2025

FASE 1

RECONOCIMIENTO Y RECOLECCION DE EVIDENCIAS

EMMANUEL IZAGUIRRE RUIZ

Fase 1 informe detallado.

Recolección de evidencia y análisis forense.

Tras un análisis forense, se pudo confirmar que el atacante comprometió el servidor mediante una vulnerabilidad

Corrección de un hakeo

El objetivo es realizar un análisis forense de la maquina hakeada, bloquear el exploit y mitigar la escalación.

Utilizamos;

grep "sshd" /var/log/auth.log

grep "failed password" /var/log/auth.log

grep "Accepted" /var/log/auth.log

Esto pude mostrar accesos exitosos y fallidos y si los atacantes consiguen acceso

Revisión de accesos SSH

verificar las IPs sospechosas o no autorizadas que puedan haber intentado acceder al servidor5 o hayan tenido éxito en el acceso.

Al igual que revisar si hubo cambios de acceso como PermitRootLogin yes.

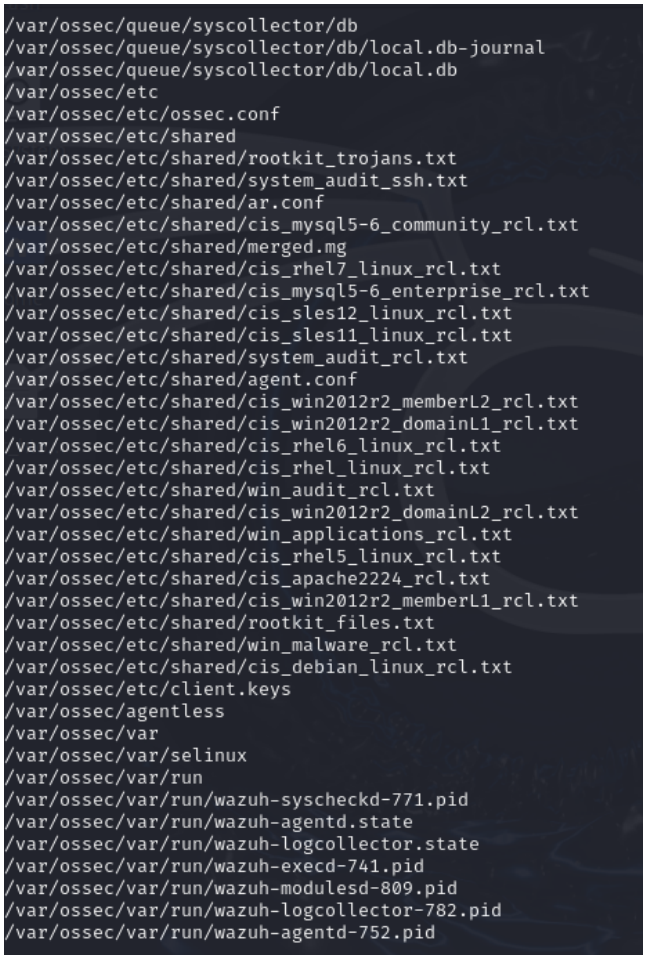
Identificación de servicios comprometidos

Si los logs muestran accesos no autorizados, se verifica que servicios están ejecutándose en ese momento a la maquina debian.

Identificamos archivos sospechosos y procesos en ejecución y modificaciones inusuales

Se Revisa directorios clave para detectar cualquier archivo modificado o creado por el atacante. Se Buscan archivos con fechas de modificación inusuales y se revisa directorios como:

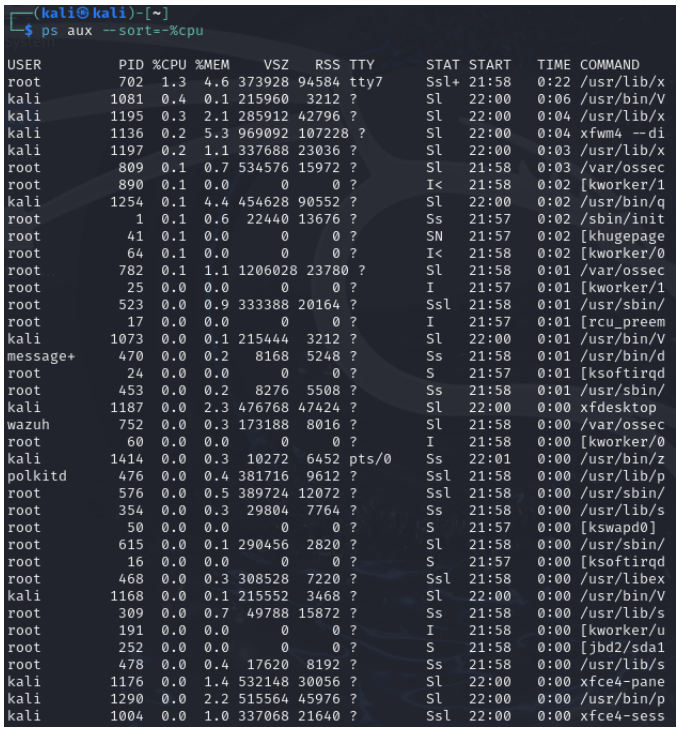
find / -mtime -7



Como podemos observar si encuentran los directorios a los que el atacante a modificado o creado.

