

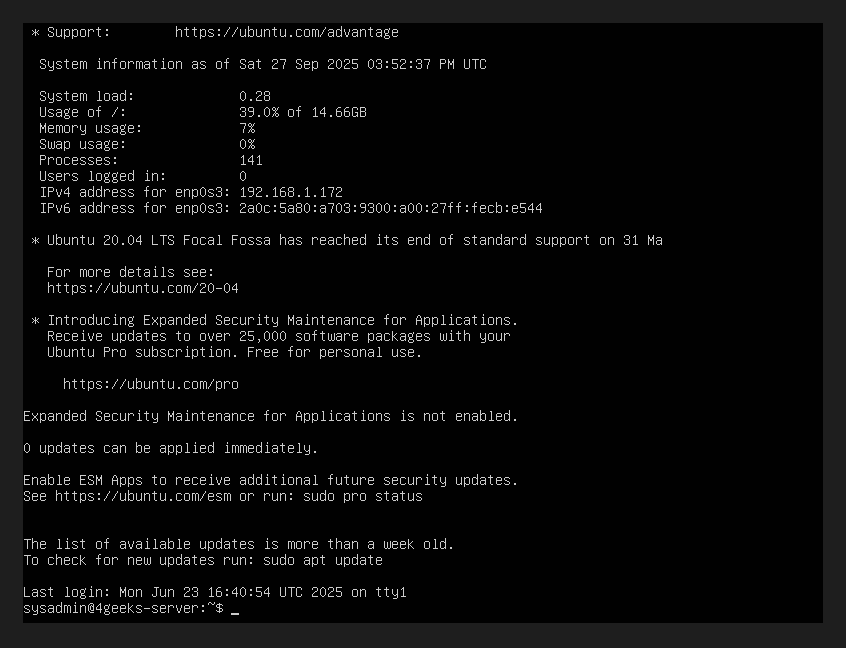
# Introducción

Este informe documenta un ejercicio de Live Incident Response sobre un servidor Linux comprometido. El objetivo fue identificar la intrusión, contenerla en vivo sin apagar el sistema, erradicar la persistencia y dejar el sistema endurecido. Se incluyen evidencias con capturas y explicaciones breves de los comandos usados.

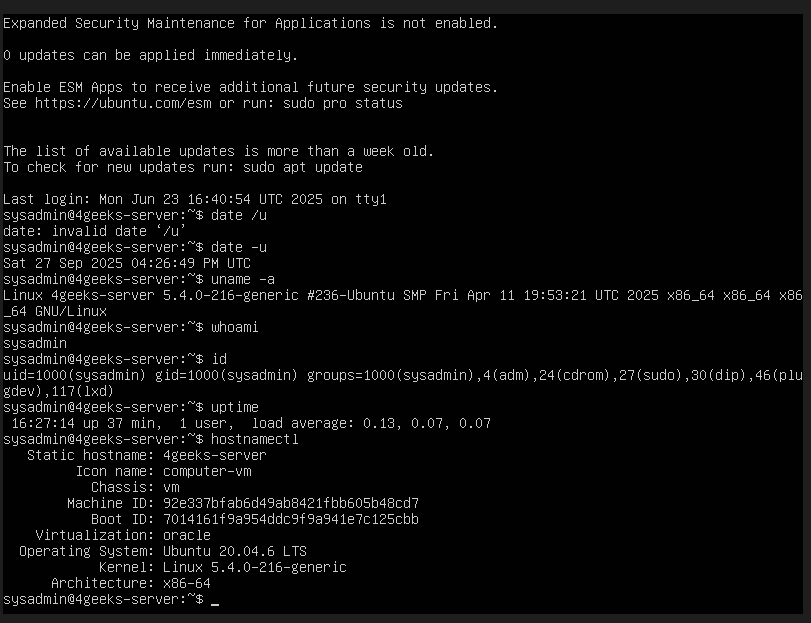
# Fase 1 – Detección y Análisis (Live)

Se recopiló evidencia de accesos, usuarios, servicios y artefactos maliciosos.

Contexto del sistema (banner y huella inicial).

