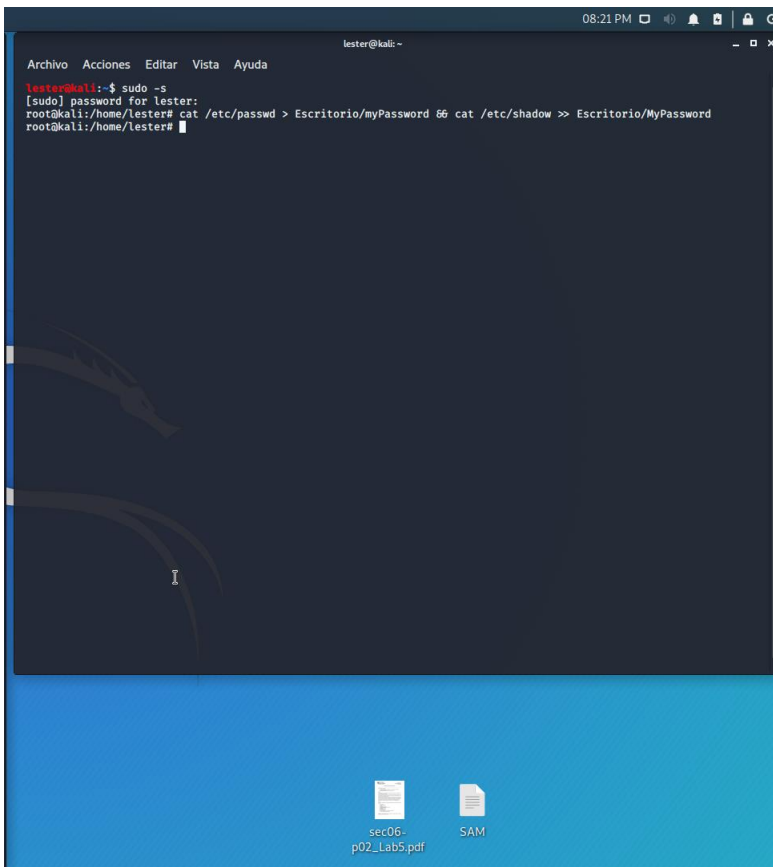


Axel Rodríguez 1229715
Lester García 1003115
Edwin Hilario 1298816
Manuel Catalán 1038416
Steven Villatoro 1129215

Laboratorio Seguridad - Passwords en Sistemas operativos

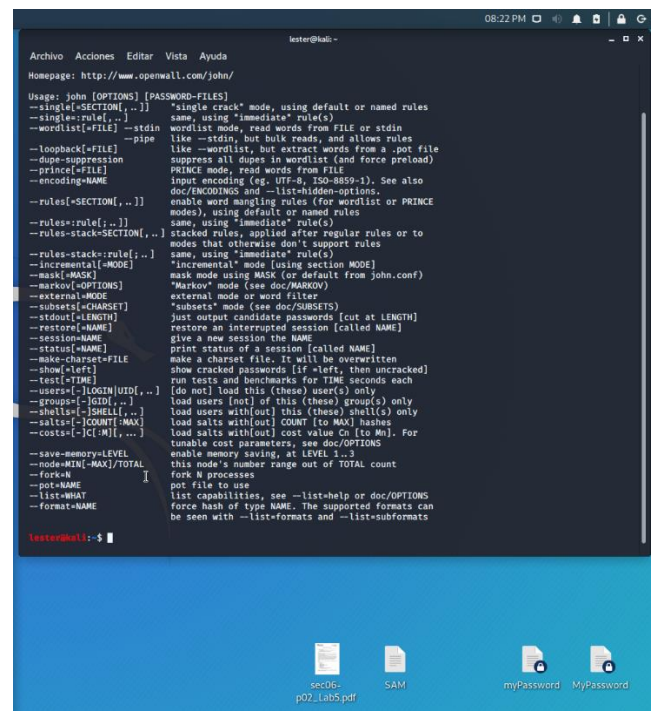
Parte 01

En el escritorio luego de ejecutar el comando: `cat /etc/passwd > Desktop/myPassword && cat /etc/shadow >> Desktop/MyPassword` se generaron dos archivos con el nombre myPassword y MyPassword los cuales contendrán la concatenación de las contraseñas de Kali Linux en funcionamiento y la información general del archivo Shadow.



```
ltester@kali:~$ sudo -s
[sudo] password for ltester:
root@kali:~# cat /etc/passwd > Escritorio/myPassword && cat /etc/shadow >> Escritorio/MyPassword
root@kali:~#
```

