UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERÍA
LICENCIATURA EN SISTEMAS COMPUTACIONALES

NOMBRE	MATERIA	GRUPO	FECHA
Erandi Sacbe Moreno Avendaño	Taller de Linux	103	10/10/2022
MAESTRA	**MATRICULA**	**PRÁCTICA**	
Julia Corrales Espinoza	1190721	#14	

1. Verifique si se intentó ingresar al servidor con los siguientes nombres de usuario: *admin*, *apache*, *mysql*, *juan*, *bd103*.

Con admin si se intentó

```
tl307@vsistemas:~$ grep -w admin auth.log
Jul 28 05:15:02 computacion sshd[8091]: Invalid user admin from 174.133.3.178
Jul 28 05:15:02 computacion sshd[8091]: input_userauth_request: invalid user admin [preauth]
Jul 28 05:15:04 computacion sshd[8091]: Failed password for invalid user admin from 174.133.3.178 port 43796
h2
Jul 28 05:15:04 computacion sshd[8095]: Invalid user admin from 174.133.3.178
Jul 28 05:15:04 computacion sshd[8095]: input_userauth_request: invalid user admin [preauth]
Jul 28 05:15:06 computacion sshd[8095]: Failed password for invalid user admin from 174.133.3.178 port 43952
h2
Jul 28 05:15:07 computacion sshd[8099]: Invalid user admin from 174.133.3.178
Jul 28 05:15:07 computacion sshd[8099]: input_userauth_request: invalid user admin [preauth]
```

Con apache también

```
tl307@vsistemas:~$ grep -w apache auth.log
Jul 28 02:35:14 computacion sshd[22149]: Invalid user apache from 174.133.3.178
Jul 28 02:35:14 computacion sshd[22149]: input_userauth_request: invalid user apache [preauth]
Jul 28 02:35:17 computacion sshd[22149]: Failed password for invalid user apache from 174.133.3.178 port 51580
ssh2
Jul 28 02:35:17 computacion sshd[22157]: Invalid user apache from 174.133.3.178
Jul 28 02:35:17 computacion sshd[22157]: input_userauth_request: invalid user apache [preauth]
Jul 28 02:35:19 computacion sshd[22157]: Failed password for invalid user apache from 174.133.3.178 port 52904
ssh2
Jul 28 02:35:20 computacion sshd[22163]: Invalid user apache from 174.133.3.178
Jul 28 02:35:20 computacion sshd[22163]: input_userauth_request: invalid user apache [preauth]
Jul 28 02:35:22 computacion sshd[22163]: Failed password for invalid user apache from 174.133.3.178 port 53595
ssh2
```

Con mysql también

```
tl307@vsistemas:~$ grep -w mysql auth.log
Jul 28 02:41:51 computacion sshd[23238]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
=ssh ruser= rhost=b2.3.85ae.static.theplanet.com  user=mysql
Jul 28 02:41:53 computacion sshd[23238]: Failed password for mysql from 174.133.3.178 port 54832 ssh2
Jul 28 02:41:53 computacion sshd[23244]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
=ssh ruser= rhost=b2.3.85ae.static.theplanet.com  user=mysql
Jul 28 02:41:55 computacion sshd[23244]: Failed password for mysql from 174.133.3.178 port 55447 ssh2
Jul 28 02:41:56 computacion sshd[23250]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
=ssh ruser= rhost=b2.3.85ae.static.theplanet.com  user=mysql
```

Con juan también

```
tl307@vsistemas:~$ grep -w juan auth.log
Jul 28 05:13:46 computacion sshd[7959]: Invalid user juan from 174.133.3.178
Jul 28 05:13:46 computacion sshd[7959]: input_userauth_request: invalid user juan [preauth]
Jul 28 05:13:48 computacion sshd[7959]: Failed password for invalid user juan from 174.133.3.178 port 33106
2
Jul 28 05:13:49 computacion sshd[7963]: Invalid user juan from 174.133.3.178
Jul 28 05:13:49 computacion sshd[7963]: input_userauth_request: invalid user juan [preauth]
Jul 28 05:13:51 computacion sshd[7963]: Failed password for invalid user juan from 174.133.3.178 port 33257
2
Jul 28 05:15:07 computacion sshd[8098]: Invalid user juan from 174.133.3.178
Jul 28 05:15:07 computacion sshd[8098]: input_userauth_request: invalid user juan [preauth]
```

También con bd103

```
Jul 27 05:27:31 computacion sshd[3413]: Accepted password for bd103 from 189.222.30.218 port 52362 ssh2
Jul 27 05:27:31 computacion sshd[3413]: pam_unix(sshd:session): session opened for user bd103 by (uid=0)
Jul 27 05:30:28 computacion sshd[3413]: pam_unix(sshd:session): session closed for user bd103
```

