repoforge.org/john/john-1.7.9-1.el6.rf.x86_64.rpm

rpm -Uvh john*.rpm

O directamente de la terminal:

yum install john

Preferentemente se recomienda descargar la versión "bundle", que se encuentra en el repositorio de github. Este es el descifrador de contraseñas sin conexión avanzado, que admite cientos de tipos de cifrado y hash, y se ejecuta en muchos sistemas operativos, CPU, GPU e incluso algunos FPGA.

Para instalarlo, se hace una descarga del repositorio a cualquier ubicación del sistema de archivos de Linux (se prefiere que se descargue en la carpeta /Desktop y luego se instale en la carpeta /sbin/ ya que ahí se almacenan los programas ajenos al sistema operativo pero que solo se ejecutan de manera administrativa) con el comando:

git clone [git@github.com:openwall/john.git](https://github.com/openwall/john)

Una vez clonado el repositorio, se descomprime el archivo zip usando el comando **unzip** y al terminar la extracción, nos adentramos a la carpeta, dirigiéndonos a la carpeta **src** y ejecutamos el comando **./configure && make** para compilar los archivos fuentes de make. Una vez finalizado, podemos mover la carpeta **/run** que se encuentra adentro de **/John** y la movemos a **/sbin**; antes de mover la carpeta, se recomienda renombrar la carpeta **/run** a **/John**, se puede lograr esto con el comando **mv /run John**. Ya renombrada la carpeta, ahora si se mueve usando el comando **mv /run /sbin/**. Para mas información sobre la instalación, viene un manual de instalación parfa cada distribución de Linux en la carpeta **/docs**.

- **¿Como ejecutarlo?**

Si se configuro una variable de entorno al momento de hacer la instalación de john, se podría ejecutar desde cualquier ubicación en el árbol de archivos de Linux usando el comando **john**; al ejecutar este sencillo comando, le mostrara una lista de argumentos (ya que esta incompleto el simple comando "john"), para que agregue funcionalidad. Un ejemplo:

John -format=crypto -wordlist=/usr/share/wordlist/rockyou.txt [hash]

Donde **-format=** indica el algoritmo de encriptación a utilizar para generar el hash y **-wordlist** indica el diccionario de datos a utilizar para adivinar la contraseña no cifrada, en este caso se utilizo **rockyou.txt** que es una lista que viene por defecto al instalar john.

- En otro caso, si al instalar no se configuro una variable de entorno para john, se deberá de navegar al directorio en donde se encuentre descargado el archivo ejecutable de este programa (john).

- **Consultar algún video del uso de John The Ripper, en youtube. Y proporcionar la liga consultada.**

John Hammond: picoCTF 2018[04] Here's Johnny! => [picoCTF 2018 \[04\] Here's Johnny! - YouTube](#)

Network Chuck: how to HACK a password // password cracking with Kali Linux and HashCat => [\(1\) how to HACK a password // password cracking with Kali Linux and HashCat - YouTube](#)

- **Mencionar las funcionalidades que presta la herramienta para ayudarnos a administrar cuentas y contraseñas de los usuarios de los sistemas Linux.**

Es una herramienta de seguridad muy popular, ya que permite a los administradores de sistemas comprobar que las contraseñas de los usuarios son suficientemente buenas. John the Ripper es capaz de autodetectar el tipo de cifrado de entre muchos disponibles, y se puede personalizar su algoritmo de prueba de contraseñas.

3.- Ejemplo de Craqueo de contraseñas de un usuario en Linux.

- **adduser joaquin -> 123456**

Se crea un nuevo usuario con contraseña 123456.

