4. [HACKING SERVICIOS] - Matrix: Huellas en el Código

FASE 1 — Generación de identidades (crear usuarios)

Crear un usuario estándar

- sudo adduser trinity

```
ub@ub:~$ sudo adduser trinity
[sudo] contraseña para ub:
info: Añadiendo el usuario `trinity' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo `trinity' (1002) ...
info: Adding new user `trinity' (1002) with group `trinity (1002)' ...
info: Creando el directorio personal `/home/trinity' ...
info: Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para trinity
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: trinity
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
info: Adding new user `trinity' to supplemental / extra groups `users' ...
info: Añadiendo al usuario `trinity' al grupo `users' ...
```

- sudo adduser apoc

```
ub@ub:~$ sudo adduser apoc
info: Añadiendo el usuario `apoc' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo `apoc' (1003) ...
info: Adding new user `apoc' (1003) with group `apoc (1003)' ...
info: Creando el directorio personal `/home/apoc' ...
info: Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para apoc
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: apoc
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
info: Adding new user `apoc' to supplemental / extra groups `users' ...
info: Añadiendo al usuario `apoc' al grupo `users' ...
```

- sudo adduser switch

```
ub@ub:~$ sudo adduser switch
info: Añadiendo el usuario `switch' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo `switch' (1004) ...
info: Adding new user `switch' (1004) with group `switch (1004)' ...
info: Creando el directorio personal `/home/switch' ...
info: Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para switch
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: switch
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
info: Adding new user `switch' to supplemental / extra groups `users' ...
info: Añadiendo al usuario `switch' al grupo `users' ...
```

Crear neo (sudo)

- sudo adduser neo

```
ub@ub:~$ sudo adduser neo
info: Añadiendo el usuario `neo' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo `neo' (1005) ...
info: Adding new user `neo' (1005) with group `neo (1005)' ...
info: Creando el directorio personal `/home/neo' ...
info: Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para neo
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: neo
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
info: Adding new user `neo' to supplemental / extra groups `users' ...
info: Añadiendo al usuario `neo' al grupo `users' ...
```

Añadir neo al grupo sudo

- sudo usermod -aG sudo neo

```
ub@ub:~$ sudo usermod -aG sudo neo
```

Verificación

- groups neo

```
ub@ub:~$ groups neo
neo : neo sudo users
```

FASE 2 — Crear grupos: Escuadrones de la Resistencia

Crear grupo

- sudo groupadd zion

```
ub@ub:~$ sudo groupadd zion
```

- sudo groupadd matrix

```
ub@ub:~$ sudo groupadd matrix
```

Asignar usuarios a grupos

- sudo usermod -aG zion neo
- sudo usermod -aG zion trinity
- sudo usermod -aG matrix neo
- sudo usermod -aG matrix apoc
- sudo usermod -aG matrix switch

```
ub@ub:~$ sudo usermod -aG zion neo
ub@ub:~$ sudo usermod -aG zion trinity
ub@ub:~$ sudo usermod -aG matrix neo
ub@ub:~$ sudo usermod -aG matrix apoc
ub@ub:~$ sudo usermod -aG matrix switch
```

Verificación

- groups（user name）

```
ub@ub:~$ groups neo
neo : neo sudo users zion matrix
ub@ub:~$ groups trinity
trinity : trinity users zion
ub@ub:~$ groups apoc
apoc : apoc users matrix
ub@ub:~$ groups switch
switch : switch users matrix
```

FASE 3 — Estructura de directorios: Los Distritos de Matrix

Crear directorio

- sudo mkdir /mission-data
- sudo mkdir /simulacion
- sudo mkdir /backdoor

```
ub@ub:~$ sudo mkdir /mission-data
ub@ub:~$ sudo mkdir /simulacion
ub@ub:~$ sudo mkdir /backdoor
```

Carpeta dedicada de Zion : /mission-data

- sudo chown :zion /mission-data
- sudo chmod 770 /mission-data

```
ub@ub:~$ sudo chown :zion /mission-data
ub@ub:~$ sudo chmod 770 /mission-data
```

Carpeta dominada por matrices : /simulacion

- sudo chown :matrix /simulacion
- sudo chmod 775 /simulacion

```
ub@ub:~$ sudo chown :matrix /simulacion
ub@ub:~$ sudo chmod 775 /simulacion
```