2. ¿Cuántas veces se hizo el intento con cada usuario del ejercicio anterior?

admin 8

```
tl307@vsistemas:~$ grep -wc "Invalid user admin" auth.log
8
```

apache 40

```
tl307@vsistemas:~$ grep -wc "Invalid user apache" auth.log
40
tl307@vsistemas:~$
```

mysql 122

```
tl307@vsistemas:~$ grep -wc "user=mysql" auth.log
122
```

juan 4

```
tl307@vsistemas:~$ grep -wc "Invalid user juan" auth.log
4
```

3. Muestre un listado de todos los intentos por ingresar al servidor con un nombre de usuario inexistente.

```
grep -i "invalid user" auth.log
```

```
st from 174.133.3.178 port 55466 ssh2
Jul 28 04:16:55 computacion sshd[858]: Failed password for invalid user lieke from 174.133.3.178 port 55475
2
Jul 28 04:16:55 computacion sshd[861]: Failed password for invalid user test1 from 174.133.3.178 port 55500
2
Jul 28 04:16:55 computacion sshd[862]: Failed password for invalid user tanya from 174.133.3.178 port 55504
2
Jul 28 04:16:55 computacion sshd[863]: Failed password for invalid user keith from 174.133.3.178 port 55505
2
Jul 28 04:16:56 computacion sshd[865]: Failed password for invalid user jboss from 174.133.3.178 port 55514
2
Jul 28 04:16:56 computacion sshd[869]: Invalid user test from 174.133.3.178
Jul 28 04:16:56 computacion sshd[869]: input_userauth_request: invalid user test [preauth]
Jul 28 04:16:56 computacion sshd[871]: Invalid user lieke from 174.133.3.178
Jul 28 04:16:56 computacion sshd[871]: input_userauth_request: invalid user lieke [preauth]
Jul 28 04:16:56 computacion sshd[873]: Invalid user test1 from 174.133.3.178
Jul 28 04:16:56 computacion sshd[873]: input_userauth_request: invalid user test1 [preauth]
Jul 28 04:16:56 computacion sshd[874]: Invalid user tanya from 174.133.3.178
Jul 28 04:16:56 computacion sshd[874]: input_userauth_request: invalid user tanya [preauth]
Jul 28 04:16:56 computacion sshd[875]: Invalid user mason from 174.133.3.178
Jul 28 04:16:56 computacion sshd[875]: input_userauth_request: invalid user mason [preauth]
Jul 28 04:16:56 computacion sshd[879]: Invalid user jboss from 174.133.3.178
Jul 28 04:16:56 computacion sshd[879]: input_userauth_request: invalid user jboss [preauth]
Jul 28 04:16:58 computacion sshd[869]: Failed password for invalid user test from 174.133.3.178 port 56617 s
Jul 28 04:16:58 computacion sshd[871]: Failed password for invalid user lieke from 174.133.3.178 port 56632
2
Jul 28 04:16:58 computacion sshd[873]: Failed password for invalid user test1 from 174.133.3.178 port 56654
2
Jul 28 04:16:58 computacion sshd[874]: Failed password for invalid user tanya from 174.133.3.178 port 56656
2
Jul 28 04:16:58 computacion sshd[875]: Failed password for invalid user mason from 174.133.3.178 port 56659
2
Jul 28 04:16:58 computacion sshd[879]: Failed password for invalid user jboss from 174.133.3.178 port 56694
2
Jul 28 04:16:58 computacion sshd[881]: Invalid user test from 174.133.3.178
Jul 28 04:16:58 computacion sshd[881]: input_userauth_request: invalid user test [preauth]
Jul 28 04:16:58 computacion sshd[883]: Invalid user lieke from 174.133.3.178
Jul 28 04:16:58 computacion sshd[883]: input_userauth_request: invalid user lieke [preauth]
Jul 28 04:16:58 computacion sshd[884]: Invalid user test1 from 174.133.3.178
```

4. ¿Cuantas veces intentaron ingresar al servidor con nombres de usuario válidos?

```
tl307@vsistemas:~$ grep -wc "session opened for" auth.log
2737
```

¿Con qué usuario lograron ingresar al servidor (*hackerar*)?

Se utilizará el siguiente comando para buscar las sesiones iniciadas en ese servidor
grep -w “session opened for” auth.log

6. ¿En qué fecha *hackearon* el servidor?

2012

7. ¿Desde qué direcciones de Internet se estuvo lanzando el ataque al servidor?

