Laboratorio

ADMINISTRACIÓN DE REGISTROS

Hecho por Ignacio Suárez

Objetivos

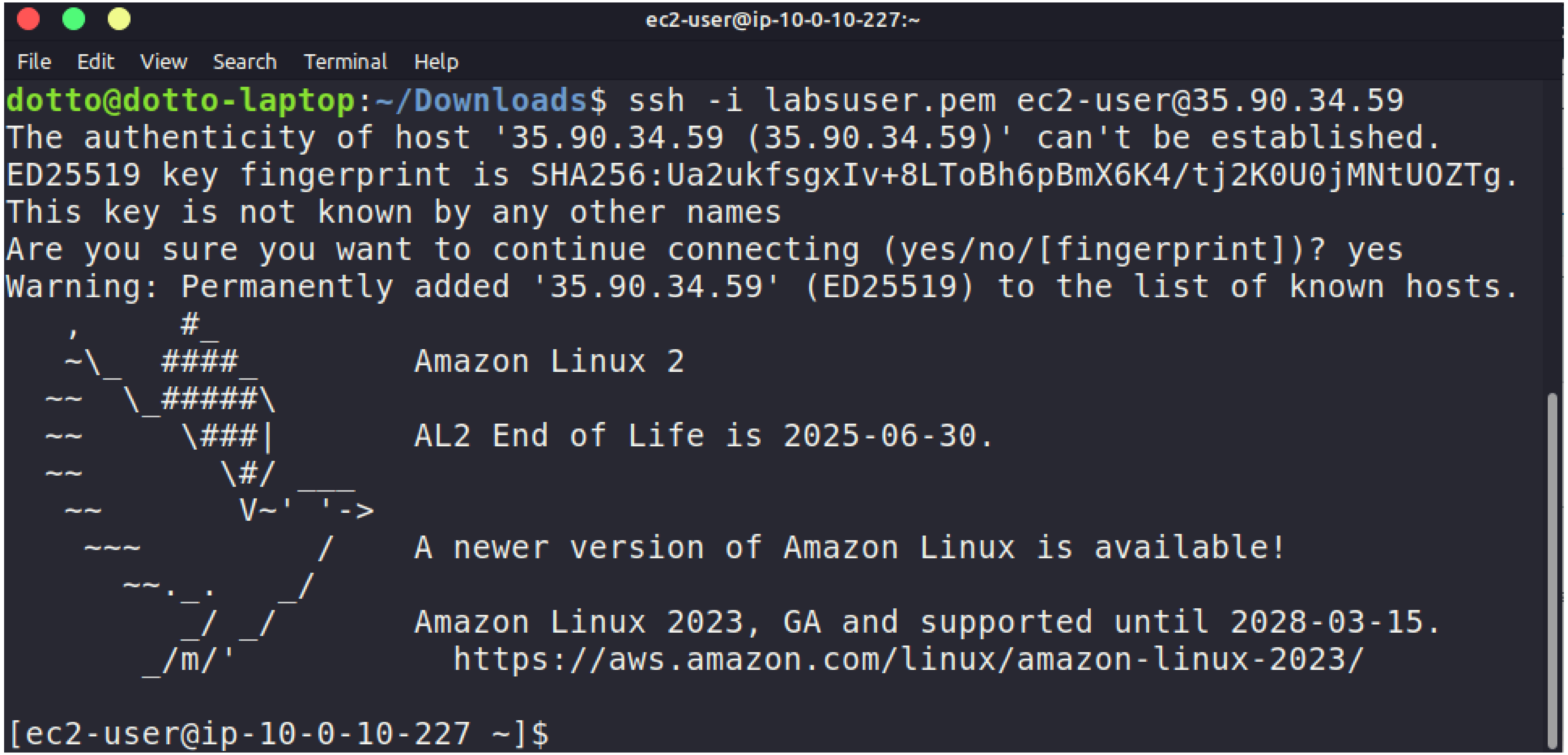
- Analizar los registros de seguridad y de logeo.

Tarea 1: Conectarse a la instancia utilizando SSH.

- Esperaremos a que la instancia esté cargada y nos conectaremos a la misma utilizando SSH.