Carpeta exclusiva de neo : /backdoor

- sudo chown neo:neo /backdoor
- sudo chmod 700 /backdoor

```
ub@ub:~$ sudo chown neo:neo /backdoor
ub@ub:~$ sudo chmod 700 /backdoor
```

FASE 4 — Pruebas de acceso: El Oráculo y los obstáculos

Verificación

```
ub@ub:~$ ls -ld /mission-data /simulacion /backdoor
drwx------ 2 neo  neo    4096 dic 19 16:36 /backdoor
drwxrwx--- 2 root zion   4096 dic 19 16:36 /mission-data
drwxrwxr-x 2 root matrix 4096 dic 19 16:36 /simulacion
```

trinity :

```
ub@ub:~$ su - trinity
Contraseña:
trinity@ub:~$ touch /mission-data/test.txt
```

```
trinity@ub:~$ cd /backdoor
-bash: cd: /backdoor: Permiso denegado
```

```
trinity@ub:~$ cd /simulacion
trinity@ub:/simulacion$ touch test1.txt
touch: no se puede efectuar `touch' sobre 'test1.txt': Permiso denegado
trinity@ub:/simulacion$ ll
total 8
drwxrwxr-x  2 root matrix 4096 dic 19 16:36 ./
drwxr-xr-x 26 root root   4096 dic 19 16:36 ../
```

```
trinity@ub:~$ id
uid=1002(trinity) gid=1002(trinity) grupos=1002(trinity),100(users),1006(zion)
trinity@ub:~$ groups
trinity users zion
```

```
trinity@ub:~$ touch /mission-data/test-trinity.txt
trinity@ub:~$ mkdir /mission-data/trinity
trinity@ub:~$ ls /mission-data
test-trinity.txt  test.txt  trinity
```

apoc:

```
ub@ub:~$ su - apoc
Contraseña:
apoc@ub:~$ touch /mission-data/test1.txt
touch: no se puede efectuar `touch' sobre '/mission-data/test1.txt': Permiso denegado
apoc@ub:~$ ls /backdoor
ls: no se puede abrir el directorio '/backdoor': Permiso denegado
apoc@ub:~$ touch /simulacion/test.txt
```

```
apoc@ub:~$ id
uid=1003(apoc) gid=1003(apoc) grupos=1003(apoc),100(users),1007(matrix)
```

```
apoc@ub:~$ cd /simulacion
apoc@ub:/simulacion$ ll
total 8
drwxrwxr-x  2 root matrix 4096 dic 19 16:57 ./
drwxr-xr-x 26 root root   4096 dic 19 16:36 ../
-rw-rw-r--  1 apoc apoc      0 dic 19 16:57 test.txt
apoc@ub:/simulacion$ mkdir apoc
apoc@ub:/simulacion$ ll
total 12
drwxrwxr-x  3 root matrix 4096 dic 19 16:59 ./
drwxr-xr-x 26 root root   4096 dic 19 16:36 ../
drwxrwxr-x  2 apoc apoc   4096 dic 19 16:59 apoc/
-rw-rw-r--  1 apoc apoc      0 dic 19 16:57 test.txt
```

```
apoc@ub:/simulacion$ ls
apoc  test.txt
apoc@ub:/simulacion$ groups
apoc users matrix
```

```
apoc@ub:~$ ls /mission-data
ls: no se puede abrir el directorio '/mission-data': Permiso denegado
apoc@ub:~$ ls /backdoor
ls: no se puede abrir el directorio '/backdoor': Permiso denegado
```

switch:

```
ub@ub:~$ su - switch
Contraseña:
switch@ub:~$ id
uid=1004(switch) gid=1004(switch) grupos=1004(switch),100(users),1007(matrix)
switch@ub:~$ groups
switch users matrix
switch@ub:~$  ls /backdoor
ls: no se puede abrir el directorio '/backdoor': Permiso denegado
switch@ub:~$ ls /mission-data
ls: no se puede abrir el directorio '/mission-data': Permiso denegado
switch@ub:~$ ls /simulacion
apoc  test.txt
switch@ub:~$ touch /simulacion/test-switch.txt
switch@ub:~$ mkdir /simulacion/switch
switch@ub:~$ ls /simulacion
apoc  switch  test-switch.txt  test.txt
```