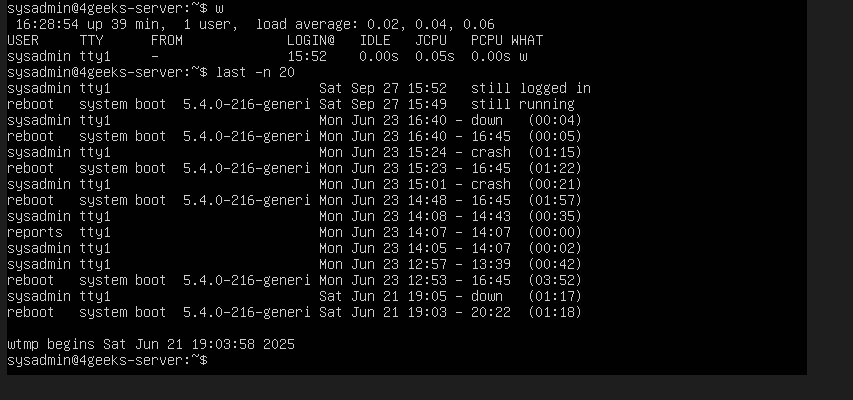


*Figura 1. Pantalla inicial de la VM y banner del sistema (Ubuntu 20.04).*

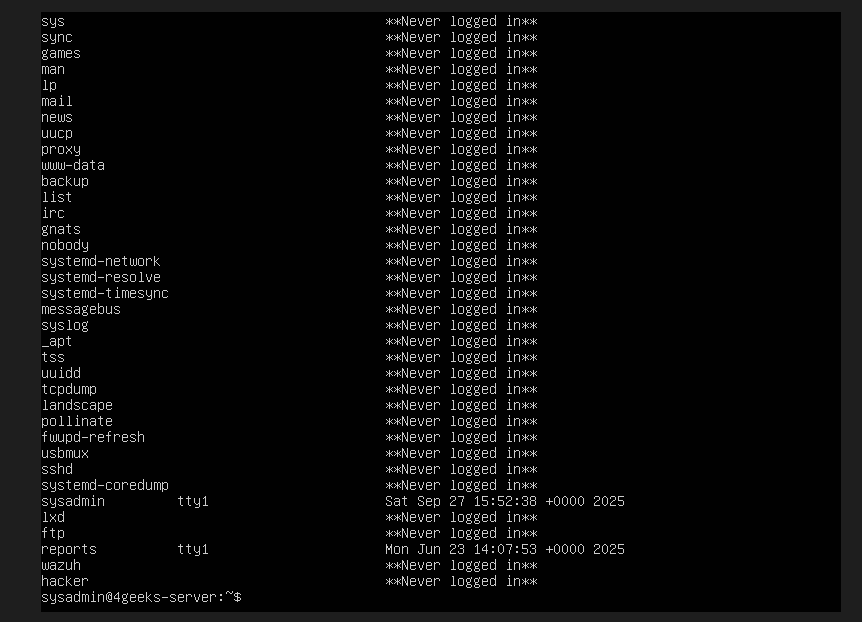


*Figura 2. Huella básica: fecha UTC, kernel, usuario, uptime y hostname.*

Autenticación: accesos válidos y fuerza bruta detectada en SSH.



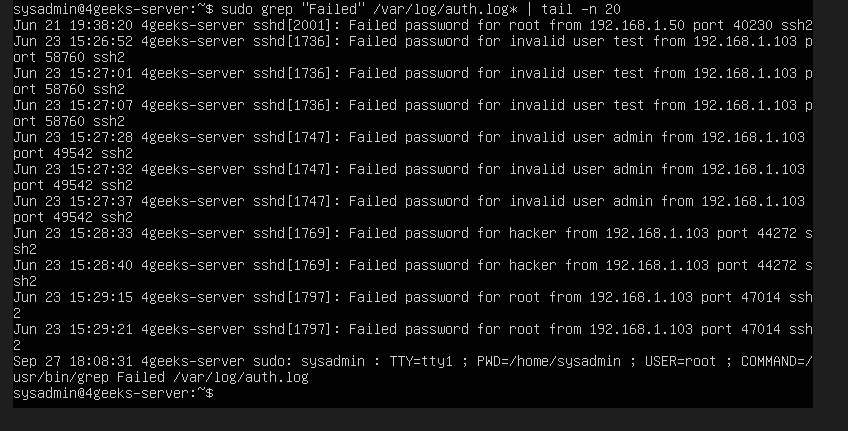
*Figura 3. Sesiones recientes con 'last' (usuarios sysadmin/reports).*