- En Windows: usaremos PuTTY
- En Linux: con el comando ssh

Conexión con la instancia


ec2-user@ip-10-0-10-227:~
File Edit View Search Terminal Help

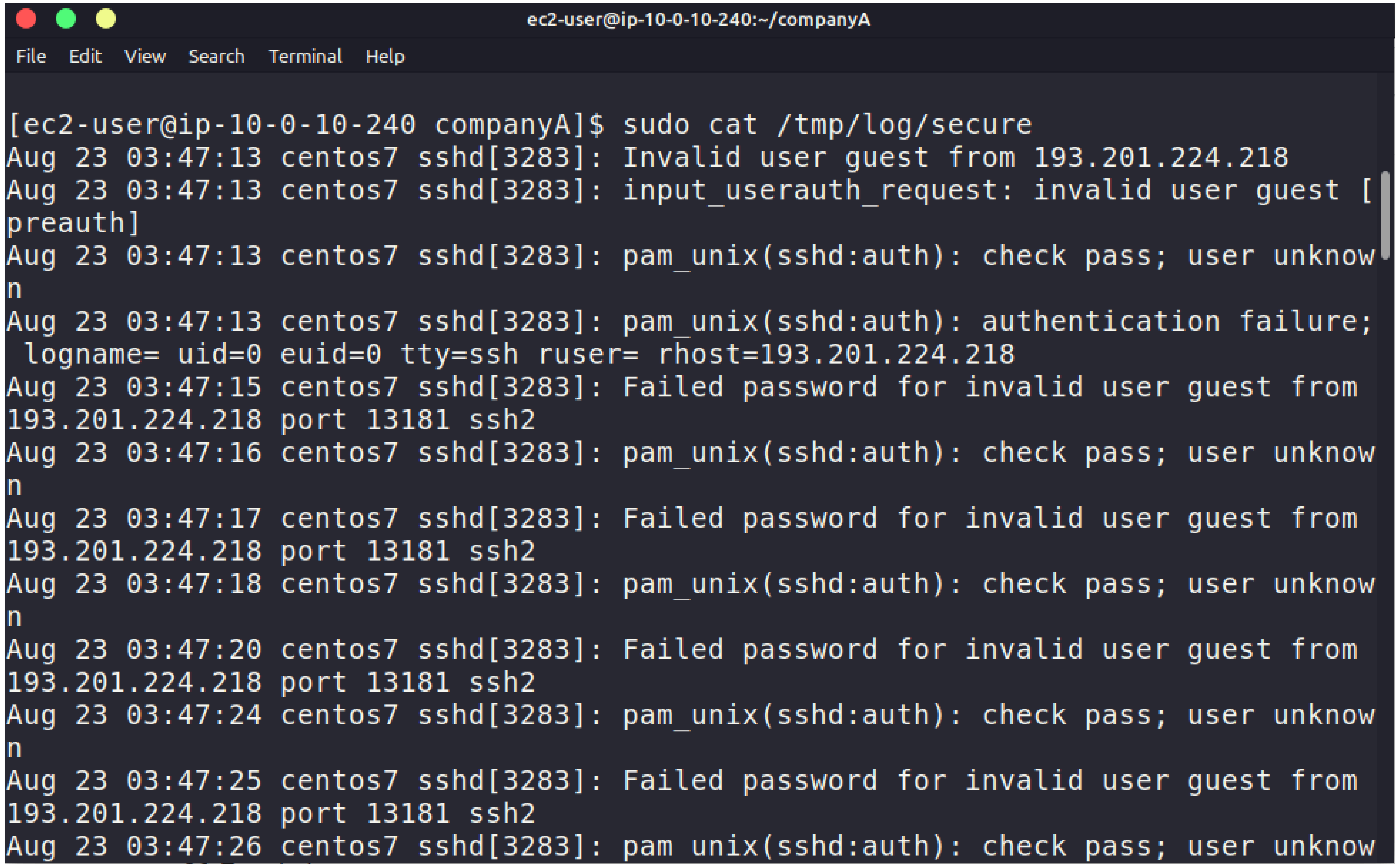
```
dotto@dotto-laptop:~/Downloads$ ssh -i labsuser.pem ec2-user@35.90.34.59
The authenticity of host '35.90.34.59 (35.90.34.59)' can't be established.
ED25519 key fingerprint is SHA256:Ua2ukfsgxIv+8LToBh6pBmX6K4/tj2K0U0jMNtUOZTg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '35.90.34.59' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-10-227 ~]$
```

Tarea 2: Analizar los archivos de registros.

- En esta tarea estaremos analizando dos archivos que guardan registros de seguridad y logeo.