neo:

```
ub@ub:~$ su - neo
Contraseña:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
neo@ub:~$ id
uid=1005(neo) gid=1005(neo) grupos=1005(neo),27(sudo),100(users),1006(zion),1007(matrix)
neo@ub:~$ groups
neo sudo users zion matrix
```

```
neo@ub:~$ touch /mission-data/test-neo.txt
neo@ub:~$ touch /simulacion/test-neo.txt
neo@ub:~$ mkdir /simulacion/neo
neo@ub:~$ mkdir /mission-data/neo
```

```
neo@ub:~$ ls /simulacion
apoc  neo  switch  test-neo.txt  test-switch.txt  test.txt
neo@ub:~$ ls /mission-data
neo  test-neo.txt  test-trinity.txt  test.txt  trinity
```

```
neo@ub:~$ touch /backdoor/test-neo.txt
neo@ub:~$ mkdir /backdoor/neo
neo@ub:~$ ls /backdoor
neo  test-neo.txt
```

FASE 5 — Mini misión final: Neutralizar al Agente Smith

Crear smith

- sudo adduser smith

```
ub@ub:~$ sudo adduser smith
[sudo] contraseña para ub:
info: Añadiendo el usuario `smith' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo `smith' (1008) ...
info: Adding new user `smith' (1008) with group `smith (1008)' ...
info: Creando el directorio personal `/home/smith' ...
info: Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para smith
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: smith
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n]
info: Adding new user `smith' to supplemental / extra groups `users' ...
info: Añadiendo al usuario `smith' al grupo `users' ...
```

Bloquear el directorio de inicio

- sudo chmod 700 /home/smith

```
ub@ub:~$ sudo chmod 700 /home/smith
```

Verificación

```
ub@ub:~$ su - smith
Contraseña:
smith@ub:~$ ls /backdoor
ls: no se puede abrir el directorio '/backdoor': Permiso denegado
smith@ub:~$ ls /mission-data
ls: no se puede abrir el directorio '/mission-data': Permiso denegado
```

Smith no pertenece a ningún grupo, los permisos del directorio niegan el acceso a otros y, por lo tanto, está completamente aislado.

FASE 6 — La lluvia de código (logs en tiempo real)

Supervisión de los registros del sistema

- sudo journalctl -f

```
ub@ub:~$ sudo journalctl -f
dic 19 17:26:01 ub sudo[26077]: pam_unix(sudo:session): session opened for user root(uid=0) by ub(uid=1000)
dic 19 17:26:01 ub sudo[26077]: pam_unix(sudo:session): session closed for user root
dic 19 17:26:50 ub su[26081]: (to smith) ub on pts/1
dic 19 17:26:50 ub su[26081]: pam_unix(su-l:session): session opened for user smith(uid=1008) by ub(uid=1000)
dic 19 17:27:31 ub su[26081]: pam_unix(su-l:session): session closed for user smith
dic 19 17:27:38 ub su[26099]: (to smith) ub on pts/1
dic 19 17:27:38 ub su[26099]: pam_unix(su-l:session): session opened for user smith(uid=1008) by ub(uid=1000)
dic 19 17:28:56 ub su[26099]: pam_unix(su-l:session): session closed for user smith
dic 19 17:28:58 ub sudo[26116]:       ub : TTY=pts/1 ; PWD=/home/ub ; USER=root ; COMMAND=/usr/bin/journalctl -f
dic 19 17:28:58 ub sudo[26116]: pam_unix(sudo:session): session opened for user root(uid=0) by ub(uid=1000)
```

FASE 7 — El rastro de entrada y salida

Usuarios actuales en línea

- who

```
ub@ub:~$ who
ub         seat0        2025-12-19 14:40 (login screen)
ub         tty2         2025-12-19 14:40 (tty2)
ub         pts/1        2025-12-19 14:42 (192.168.118.1)
```