The terminal window shows the user ltester@kali. The command executed is `cat /etc/passwd > Escritorio/myPassword && cat /etc/shadow >> Escritorio/MyPassword`. The desktop background is Kali Linux, and the files `sec06-p02_Lab5.pdf` and `SAM` are visible on the desktop.



```
ltester@kali:~$ john --help
Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,...]] "single crack" mode, using default or named rules
--single-rule[=RULE] same, using "immediate" rule(s)
--wordlist[=FILE] wordlist mode, read words from FILE or stdin
--pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE] like --wordlist, but extract words from a .pot file
--dupes-suppression suppress all dupes in wordlist (and force preload)
--prince[=FILE] PRINCE mode, read words from FILE
--encoding=NAME input encoding (eg. UTF-8, ISO-8859-1). See also
--rules[=SECTION[,...]] enable word mangling rules (for wordlist or PRINCE
--rules=rule[,...]) modes), using default or named rules
--rules-stack=SECTION[,...] same, using "immediate" rule(s)
--rules-stack=rule[,...] stacked rules, applied after regular rules or to
--rules-stack=SECTION[,...] modes that otherwise don't support rules
--rules-stack=rule[,...] same, using "immediate" rule(s)
--incremental[=MODE] "incremental" mode [using section MODE]
--mask[=MASK] mask mode using MASK (or default from john.conf)
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)
--external=MODE external mode or word filter
--subsets[=CHARSET] "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset file. It will be overwritten
--show[=left] show cracked passwords [if left, then uncracked]
--test[=TIME] run tests and benchmarks for TIME seconds each
--users[=LOGIN|UID[,...]] (do not) load this (these) user(s) only
--groups[=GID[,...]] load users [out] of this (these) group(s) only
--shells[=SHELL[,...]] load users with[out] this (these) shell(s) only
--salts[=COUNT|MAX] load salts with[out] COUNT (to MAX) hashes
--costs[=C|C-MIN[,...]] load salts with[out] cost value Cn [to Mn]. For
tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL enable memory saving, at LEVEL 1-3
--node=MIN[-MAX]/TOTAL this node's number range out of TOTAL count
--fork=N fork N processes
--pot=NAME pot file to use
--list=WHAT list capabilities, see --list-help or doc/OPTIONS
--format=NAME force hash of type NAME. The supported formats can
be seen with --list-formats and --list-subformats

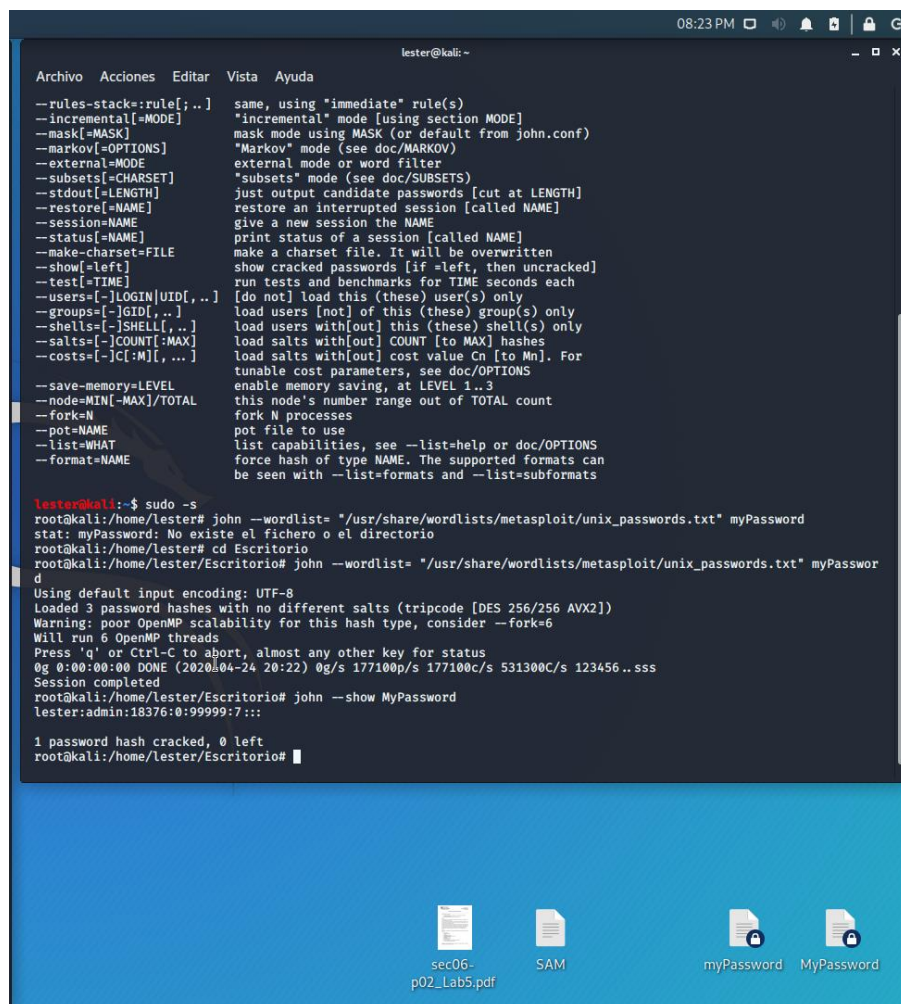
ltester@kali:~$
```