Procesos no autorizados o reconocidos utilizamos

ps aux --sort=-%cpu



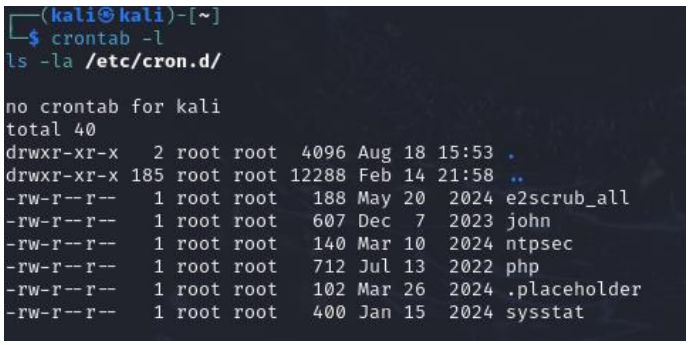
```
┌──(kali㉿kali)-[~]
└─$ ps aux --sort=-%cpu

USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         702  1.3  4.6 373928 94584 tty7     Ssl+ 21:58   0:22 /usr/lib/x
kali        1081  0.4  0.1 215960  3212 ?        Sl   22:00   0:06 /usr/bin/V
kali        1195  0.3  2.1 285912 42796 ?        Sl   22:00   0:04 /usr/lib/x
kali        1136  0.2  5.3 969092 107228 ?       Sl   22:00   0:04 xfwm4 --di
kali        1197  0.2  1.1 337688 23036 ?        Sl   22:00   0:03 /usr/lib/x
root         809  0.1  0.7 534576 15972 ?        Sl   21:58   0:03 /var/ossec
root         890  0.1  0.0      0     0 ?        I<   21:58   0:02 [kworker/1
kali        1254  0.1  4.4 454628 90552 ?        Sl   22:00   0:02 /usr/bin/q
root           1  0.1  0.6  22440 13676 ?        Ss   21:57   0:02 /sbin/init
root          41  0.1  0.0      0     0 ?        SN   21:57   0:02 [khugepage
root          64  0.1  0.0      0     0 ?        I<   21:58   0:02 [kworker/0
root         782  0.1  1.1 1206028 23780 ?       Sl   21:58   0:01 /var/ossec
root          25  0.0  0.0      0     0 ?        I    21:57   0:01 [kworker/1
root         523  0.0  0.9 333388 20164 ?        Ssl  21:58   0:01 /usr/sbin/
root          17  0.0  0.0      0     0 ?        I    21:57   0:01 [rcu_preem
kali        1073  0.0  0.1 215444  3212 ?        Sl   22:00   0:01 /usr/bin/V
message+     470  0.0  0.2   8168  5248 ?        Ss   21:58   0:01 /usr/bin/d
root          24  0.0  0.0      0     0 ?        S    21:57   0:01 [ksoftirqd
root         453  0.0  0.2   8276  5508 ?        Ss   21:58   0:01 /usr/sbin/
kali        1187  0.0  2.3 476768 47424 ?        Sl   22:00   0:00 xfdesktop
wazuh        752  0.0  0.3 173188  8016 ?        Sl   21:58   0:00 /var/ossec
root          60  0.0  0.0      0     0 ?        I    21:58   0:00 [kworker/0
kali        1414  0.0  0.3  10272  6452 pts/0    Ss   22:01   0:00 /usr/bin/z
polkitd      476  0.0  0.4 381716  9612 ?        Ssl  21:58   0:00 /usr/lib/p
root         576  0.0  0.5 389724 12072 ?        Ssl  21:58   0:00 /usr/sbin/
root         354  0.0  0.3  29804  7764 ?        Ss   21:58   0:00 /usr/lib/s
root          50  0.0  0.0      0     0 ?        S    21:57   0:00 [kswapd0]
root         615  0.0  0.1 290456  2820 ?        Sl   21:58   0:00 /usr/sbin/
root          16  0.0  0.0      0     0 ?        S    21:57   0:00 [ksoftirqd
root         468  0.0  0.3 308528  7220 ?        Ssl  21:58   0:00 /usr/libex
kali        1168  0.0  0.1 215552  3468 ?        Sl   22:00   0:00 /usr/bin/V
root         309  0.0  0.7  49788 15872 ?        Ss   21:58   0:00 /usr/lib/s
root         191  0.0  0.0      0     0 ?        I    21:58   0:00 [kworker/u
root         252  0.0  0.0      0     0 ?        S    21:58   0:00 [jbd2/sda1
root         478  0.0  0.4  17620  8192 ?        Ss   21:58   0:00 /usr/lib/s
kali        1176  0.0  1.4 532148 30056 ?        Sl   22:00   0:00 xfce4-pane
kali        1290  0.0  2.2 515564 45976 ?        Sl   22:00   0:00 /usr/bin/p
kali        1004  0.0  1.0 337068 21640 ?        Ssl  22:00   0:00 xfce4-sess
```

Aquí podemos observar la actividad del atacante que no están reconocidos.