Inicios de sesión históricos

- last

```
ub@ub:~$ last
ub       pts/1        192.168.118.1    Fri Dec 19 14:42   still logged in
ub       tty2         tty2             Fri Dec 19 14:40   still logged in
ub       seat0        login screen     Fri Dec 19 14:40   still logged in
reboot   system boot  6.14.0-37-generi Fri Dec 19 14:39   still running
ub       pts/1        192.168.118.1    Tue Dec 16 09:38 - 14:13  (04:35)
ub       tty2         tty2             Tue Dec 16 09:37 - down   (04:36)
ub       seat0        login screen     Tue Dec 16 09:37 - down   (04:36)
reboot   system boot  6.14.0-37-generi Tue Dec 16 09:36 - 14:14  (04:37)
ub       pts/1        192.168.118.1    Mon Dec 15 11:28 - 13:06  (01:37)
ub       tty2         tty2             Mon Dec 15 11:26 - down   (01:41)
ub       seat0        login screen     Mon Dec 15 11:26 - down   (01:41)
reboot   system boot  6.14.0-37-generi Mon Dec 15 11:26 - 13:08  (01:42)
ub       pts/1        192.168.118.1    Mon Dec 15 08:45 - 09:30  (00:45)
ub       tty2         tty2             Mon Dec 15 08:44 - down   (00:46)
```

Intentos fallidos de inicio de sesión

- sudo zgrep -i "failed" /var/log/auth.log*

```
ub@ub:~$ sudo zgrep -i "failed" /var/log/auth.log*
/var/log/auth.log:2025-12-15T09:00:36.261678+01:00 ub dbus-daemon[1335]: [system] Failed to activate service 'org.bluez': ti
med out (service_start_timeout=25000ms)
/var/log/auth.log:2025-12-15T11:39:38.090403+01:00 ub gdm-password]: pam_unix(gdm-password:auth): conversation failed
/var/log/auth.log:2025-12-15T11:49:15.095856+01:00 ub gdm-password]: pam_unix(gdm-password:auth): conversation failed
/var/log/auth.log:2025-12-15T12:00:42.167786+01:00 ub dbus-daemon[1275]: [system] Failed to activate service 'org.bluez': ti
med out (service_start_timeout=25000ms)
/var/log/auth.log:2025-12-16T09:47:37.587827+01:00 ub dbus-daemon[1315]: [system] Failed to activate service 'org.bluez': ti
med out (service_start_timeout=25000ms)
/var/log/auth.log:2025-12-19T15:00:48.473903+01:00 ub dbus-daemon[1429]: [system] Failed to activate service 'org.bluez': ti
med out (service_start_timeout=25000ms)
/var/log/auth.log:2025-12-19T17:31:17.957097+01:00 ub sudo:       ub : TTY=pts/1 ; PWD=/home/ub ; USER=root ; COMMAND=/usr/b
in/zgrep -i failed /var/log/auth.log /var/log/auth.log.1 /var/log/auth.log.2.gz /var/log/auth.log.3.gz /var/log/auth.log.4.g
z
/var/log/auth.log.1:2025-12-07T00:01:00.169240+01:00 ub dbus-daemon[1430]: [system] Failed to activate service 'org.bluez':
timed out (service_start_timeout=25000ms)
/var/log/auth.log.1:2025-12-07T00:25:41.831420+01:00 ub sshd[8766]: Failed password for ub from 192.168.118.1 port 25104 ssh
2
/var/log/auth.log.1:2025-12-12T12:01:09.245175+01:00 ub dbus-daemon[1169]: [system] Failed to activate service 'org.bluez':
timed out (service_start_timeout=25000ms)
/var/log/auth.log.3.gz:2025-11-20T21:09:35.049422+01:00 ub dbus-daemon[1434]: [system] Failed to activate service 'org.bluez
': timed out (service_start_timeout=25000ms)
/var/log/auth.log.3.gz:2025-11-21T16:14:26.291496+01:00 ub dbus-daemon[1433]: [system] Failed to activate service 'org.bluez
': timed out (service_start_timeout=25000ms)
/var/log/auth.log.4.gz:2025-10-26T00:58:05.244433+02:00 ub dbus-daemon[1431]: [system] Failed to activate service 'org.bluez
': timed out (service_start_timeout=25000ms)
```

¿Trinity accedió ayer?
NO
¿Apoc intentó entrar varias veces y falló?
NO
¿Neo ha usado sudo recientemente?
SI
¿Smith existe en los logs aunque no debería moverse por el sistema?
NO