The terminal window shows the usage of the John the Ripper password cracking tool. The command executed is `john --help`. The output shows the usage of the tool and the list of options. The desktop background is Kali Linux, and the files `sec06-p02_Lab5.pdf`, `SAM`, `myPassword`, and `MyPassword` are visible on the desktop.

Axel Rodríguez 1229715
Lester García 1003115
Edwin Hilario 1298816
Manuel Catalán 1038416
Steven Villatoro 1129215

Parte 02

Kali Linux posee una herramienta preinstalada la cual lleva por nombre “John the ripper”, la cual se encarga de vulnerar contraseñas dentro de dicho sistemas en un tipo definido de archivo. Al entrar a dicha aplicación en modo root se utilizó la opción del menú de aplicaciones y el apartado de contraseñas.



```
lester@kali: ~
Archivo Acciones Editar Vista Ayuda

--rules-stack=:rule[;..] same, using "immediate" rule(s)
--incremental[=MODE] "incremental" mode [using section MODE]
--mask[=MASK] mask mode using MASK (or default from john.conf)
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)
--external=MODE external mode or word filter
--subsets[=CHARSET] "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset file. It will be overwritten
--show[=left] show cracked passwords [if =left, then uncracked]
--test[=TIME] run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..] load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][, ...] load salts with[out] cost value Cn [to Mn]. For
tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL this node's number range out of TOTAL count
--fork=N fork N processes
--pot=NAME pot file to use
--list=WHAT list capabilities, see --list=help or doc/OPTIONS
--format=NAME force hash of type NAME. The supported formats can
be seen with --list=formats and --list=subformats

lester@kali:~$ sudo -s
root@kali:/home/lester# john --wordlist= "/usr/share/wordlists/metasploit/unix_passwords.txt" myPassword
stat: myPassword: No existe el fichero o el directorio
root@kali:/home/lester# cd Escritorio
root@kali:/home/lester/Escritorio# john --wordlist= "/usr/share/wordlists/metasploit/unix_passwords.txt" myPasswor
d
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (tripcode [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=6
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2020-04-24 20:22) 0g/s 177100p/s 177100c/s 531300C/s 123456..sss
Session completed
root@kali:/home/lester/Escritorio# john --show MyPassword
lester:admin:18376:0:99999:7:::

1 password hash cracked, 0 left
root@kali:/home/lester/Escritorio#
```