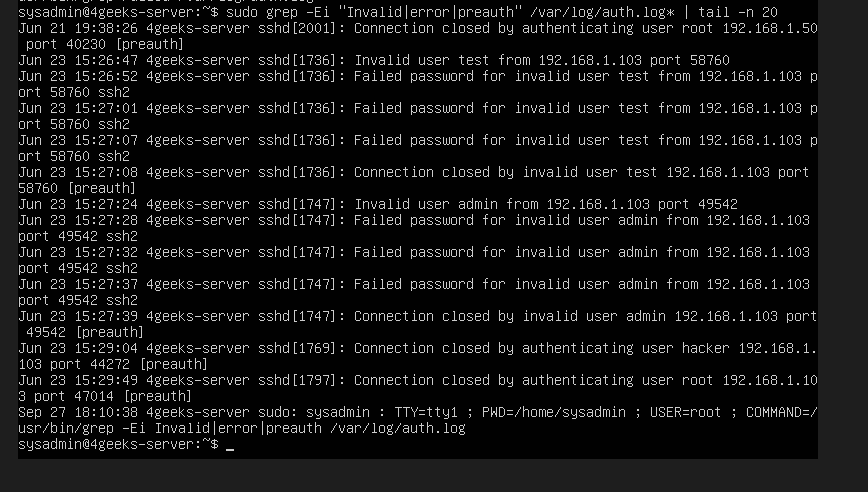
*Figura 4. Tabla de 'lastlog' mostrando usuarios y últimos accesos.*



*Figura 5. SSH logins aceptados (Accepted) — acceso exitoso desde 192.168.1.50.*



*Figura 6. Intentos de acceso fallidos (Failed).*



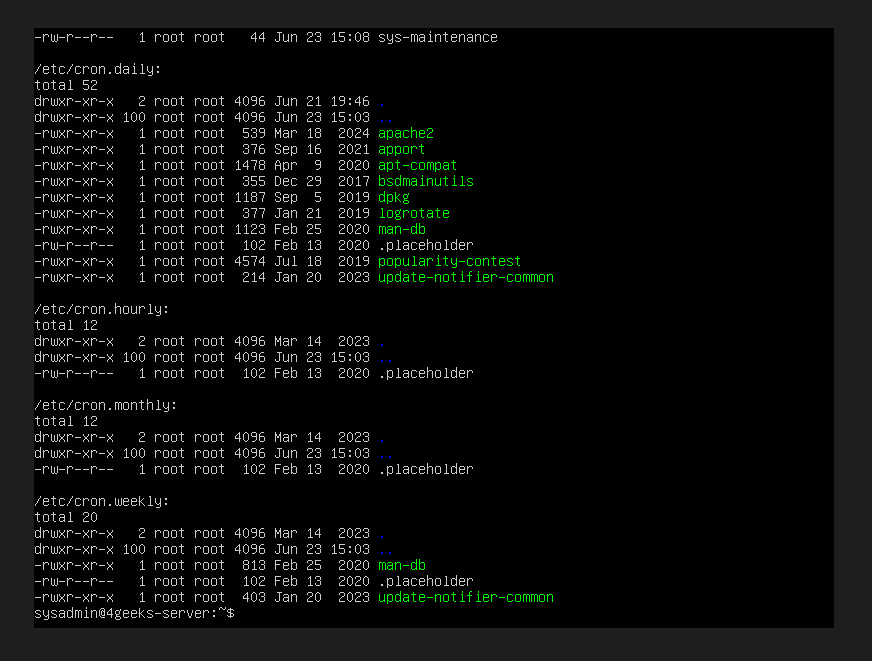
*Figura 7. Eventos sospechosos (Invalid user / preauth) desde 192.168.1.103.*

Usuarios creados por el atacante (persistencia).



*Figura 8. Detalle de usuarios locales 'reports' y 'hacker' (getent/id).*

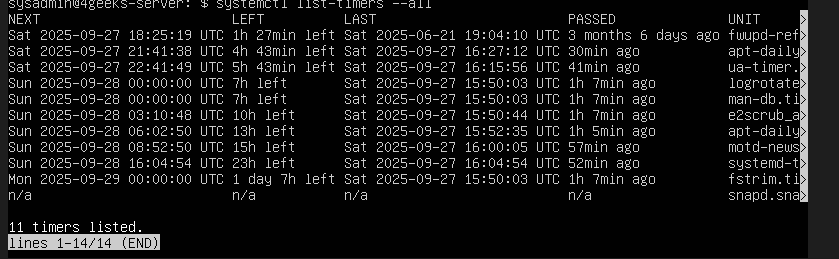
Persistencia: cron y servicios.



