Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2020 pp. 27-31 *Correo: editor@istvidanueva.edu.ec*
Volumen 4, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: septiembre 2020 *Fecha de aceptación: noviembre 2020*

Medusa herramienta para realizar ataques de fuerza bruta

Larenas Juan[1]; Rosero Alexis[2]

[1] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, juanlarenas@hotmail.com*
[2] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, fersilent@gmail.com*

Resumen: Un ataque de fuerza bruta es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Medusa es un software para atacar a nivel de fuerza bruta basándonos en diccionarios de palabras, es muy estable, sencillo, rápido y nos permitirá realizar el ataque a muchos servicios. Este programa lo podemos encontrar en los repositorios de nuestra distribución con el nombre Medusa, si no es así podemos dirigirnos a la página oficial del proyecto.

Palabras clave: Ataque, Servidor, Fuerza Bruta, Diccionario.

Medusa tool for brute-force attacks

Abstract: A brute-force attack is the way to recover a key by trying all possible combinations until you find the one that allows access. Medusa is a software to attack at brute force level based on word dictionaries, it is very stable, simple, fast and will allow us to perform the attack to many services. This program can be found in the repositories of our distribution with the name Medusa, if not we can go to the official page of the project.

Keywords: Attack, Server, Brute Force, Dictionary.

1. INTRODUCCIÓN

El compromiso de las contraseñas es siempre una seria amenaza para la confidencialidad y la integridad de los datos. En general, las contraseñas de menos de 7 caracteres son especialmente susceptibles a ataques de fuerza bruta. Sin embargo, una secuencia de comandos mal escritos o conexiones incorrectas puede ser un signo de intentos de intrusión por fuerza bruta. Rootear. (2014)

Se decidió usar virtualización para minimizar el equipamiento físico necesario. Lo primero fue descargar Kali Linux 2020. Secutity (2018)
La que sería el hospedero para la máquina virtual para usar la herramienta Medusa y Ubuntu Server 14 será la victima que recibirá el ataque. Es importante mencionar también que todo el procedimiento de ataque de fuerza bruta se lo ha realizado por CLI porque es más efectivo, pero el proceso de descargar se lo realizo desde las páginas oficiales de forma gráfica.

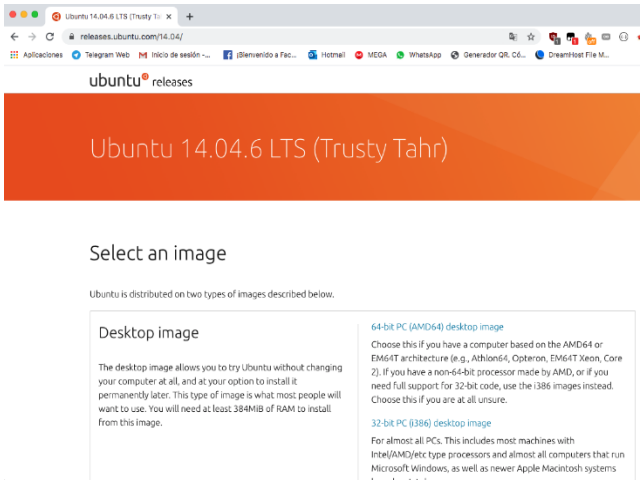

Ilustración 1: Pagina de descarga de Ubuntu Server
Fuente: (Ramos, 2014)

1. Estudiante Universidad Israel, juanlarenas@hotmail.com
2. Estudiante Universidad Israel, fersilent@gmail.com

Revista Nexos Científicos
Julio –Diciembre 2020 pp. 27-31
Volumen 4, Número 2
Fecha de recepción: septiembre 2020
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2020

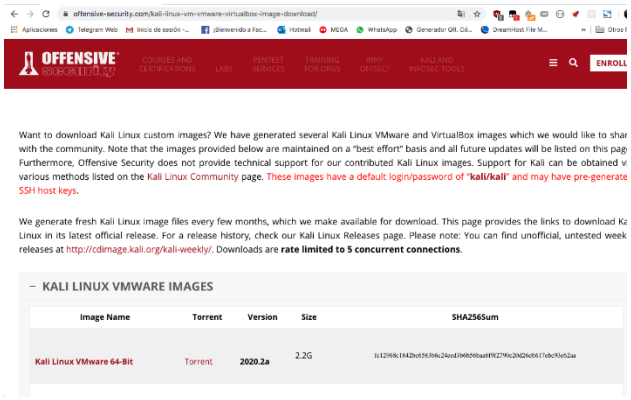

Ilustración 2: Pagina de descarga de Kali Linux
Fuente: (Ramos, 2014)

Nota

Para la virtualización usamos dos máquinas virtuales en VirtualBox. El proceso de instalación no lo describimos pues no es el objetivo primario de este trabajo y además es bastante sencillo e intuitivo, tanto para el sistema operativo de Kali como el de Ubuntu Server, pero se va a indicar los dos sistemas operativos tanto de Kali como de Ubuntu Server después que se hayan instalado en VirtualBox. Systemadmin. (s.f.).