- **/sbin/John/unshadow /etc/passwd /etc/shadow > unshadowed.txt**

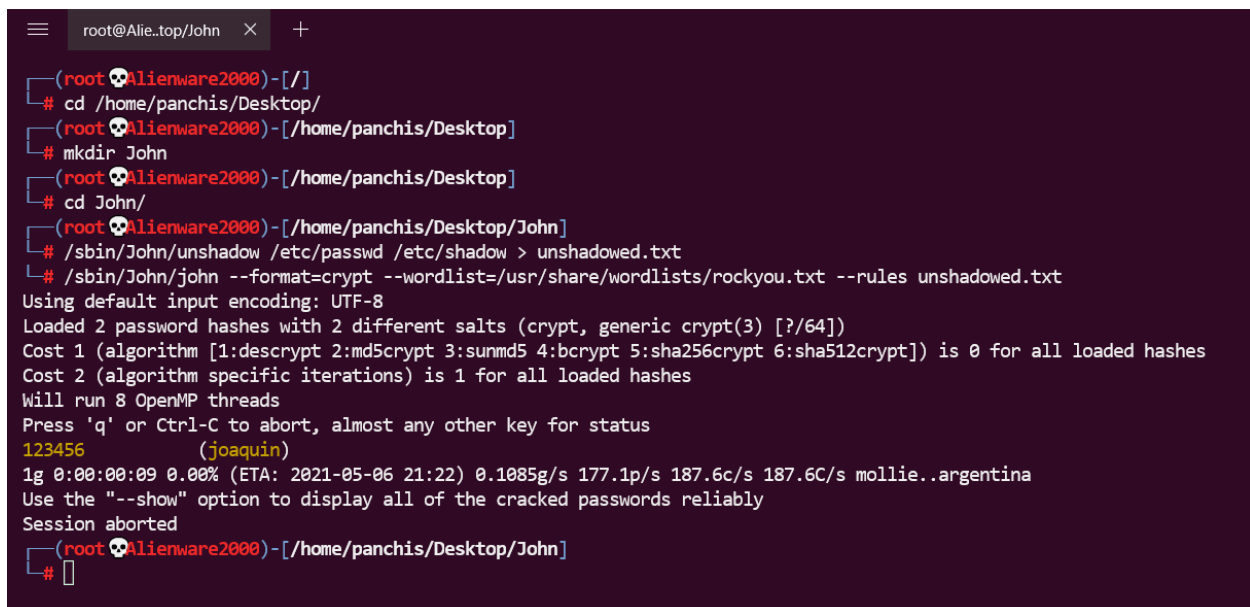
El comando unshadow básicamente combinará los datos de /etc /passwd y /etc /shadow para crear 1 archivo con detalles de nombre de usuario y contraseña.

- **/sbin/John/john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt --rules unshadowed.txt**

Con este comando, le decimos a john que la contraseña esta cifrada con --format=crypt, que agarre el wordlist "rockyou.txt" y que utilice como hash, la contraseña cifrada de los usuarios existentes en el sistema, entre ellos Joaquin. Con este comando, debería de arrojararnos la contraseña "desnuda" de joaquin.

- **deluser joaquin**

Eliminamos al usuario Joquin.



```
root@Alie.top/John X +
(root@Alienware2000)-[/]
# cd /home/panchis/Desktop/
(root@Alienware2000)-[/home/panchis/Desktop]
# mkdir John
(root@Alienware2000)-[/home/panchis/Desktop]
# cd John/
(root@Alienware2000)-[/home/panchis/Desktop/John]
# /sbin/John/unshadow /etc/passwd /etc/shadow > unshadowed.txt
# /sbin/John/john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt --rules unshadowed.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (joaquin)
1g 0:00:00.09 0.00% (ETA: 2021-05-06 21:22) 0.1085g/s 177.1p/s 187.6c/s 187.6C/s mollie..argentina
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
(root@Alienware2000)-[/home/panchis/Desktop/John]
#
```

Fig.1. Craqueo de contraseña del usuario "joaquin".

Referencias

1. Poston, H. (2021, February 18). 10 most popular password cracking TOOLS [updated 2020]. Retrieved March 13, 2021, from <https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/>
2. Kaspersky. (2020, July 16). Brute force attack: What you need to know to keep your passwords safe. Retrieved March 13, 2021, from <https://www.kaspersky.com/resource-center/definitions/brute-force-attack>

3. PhoenixNAP. (2021, March 5). How To Prevent Brute Force Attacks With 8 Easy Tactics. Retrieved March 13, 2021, from <https://phoenixnap.com/kb/prevent-brute-force-attack>
4. Chai, W. (2020, April 14). What is a data dictionary and why use one? Retrieved March 13, 2021, from <https://searchapparchitecture.techtarget.com/definition/data-dictionary>
5. Fernández, L. (2020, July 7). Ataque fuerza bruta: Que es Y Como funciona este ataque para crackear contraseñas. Retrieved March 13, 2021, from [Ataque fuerza bruta: Qué es y cómo funciona este ataque para crackear contraseñas \(redeszone.net\)](https://redeszone.net/ataque-fuerza-bruta-que-es-y-como-funciona-este-ataque-para-crackear-contrasenas/)
6. Opewall. (n.d.). John the Ripper password cracker. Openwall - bringing security into open computing environments. Retrieved March 13, 2021, from [John the Ripper password cracker \(openwall.com\)](https://openwall.com/wiki/john/)
7. Admin. (2017, February 24). Installing "John the Ripper" - The password cracker - ShellHacks. Retrieved March 13, 2021, from <https://www.shellhacks.com/install-john-the-ripper-password-cracker/>