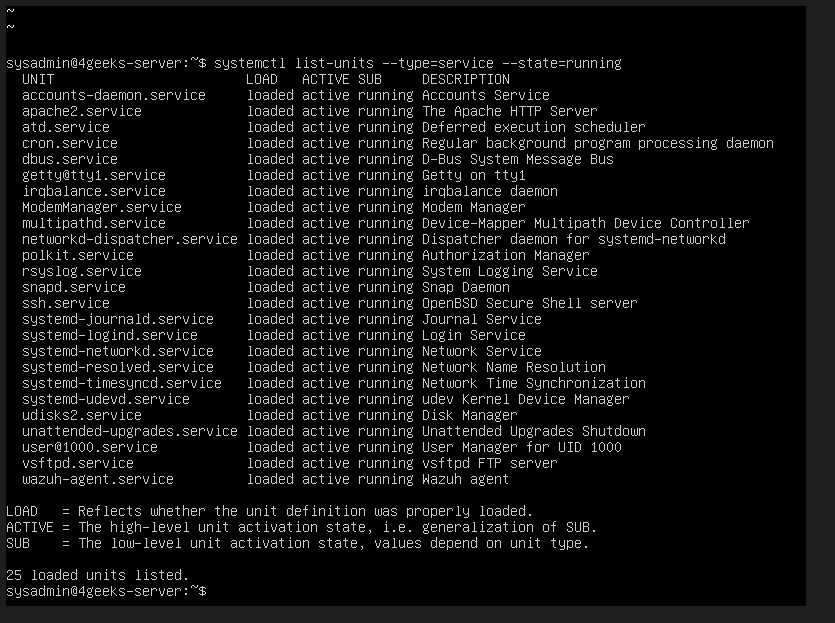
*Figura 9. Listados de /etc/cron.\* (búsqueda de cronjobs).*



*Figura 10. Revisión de /var/spool/cron/crontabs (sin crontabs de usuario).*



*Figura 11. Timers de systemd (sin anomalías).*

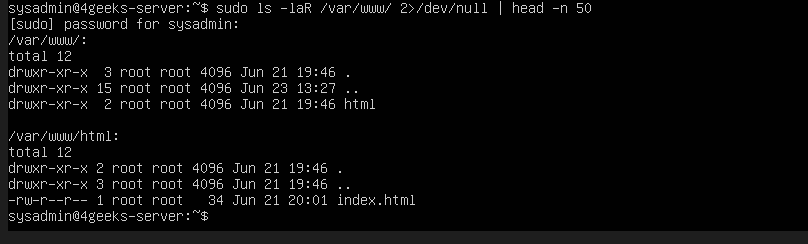


*Figura 12. Servicios systemd activos (vsftpd y wazuh-agent presentes).*

Superficie expuesta en red.



*Figura 13. Puertos abiertos con ss -tulpna (21/22/80/53).*

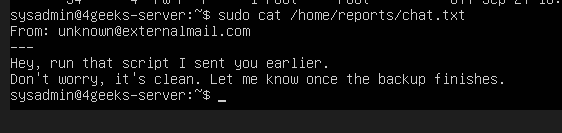


*Figura 14. Directorio web /var/www/html (sin webshells).*

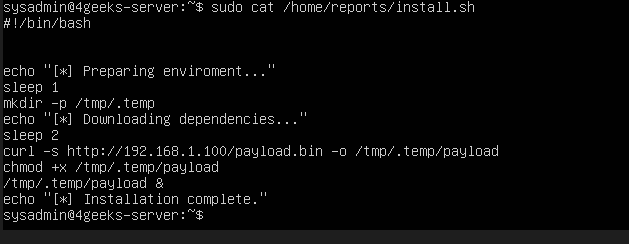
Artefactos identificados en /home y /tmp.



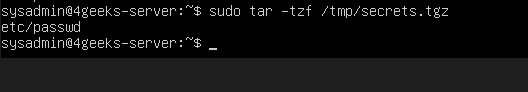
*Figura 15. Listado de archivos sospechosos en /home/reports y /tmp.*



*Figura 16. Contenido de chat.txt con instrucciones del atacante.*



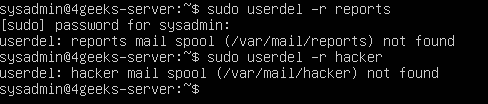
*Figura 17. Contenido de install.sh descargando payload desde 192.168.1.100.*



*Figura 18. Contenido de secrets.tgz: incluye etc/passwd.*

# Fase 2 – Contención y Erradicación

Se erradicaron cuentas, cronjobs, payloads y servicios no autorizados; se aseguró la evidencia.



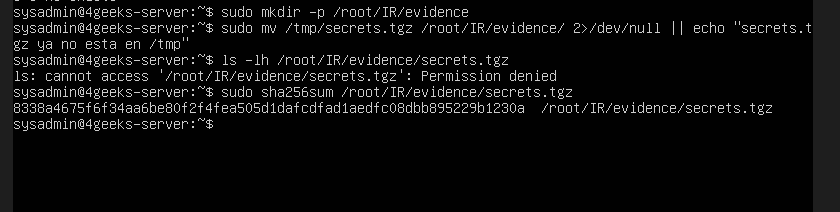
*Figura 19. Eliminación de usuarios maliciosos 'reports' y 'hacker'.*