Ilustración 3: Máquina Virtual de Kali Linux
Fuente: (Ramos, 2014)

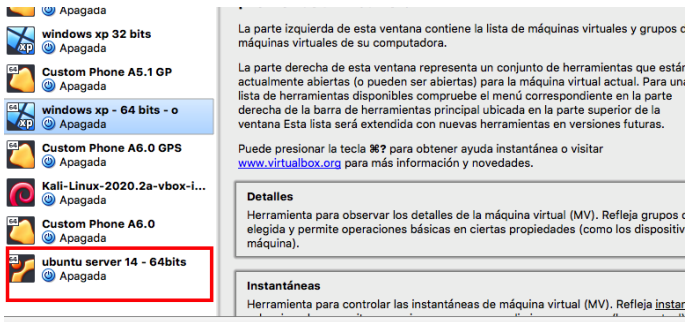

Ilustración 4: Máquina Virtual de Ubuntu Server
Fuente: (Ramos, 2014)

Luego de instalados los dos sistemas operativos, siempre es bueno actualizar, YeHub (2018) para evitar conflictos con ciertos comandos que se van a utilizar, en este caso como son las dos distribuciones Linux basadas en Debian se usarán los mismos comandos para actualizar:

```
# sudo apt-get update    (actualiza los repositorios)
# sudo apt-get upgrade    (actualiza paquetes)
```

Con esto ya tenemos lo necesario instalado y listo para comenzar. Seguridades (2019)

2. METODOLOGÍA

Una vez actualizados los 2 sistemas operativos, vamos a instalar un servidor ssh en Ubuntu Server, ya que este será el que reciba el ataque de fuerza bruta, la instalación procederá de la siguiente manera:

```
# sudo apt-get install openssh-client
(instala el servidor ssh cliente)
# sudo apt-get install openssh-server
(instala el servidor ssh base)
```

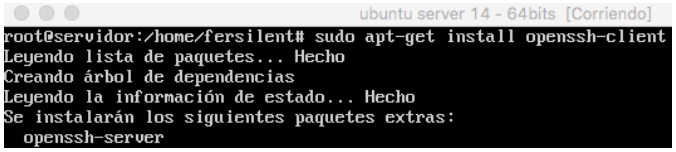

Ilustración 5: Ejecución del comando openssh-client
Fuente: (Ramos, 2014)

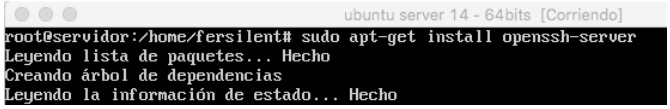

Ilustración 6: Ejecución del comando openssh-server
Fuente: (Ramos, 2014)

Ahora vamos a editar el archivo de configuración ssh, para habilitar las conexiones de entrada

```
# sudo nano /etc/ssh/sshd_config
```

Al final agregamos la siguiente línea, **PermitRootLogin** yes para poder conectarnos como root usando ssh

Revista Nexos Científicos
Julio –Diciembre 2020 pp. 27-31
Volumen 4, Número 2
Fecha de recepción: septiembre 2020
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2020

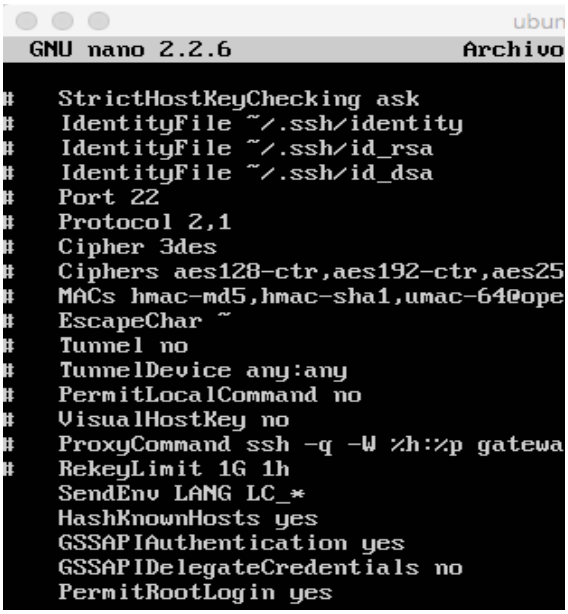

Ilustración 7: Cambio de PermitRootLogin a yes
Fuente: (Ramos, 2014)