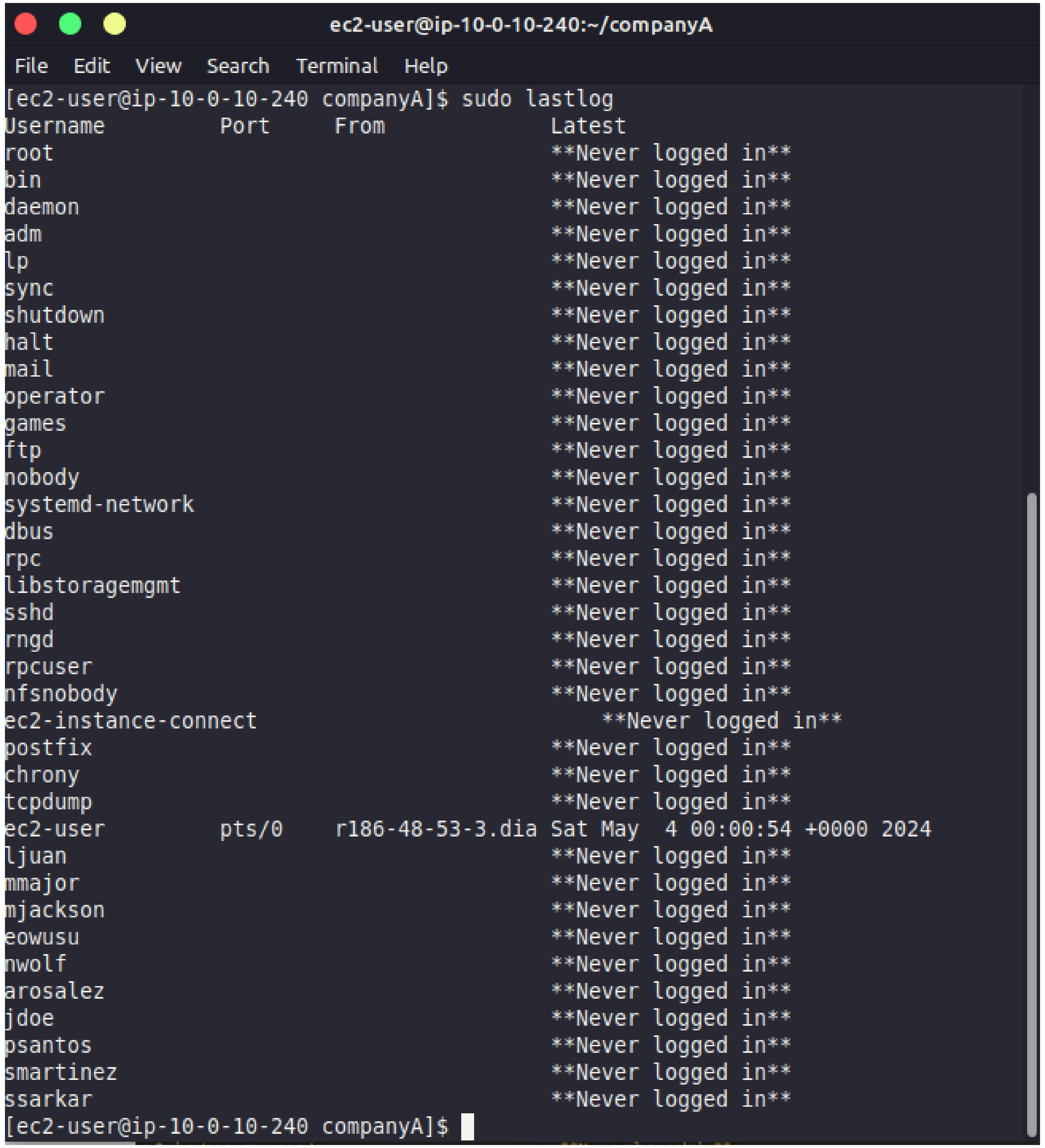
- seguridad: /var/secure/log
- logeo: sudo lastlog

Registro de seguridad


ec2-user@ip-10-0-10-240:~/companyA
File Edit View Search Terminal Help

```
[ec2-user@ip-10-0-10-240 companyA]$ sudo cat /tmp/log/secure
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218
Aug 23 03:47:13 centos7 sshd[3283]: input_userauth_request: invalid user guest [
preauth]
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow
n
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): authentication failure;
 logname= uid=0 euid=0 tty=ssh ruser= rhost=193.201.224.218
Aug 23 03:47:15 centos7 sshd[3283]: Failed password for invalid user guest from
193.201.224.218 port 13181 ssh2
Aug 23 03:47:16 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow
n
Aug 23 03:47:17 centos7 sshd[3283]: Failed password for invalid user guest from
193.201.224.218 port 13181 ssh2
Aug 23 03:47:18 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow
n
Aug 23 03:47:20 centos7 sshd[3283]: Failed password for invalid user guest from
193.201.224.218 port 13181 ssh2
Aug 23 03:47:24 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow
n
Aug 23 03:47:25 centos7 sshd[3283]: Failed password for invalid user guest from
193.201.224.218 port 13181 ssh2
Aug 23 03:47:26 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow
```

Registro de log



```
[ec2-user@ip-10-0-10-240 companyA]$ sudo lastlog
Username         Port     From             Latest
root                                       **Never logged in**
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
ftp                                        **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
dbus                                       **Never logged in**
rpc                                        **Never logged in**
libstoragemgmt                             **Never logged in**
sshd                                       **Never logged in**
rngd                                       **Never logged in**
rpcuser                                    **Never logged in**
nfsnobody                                  **Never logged in**
ec2-instance-connect                           **Never logged in**
postfix                                    **Never logged in**
chrony                                     **Never logged in**
tcpdump                                    **Never logged in**
ec2-user         pts/0    r186-48-53-3.dia Sat May  4 00:00:54 +0000 2024
ljuan                                      **Never logged in**
mmajor                                     **Never logged in**
mjackson                                   **Never logged in**
eowusu                                     **Never logged in**
nwolf                                      **Never logged in**
arosalez                                   **Never logged in**
jdoe                                       **Never logged in**
psantos                                    **Never logged in**
smartinez                                  **Never logged in**
ssarkar                                    **Never logged in**
[ec2-user@ip-10-0-10-240 companyA]$
```

Conclusiones

- Pude conocer los registros de seguridad y de logeo
- Comprendí que estos dos archivos guardan información muy importante que debería ser analizada frecuentemente.

¡Muchas gracias!

- Hecho por Ignacio Suárez. Realizado en canva.com