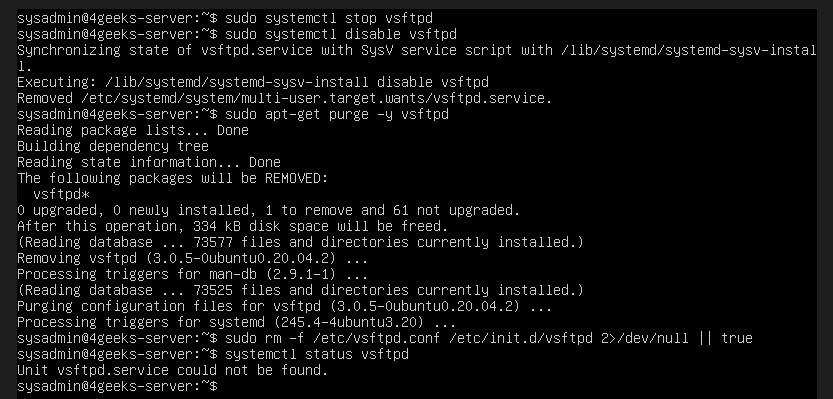
*Figura 20. Cron sospechoso removido y cron reiniciado.*



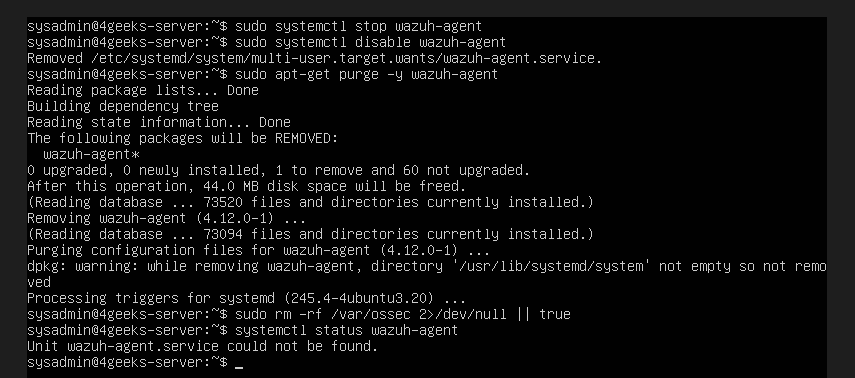
*Figura 21. Finalización del payload en /tmp y limpieza de /tmp/.temp.*



*Figura 22. Custodia de secrets.tgz y cálculo de hash SHA256 (nota: 'Permission denied' al listar /root es esperado sin sudo).*



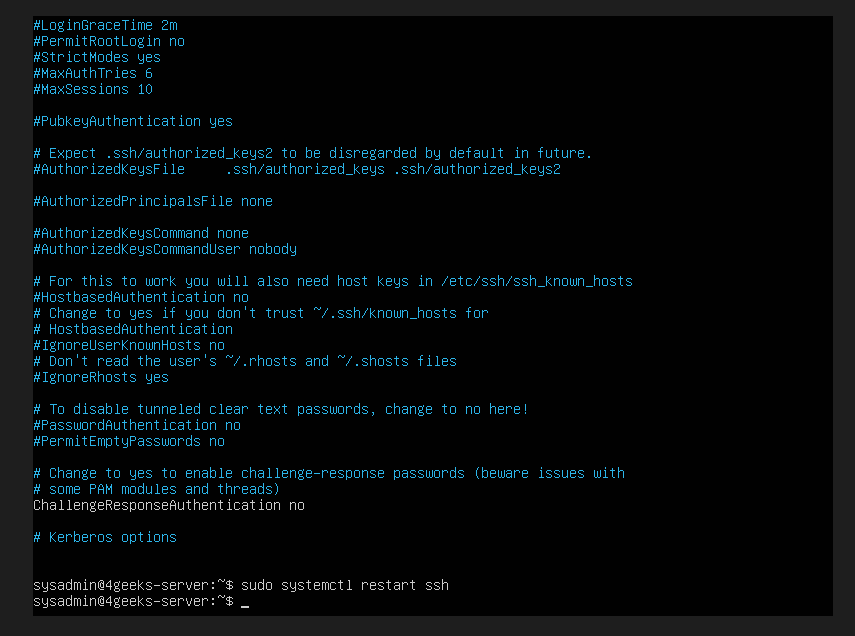
*Figura 23. vsftpd eliminado (Unit not found).*