Ahora instalaremos medusa en el sistema operativo de Kali

```
# sudo apt-get install medusa
```

Esta Al final de la instalación se podrá obtener todos los servicios a los que se puede realizar Ataque de Fuerza Bruta

```
# sudo medusa -d
```

3. RESULTADOS Y DISCUSIÓN

3.1 Prueba de autenticación de ssh a Ubuntu Server

Abrimos otra consola en el mismo equipo, enviamos a ejecutar un pedido de autenticación de prueba con las credenciales de nuestro servidor ssh

```
# ssh fersilent@192.168.0.6
```

Obtendremos una salida similar a la siguiente:

```
# nano password.txt
```

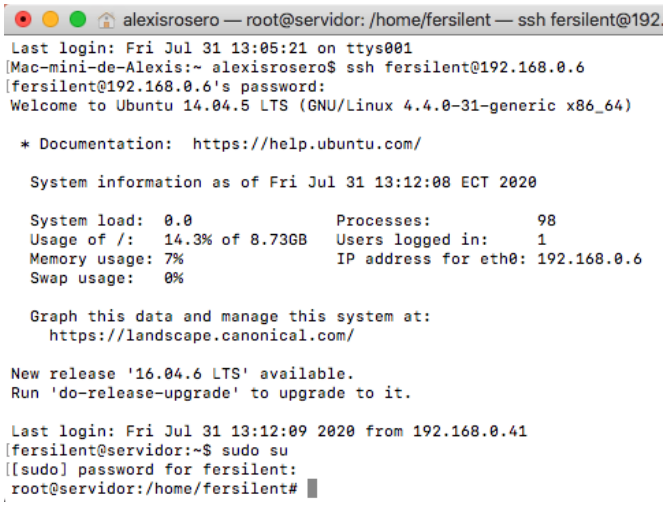

Ilustración 8: Conexión a Ubuntu Server mediante ssh
Fuente: (Ramos, 2014)

Una vez ingresadas las credenciales de **root** y **password** podremos acceder al servicio ssh de forma remota YeHub (2018).

3.2 Prueba de ataque desde kali al servidor ssh de Ubuntu Server.

En el siguiente paso que realizamos es crear un diccionario de datos usando nano con los posibles usuarios

```
# nano usuarios.txt
```

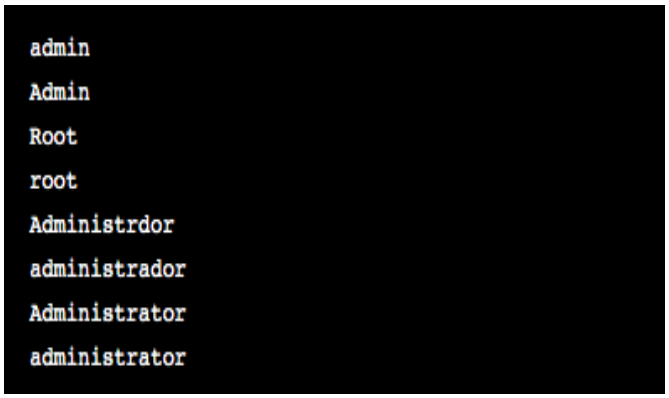

Ilustración 9: Lista de los usuarios
Fuente: (Ramos, 2014)

También debemos crear un archivo con las posibles contraseñas

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2020

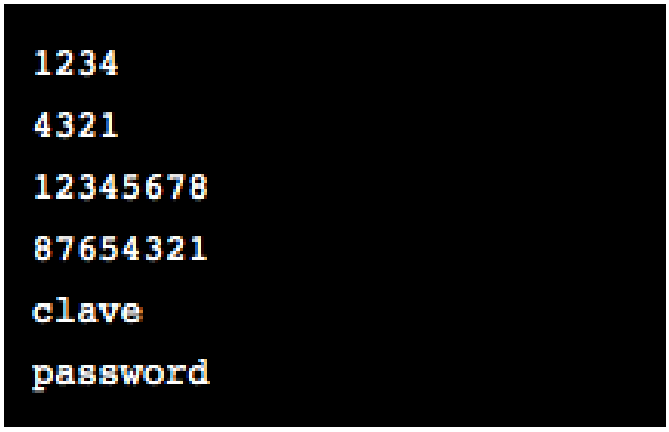

Ilustración 10: Lista de los password
Fuente: (Ramos, 2014)