Dentro de la aplicación John se ejecutó el siguiente comando estando en el escritorio para poder vulnerar el archivo de la contraseña con un ataque de diccionario.

john --wordlist= "/usr/share/wordlists/metasploit/unix_passwords.txt" myPassword

Axel Rodríguez 1229715
Lester García 1003115
Edwin Hilario 1298816
Manuel Catalán 1038416
Steven Villatoro 1129215

Como podemos observar luego de ejecutar el comando anterior y termine el proceso podemos escribir: john --show MyPassword y luego podremos ver que nos muestra tanto el usuario como la contraseña a la primera.

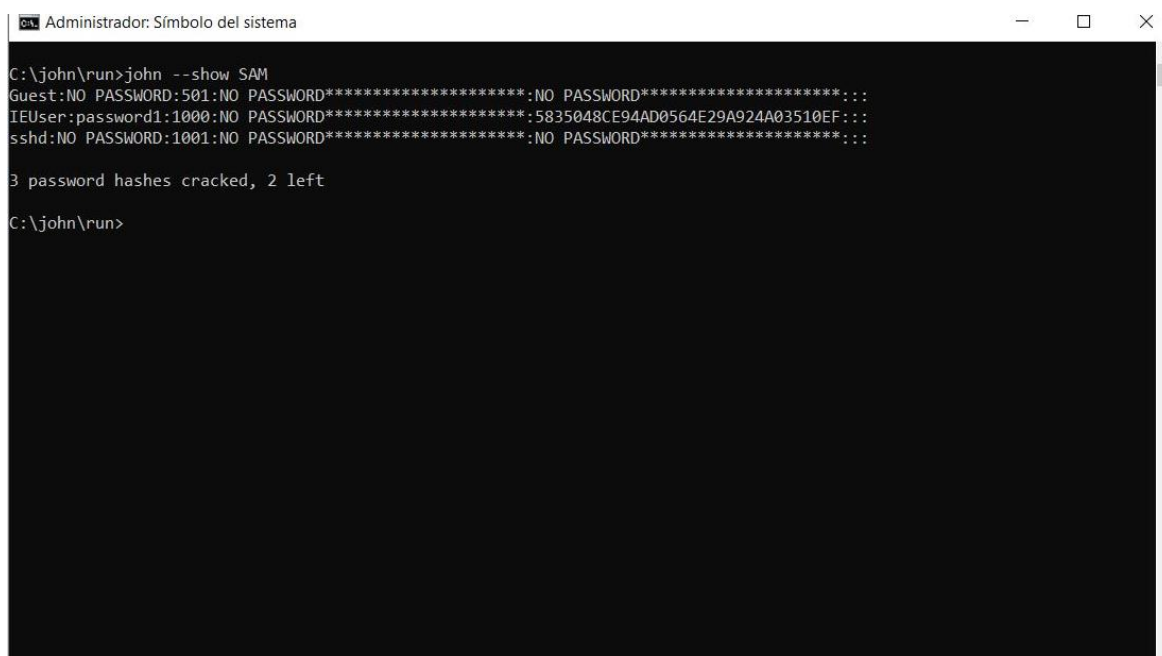
La facilidad con que el programa decodificará la contraseña será en función a la complejidad que presente la contraseña.

```
lester@kali: ~  
Archivo Acciones Editar Vista Ayuda  
--rules[=SECTION[, ..]] doc/ENCODINGS and --list=hidden-options.  
--rules=:rule[; ..]] enable word mangling rules (for wordlist or PRINCE  
--rules-stack=SECTION[, ..] modes), using default or named rules  
--rules-stack=:rule[; ..] same, using "immediate" rule(s)  
--incremental[=MODE] stacked rules, applied after regular rules or to  
--mask[=MASK] modes that otherwise don't support rules  
--markov[=OPTIONS] same, using "immediate" rule(s)  
--external=MODE "incremental" mode [using section MODE]  
--subsets[=CHARSET] mask mode using MASK (or default from john.conf)  
--stdout[=LENGTH] "Markov" mode (see doc/MARKOV)  
--restore[=NAME] external mode or word filter  
--session=NAME "subsets" mode (see doc/SUBSETS)  
--status[=NAME] just output candidate passwords [cut at LENGTH]  
--make-charset=FILE restore an interrupted session [called NAME]  
--show[=left] give a new session the NAME  
--test[=TIME] print status of a session [called NAME]  
--users[=-]LOGIN|UID[, ..] make a charset file. It will be overwritten  
--groups[=-]GID[, ..] show cracked passwords [if =left, then uncracked]  
--shells[=-]SHELL[, ..] run tests and benchmarks for TIME seconds each  
--salts[=-]COUNT[:MAX] [do not] load this (these) user(s) only  
--costs[=-]C[:Mn][, ..] load users [not] of this (these) group(s) only  
--save-memory=LEVEL load users with[out] this (these) shell(s) only  
--node=MIN[-MAX]/TOTAL load salts with[out] COUNT [to MAX] hashes  
--fork=N load salts with[out] cost value Cn [to Mn]. For  
--pot=NAME tunable cost parameters, see doc/OPTIONS  
--list=WHAT enable memory saving, at LEVEL 1..3  
--format=NAME this node's number range out of TOTAL count  
fork N processes  
pot file to use  
list capabilities, see --list=help or doc/OPTIONS  
force hash of type NAME. The supported formats can  
be seen with --list=formats and --list=subformats  
  
lester@kali:~$ sudo -s  
root@kali:/home/lester# john --wordlist= "/usr/share/wordlists/metasploit/unix_passwords.txt" myPassword  
stat: myPassword: No existe el fichero o el directorio  
root@kali:/home/lester# cd Escritorio  
root@kali:/home/lester/Escritorio# john --wordlist= "/usr/share/wordlists/metasploit/unix_passwords.txt" myPasswor  
d  
Using default input encoding: UTF-8  
Loaded 3 password hashes with no different salts (tripcode [DES 256/256 AVX2])  
Warning: poor OpenMP scalability for this hash type, consider --fork=6  
Will run 6 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
0g 0:00:00:00 DONE (2020-04-24 20:22) 0g/s 177100p/s 177100c/s 531300C/s 123456..sss  
Session completed  
root@kali:/home/lester/Escritorio# john --show MyPassword  
lester:admin:18376:0:99999:7:::  
  
1 password hash cracked, 0 left  
root@kali:/home/lester/Escritorio#
```