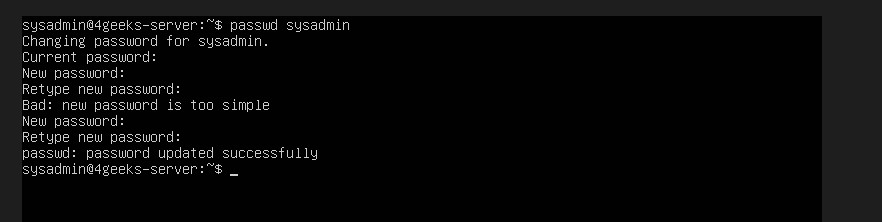
*Figura 24. wazuh-agent eliminado (Unit not found).*



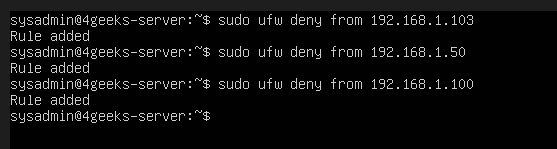
*Figura 25. Verificación: puertos limpios tras erradicación (sin 21/FTP).*



*Figura 26. Endurecimiento de SSH en /etc/ssh/sshd\_config.*



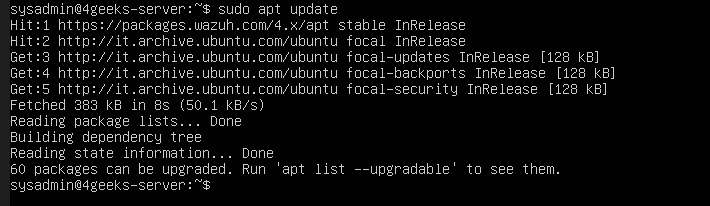
*Figura 27. Cambio de contraseña del usuario sysadmin.*



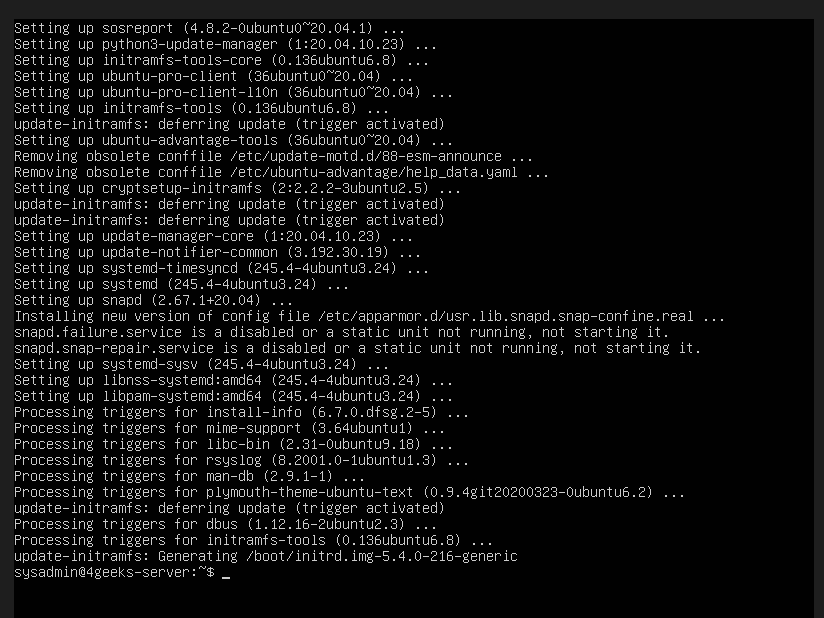
*Figura 28. Bloqueo de IPs atacante con UFW.*

# Fase 3 – Remediación y Hardening

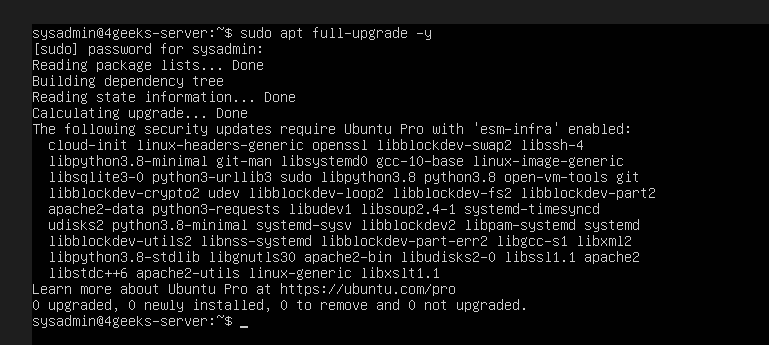
Se aplicaron parches, configuró firewall mínimo y se añadió protección anti-fuerza bruta.