FASE 8 — Sudo: quién ha manipulado Matrix
Ver el historial de uso de sudo

- sudo journalctl -u sudo
- sudo grep 'COMMAND=' /var/log/auth.log

Ver qué comandos se han ejecutado con sudo.

```
ub@ub:~$ sudo journalctl -u sudo
-- No entries --
ub@ub:~$ sudo grep 'COMMAND=' /var/log/auth.log
2025-12-15T08:45:33.335141+01:00 ub pkexec[4133]: ub: Executing command [USER=root] [TTY=unknown] [CWD=/home/ub] [COMMAND=/u
sr/lib/update-notifier/package-system-locked]
2025-12-15T08:49:18.711845+01:00 ub sudo:       ub : TTY=pts/1 ; PWD=/home/ub ; USER=root ; COMMAND=/usr/local/bin/docker-co
mpose ps
2025-12-15T08:49:37.789777+01:00 ub sudo:       ub : TTY=pts/1 ; PWD=/home/ub/red1 ; USER=root ; COMMAND=/usr/local/bin/dock
er-compose ps
2025-12-15T08:50:56.301221+01:00 ub sudo:       ub : TTY=pts/1 ; PWD=/home/ub/red1 ; USER=root ; COMMAND=/usr/local/bin/dock
er-compose up --build
2025-12-15T08:58:00.183062+01:00 ub sudo:       ub : TTY=pts/1 ; PWD=/home/ub/red1/firewall ; USER=root ; COMMAND=/usr/bin/n
ano firewall-rules.sh
```

Identificar el usuario que los ejecutó.

ub

Detectar intentos de sudo fallidos.

```
/var/log/auth.log.1:2025-12-12T12:01:09.245175+01:00 ub dbus-daemon[1169]: [system] Failed to activate service 'org.bluez':
timed out (service_start_timeout=25000ms)
/var/log/auth.log.3.gz:2025-11-20T21:09:35.049422+01:00 ub dbus-daemon[1434]: [system] Failed to activate service 'org.bluez
': timed out (service_start_timeout=25000ms)
/var/log/auth.log.3.gz:2025-11-21T16:14:26.291496+01:00 ub dbus-daemon[1433]: [system] Failed to activate service 'org.bluez
': timed out (service_start_timeout=25000ms)
/var/log/auth.log.4.gz:2025-10-26T00:58:05.244433+02:00 ub dbus-daemon[1431]: [system] Failed to activate service 'org.bluez
': timed out (service_start_timeout=25000ms)
```

FASE 9 — Huellas en el historial: El Código dejado atrás
Ver el historial de cada usuario

- su - trinity
- history

```
ub@ub:~$ su - trinity
Contraseña:
trinity@ub:~$ history
    1  touch /mission-data/test.txt
    2  cd simulacion
    3  cd /simulacion
    4  cd
    5  cd /backdoor
    6  exit
    7  cd simulacion
    8  cd /simulacion
    9  touch test1.txt
   10  ll
   11  exit
   12  id
   13  groups
   14  ls mission-data
   15  ls /mission-data
   16  touch /mission-data/test-trinity.txt
   17  mkdir /mission-data/trinity
   18  ls /mission-data
   19  exit
   20  history
```

o ver el archivo directamente

- cat /home/trinity/.bash_history

```
trinity@ub:~$ cat /home/trinity/.bash_history
touch /mission-data/test.txt
cd simulacion
cd /simulacion
cd
cd /backdoor
exit
cd simulacion
cd /simulacion
touch test1.txt
ll
exit
id
groups
ls mission-data
ls /mission-data
touch /mission-data/test-trinity.txt
mkdir /mission-data/trinity
ls /mission-data
exit
```

¿Quién creó un archivo dentro de /simulacion fuera de su hora de trabajo?
El usuario trinity