Antes de ejecutar el comando de ataque al servidor ssh de Ubuntu Server es necesario concocer los parámetros importantes de Medusa.

```
-h: El host al cual le vamos a
realizar el ataque

-H: Para especificar una lista de
hosts

-u: Usuario al que le vamos a realizar
el ataque

-U: Para especificar una lista de
usuarios

-P: Para especificar una lista de
contraseñas

-O: Crea un log

-e: Incluye la verificación con un
password vacío y que el password sea
el        mismo nombre

-M: El modulo que deseamos emplear
(sin la extension .mod)

-n: Para especificar el puerto del
servicio (En caso de que no este
corriendo      en el default)

-s: Habilita ssl

-f: Se detiene al encontrar la
contraseña

-b: Suprime los banners
```

Una vez conocido el significado de los parámetros de ataque, ejecutamos el comando para obtener el usuario y el password de nuestro servidor ssh en Ubuntu Server. YeHub (2020)

El resultado después de unos minutos será el siguiente:

```
# medusa -h 192.168.0.6 -U usuarios.txt
-P password.txt -M ssh -f -b -v 6 -e ns
```

Al final de todo esto hemos obtenido el usuario y contraseña que hemos ingresado antes para conectarnos a nuestro servidor ssh de Ubuntu Server.

```
ACCOUNT FOUND: [ssh] Host: 192.168.0.6
User: root Password: password [SUCCESS]
```

4. CONCLUSIONES

- Para encontrar que servicios y en que puertos se está ejecutando en determinado equipo debemos utilizar otras herramientas como Nmap.
- Podemos ir armando nuestros propios diccionarios, también en Internet se pueden encontrar listado de diccionarios con claves y usuario comunes.
- La mejor forma de defenderse de este tipo de programas es restringir el número de intentos de autentificación, y tener una compleja combinación de usuario/contraseña.
- Excelente herramienta para atacar a nivel de fuerza bruta basada en diccionarios de palabras, tanto para descifrar usuarios y contraseñas
- Fácil de entender y usar, ya que una vez instalada en el sistema operativo muestra los diferentes comandos de ayuda con el comando help
- Se puede crackear por diccionario de una manera muy rápida a una gran cantidad de servicios ya que es compatible con múltiples protocolos.

- Compatible con sistemas operativos Unix y Linux.

- En comparación con otras herramientas como Hydra, Medusa es más lento ya que es una herramienta bastante antigua.

- No se debe usar contraseñas débiles, ya que cualquier persona con un conocimiento en esta herramienta podría realizar un ataque de fuerza bruta.

- Esta herramienta no solo sirve para realizar ataques de fuerza bruta a servicios de consola como ssh, también se la puede emplear para realizar ataques a formularios web.

REFERENCIAS

Rootear. (Abril 19, 2014). Ataques de fuerza bruta. Obtenido de https://rootear.com/ubuntu-linux/ataques-defuerzabruta#:~:text=Medusa%20es%20un%20software%20para,el%20ataque%20a%20muchos%20servicios

Secutity. (Octubre 14, 2018). Obteniendo contraseñas de cualquier servidor. Obtenido de https://securityhacklabs.net/articulo/hacking-ssh-obteniendo-contrasenas-de-cualquier-servidor-mediante-fuerza-bruta

YeHub. (April 23, 2018). Bruteforce Password. Obtenido de https://www.yeahhub.com/bruteforce-password-cracking-medusa-kali-linux/

Systemadmin. (s.f.). Medusa. Obtenido de http://systemadmin.es/2010/09/medusa-herramienta-generica-para-hacer-ataques-de-fuerza-bruta

Seguridades. (Mayo 19, 2019). Medusa Herramienta Generica. Obtenido de http://seguridades.com/herramienta-generica

Mundohackers. (s.f.). Herramientas de Fuerza Bruta. Obtenido de http://mundohackers.com/

Mundohackers. (s.f.). Uso de Medusa en Kali. Obtenido de http://mundohackers.com/medusa

Kalilinux. (s.f.). Uso de Kali linux. Obtenido de http://kalilinux.com/downloads

YeHub. (April 23, 2018). Medusa in Kali. Obtenido de https://www.yeahhub.com/kali-linux/

YeHub. (May 28, 2020). Security in Kali https://www.yeahhub.com/security/kali