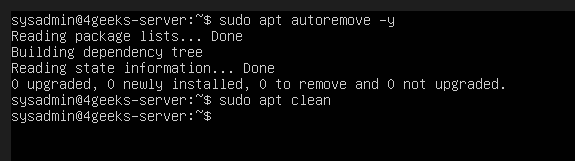
*Figura 29. apt update – índices de paquetes actualizados.*



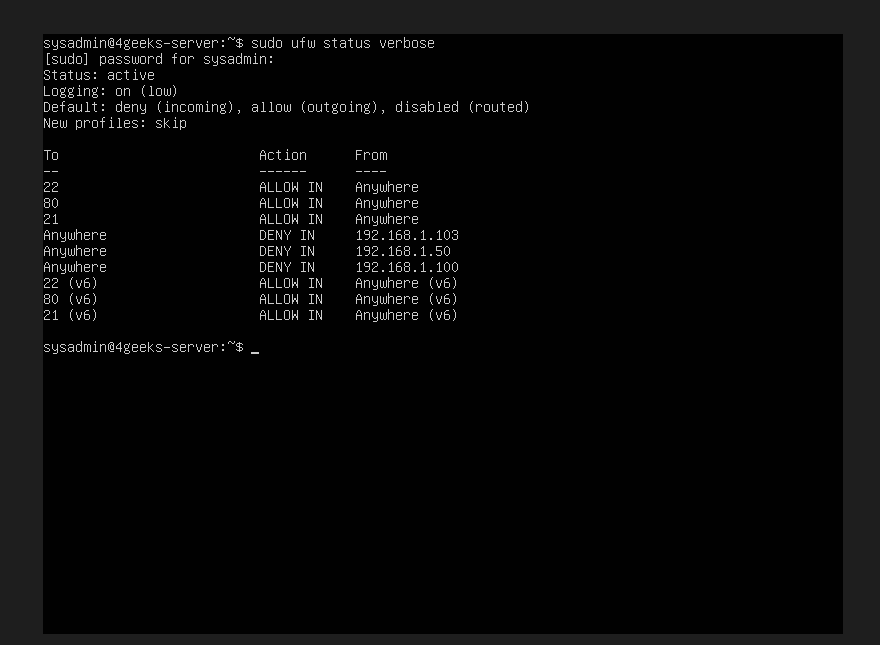
*Figura 30. apt upgrade – paquetes actualizados.*



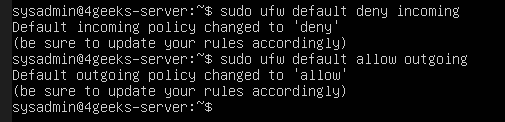
*Figura 31. apt full-upgrade – actualización completa (algunos parches requieren ESM).*



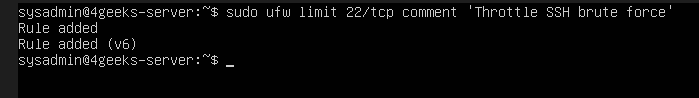
*Figura 32. Limpieza: apt autoremove / apt clean.*



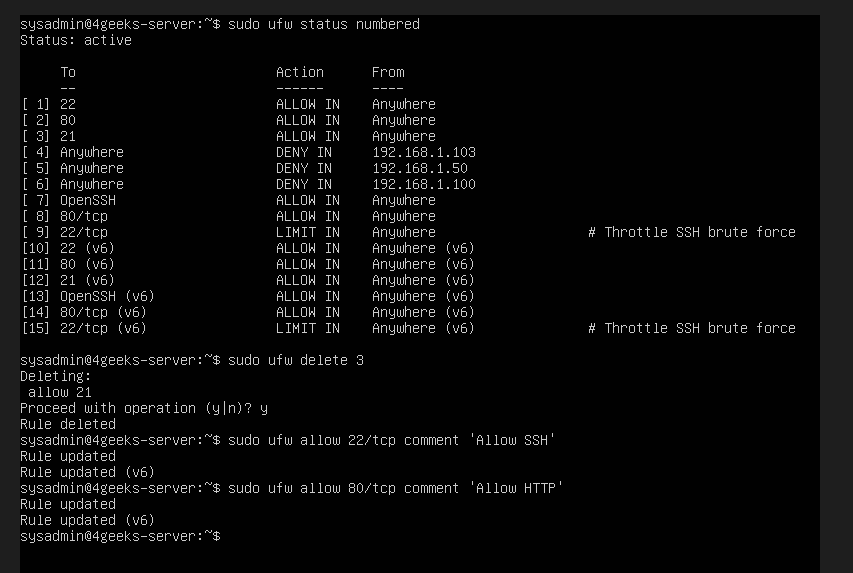
*Figura 33. UFW – estado inicial de reglas y puertos.*