Axel Rodríguez 1229715
Lester García 1003115
Edwin Hilario 1298816
Manuel Catalán 1038416
Steven Villatoro 1129215

Parte 03

En Windows 10 se utilizó el software “*John the ripper password cracker*”, la versión 1.9-jumbo-1-64-bit. Luego se abrió un nuevo Símbolo de sistema (CMD) con permisos de administrador y se estableció la ruta del disco local C donde se encuentra el ejecutable John y el archivo SAM que contiene los usuarios y contraseñas cifradas fue proporcionado en el portal. Se usó comando “*John –show SAM*”, teniendo como resultado que se obtuvieron 3 contraseñas en el siguiente formato:



```
Administrador: Símbolo del sistema

C:\john\run>john --show SAM
Guest:NO PASSWORD:501:NO PASSWORD*****:NO PASSWORD*****:
IEUser:password1:1000:NO PASSWORD*****:5835048CE94AD0564E29A924A03510EF:
sshd:NO PASSWORD:1001:NO PASSWORD*****:NO PASSWORD*****:

3 password hashes cracked, 2 left

C:\john\run>
```

Y si abrimos el archivo en un bloc de notas nos mostrará lo mismo:



```
SAM.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda

Administrator:500:NO PASSWORD*****:FC525C9683E8FE067095BA2DDC971889::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
IEUser:1000:NO PASSWORD*****:5835048CE94AD0564E29A924A03510EF:
sshd:1001:NO PASSWORD*****:NO PASSWORD*****:
sshd_server:1002:NO PASSWORD*****:8D0A16CFC061C3359DB455D00EC27035::
```