¿Quién intentó entrar a /backdoor aunque no tenía permisos?
El usuario trinity

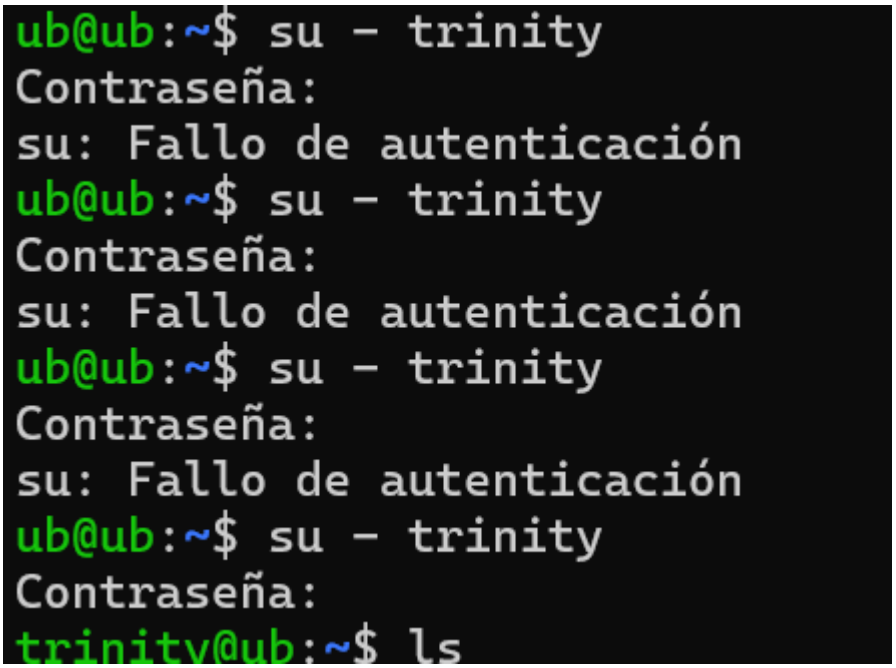
¿Qué usuario ejecutó comandos sospechosos como ? sudo su
No se encontró ningún usuario que haya ejecutado “sudo su”.

¿Acaso Smith intentó copiar algo desde mission-data?
Nada

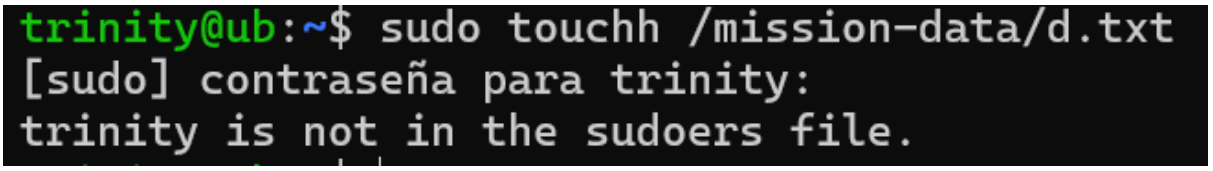
FASE 10 — Localizar la intrusión: reconstrucción forense

Operación (escenarios de fabricación)

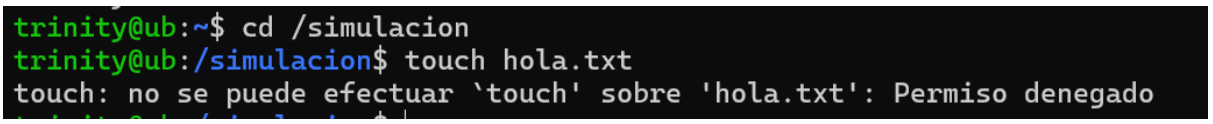
Introduzca una contraseña incorrecta tres veces consecutivas.



Falla la ejecución de sudo.



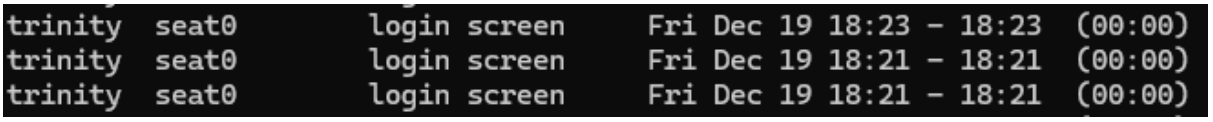
Acceda a /simulacion fuera del plazo permitido.



Procedimiento de recogida de pruebas

- sudo grep 'COMMAND=' /var/log/auth.log

- sudo lastb



Usuario: trinity
Hora: 19 de diciembre de 2025, 18:21
Evento: 3 intentos fallidos de inicio de sesión
Explicación técnica: contraseña incorrecta
Evento: error en la escalada de privilegios de sudo
Motivo: no pertenece al grupo sudo
Fuente del registro: /var/log/auth.log