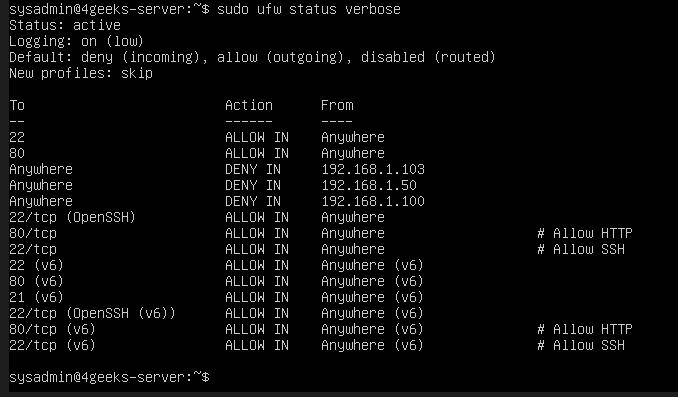
*Figura 34. Políticas por defecto: deny incoming / allow outgoing.*



*Figura 35. Limitación anti-bruteforce en SSH (ufw limit 22/tcp).*



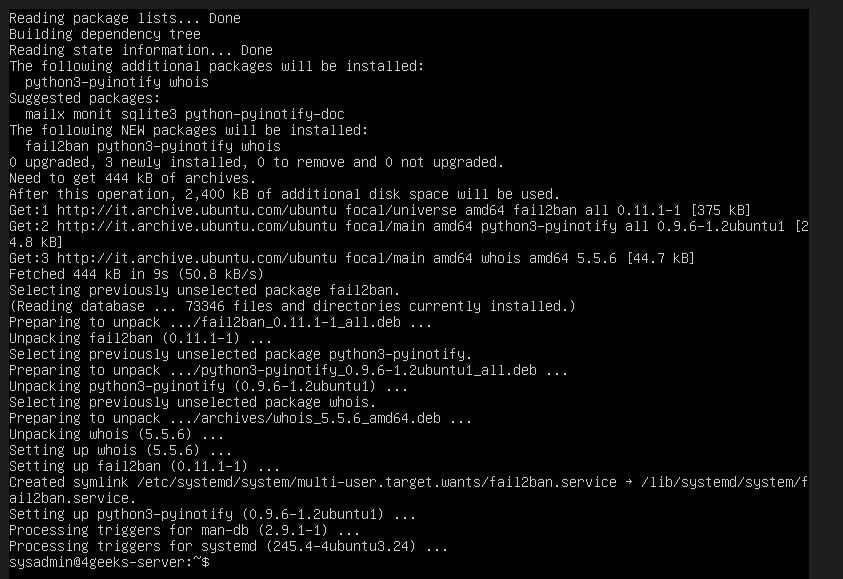
*Figura 36. UFW – reglas numeradas para afinado.*



*Figura 37. UFW – eliminación de regla FTP (21/tcp).*

## Fase 3 Adicional instalar Fail2ban para SSH

Como medida adicional de hardening, se instaló y configuró Fail2ban para proteger SSH contra fuerza bruta.



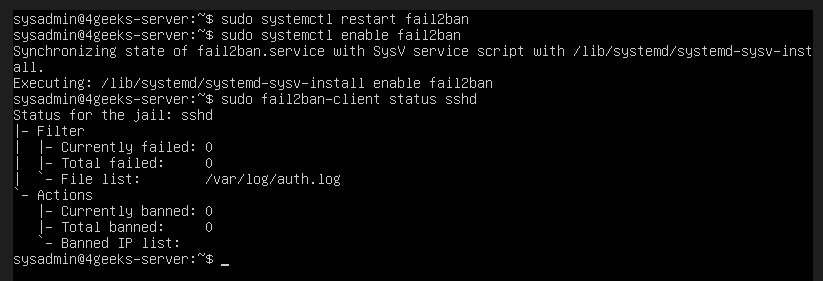
*Figura 38. Instalación de Fail2ban.*



*Figura 39. Copia de jail.conf a jail.local (buenas prácticas).*



*Figura 40. Configuración del jail [sshd] en /etc/fail2ban/jail.local.*



*Figura 41. Estado de Fail2ban para SSH (sin IPs baneadas en ese momento).*

# Conclusión

El incidente fue contenido en vivo y la persistencia eliminada. Se reforzó el entorno con parches, firewall mínimo y protección anti-fuerza bruta.

# Recomendaciones

- Mantener el sistema actualizado con parches de seguridad.

- Usar llaves SSH en lugar de contraseñas; deshabilitar PermitRootLogin.

- Rotar credenciales periódicamente.

- Reducir superficie de ataque (eliminar servicios innecesarios).

- Centralizar logs y monitoreo (SIEM/IDS) según el contexto.

- Configurar alertas (por ejemplo, Fail2ban con correo).

- Realizar auditorías y pruebas de seguridad periódicas.

- Mantener copias de seguridad cifradas y probadas.