174.133.3.178

10. Muestre con números de línea las 4 líneas anteriores y las 4 líneas posteriores al ingreso del usuario **prueba**.

grep -C 4 “opened.*prueba” auth.log

12. El directorio **/etc/init.d** contiene archivos para controlar el inicio y término de algunos servicios que se ejecutan en el servidor. Genere un listado de todas las veces que aparece la palabra *“start”* en cada archivo de este directorio. Incluya el número de línea en la que aparece la palabra dentro del archivo.

```
tl307@vsistemas:~$ grep -r -n "start" /etc/init.d/ > start.txt
```

```
tl307@vsistemas:~$ cat start.txt
/etc/init.d/console-setup.sh:18:        start|force-reload|restart|reload)
/etc/init.d/console-setup.sh:42:            echo 'Usage: /etc/init.d/console-setup {start|reload|restart|force-reload|stop|status}'
/etc/init.d/rsyslog:39:do_start()
/etc/init.d/rsyslog:42: #   0 if daemon has been started
/etc/init.d/rsyslog:44: #   other if daemon could not be started or a failure occured
/etc/init.d/rsyslog:45: start-stop-daemon --start --quiet --pidfile $PIDFILE --exec $DAEMON -- $RSYSLOGD_OPTIONS
/etc/init.d/rsyslog:54: start-stop-daemon --stop --quiet --retry=TERM/30/KILL/5 --pidfile $PIDFILE --exec $DAEMON
/etc/init.d/rsyslog:61: start-stop-daemon --stop --signal HUP --quiet --pidfile $PIDFILE --exec $DAEMON
/etc/init.d/rsyslog:84:  start)
/etc/init.d/rsyslog:87: do_start
/etc/init.d/rsyslog:91:         1) log_progress_msg "already started"
/etc/init.d/rsyslog:113:  restart|force-reload)
/etc/init.d/rsyslog:115:        $0 start
/etc/init.d/rsyslog:117:  try-restart)
```

13. ¿Cuáles archivos contienen la palabra *“el”* en los directorios del grupo **tu100**?

```
tl307@vsistemas:~$ grep -rw "el" /externos/home/clases/tl100/
grep: /externos/home/clases/tl100/tl105/.Xauthority: Permission denied
grep: /externos/home/clases/tl100/tl105/.ssh: Permission denied
grep: /externos/home/clases/tl100/tl105/.lesshst: Permission denied
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-16-47.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-27.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-06.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-49-18.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-45.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-39.png matches
grep: /externos/home/clases/tl100/tl105/.ICEauthority: Permission denied
grep: /externos/home/clases/tl100/tl105/.mozilla: Permission denied
grep: /externos/home/clases/tl100/tl105/.gnupg: Permission denied
grep: /externos/home/clases/tl100/tl105/.bash_history: Permission denied
/externos/home/clases/tl100/tl105/practica7/peliculas.txt:El tigre y el Dragon/Ang Lee/Accion/2001
```

14. Utilizando el redireccionamiento de error, elimine los mensajes de error que se mostraron en el ejercicio anterior.

```
tl307@vsistemas:~$ grep -rw "el" /externos/home/clases/tl100/ 2> el.txt
```

```
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-16-47.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-27.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-06.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-49-18.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-45.png matches
Binary file /externos/home/clases/tl100/tl105/Pictures/Screenshot from 2022-09-07 10-17-39.png matches
/externos/home/clases/tl100/tl105/practica7/peliculas.txt:El tigre y el Dragon/Ang Lee/Accion/2001
Binary file /externos/home/clases/tl100/tl105/bin/join matches
Binary file /externos/home/clases/tl100/tl105/bin/git matches
```

Muestre los números de línea en los que aparece la palabra *"linux"* en los archivos que se encuentran en los directorios del grupo tu200 sin que aparezcan mensaje de error.

```
tl307@vsistemas:~$ grep -rw "linux" /externos/home/clases/tl200/ 2> linux.txt
Binary file /externos/home/clases/tl200/tl201/mknod matches
Binary file /externos/home/clases/tl200/tl201/Downloads/practica 4 linux.pdf matches
Binary file /externos/home/clases/tl200/tl201/mkfifo matches
Binary file /externos/home/clases/tl200/tl201/mkdir matches
Binary file /externos/home/clases/tl200/tl201/mksquashfs matches
Binary file /externos/home/clases/tl200/tl201/mktemp matches
Binary file /externos/home/clases/tl200/tl205/Downloads2/Downloads/practica4.pdf matches
Binary file /externos/home/clases/tl200/tl205/Downloads/practica4.pdf matches
/externos/home/clases/tl200/tl205/screenrc:termcapinfo xterm*|linux*|rxvt*|Eterm* OP
```

Conclusiones

El comando grep de linux se utiliza para buscar palabras, caracteres o cadenas dentro de un archivo o directorio, mediante expresiones regulares y parámetros, este comando es de gran utilidad, puesto que, recorta la información a las necesidades del usuario, para facilitar la busqueda de informacion