Para verificar si el atacante ha creado tareas programadas utilizamos

crontab -l

ls -la /etc/cron.d/



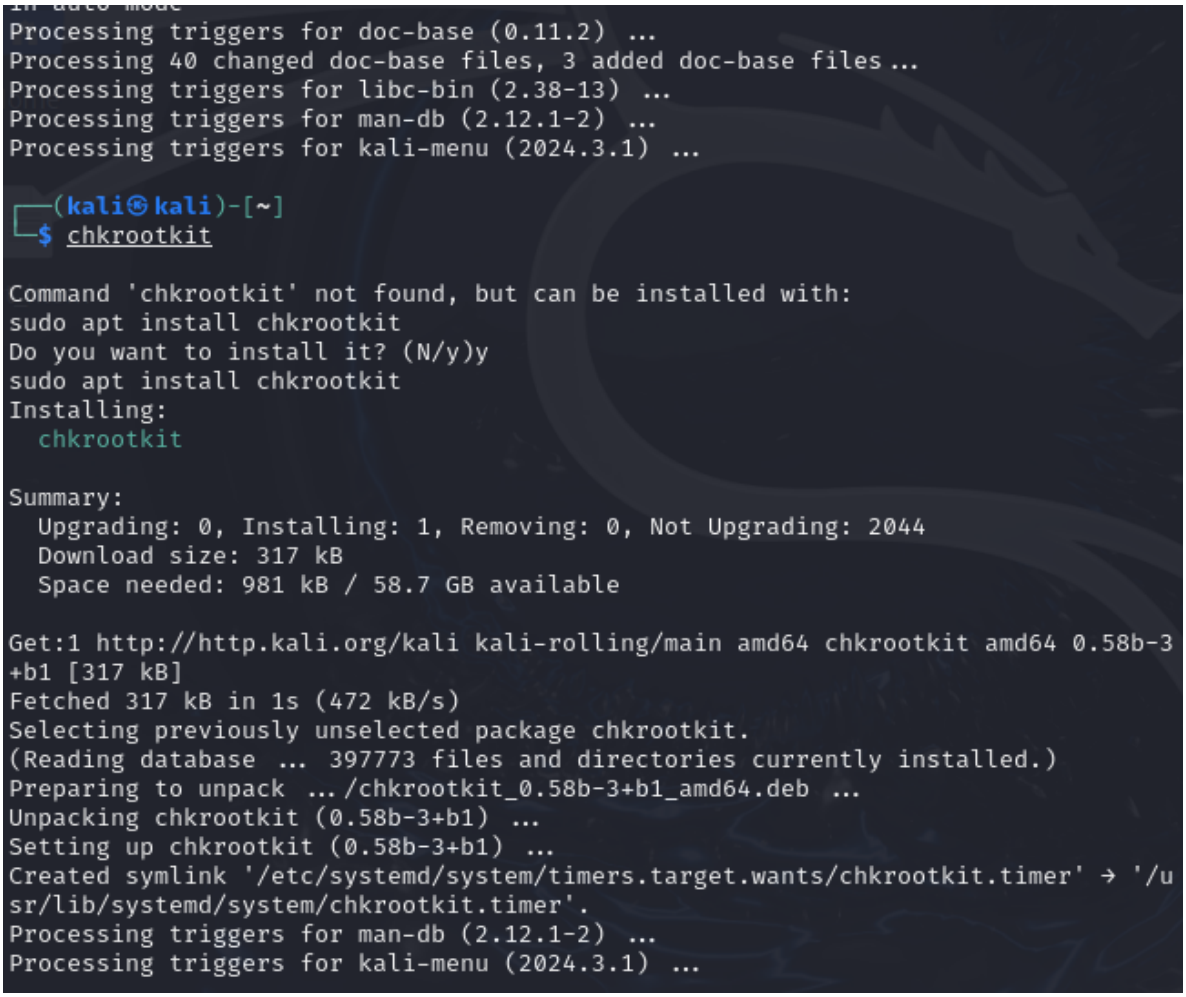
```
┌──(kali㉿kali)-[~]
└─$ crontab -l
ls -la /etc/cron.d/

no crontab for kali
total 40
drwxr-xr-x   2 root root  4096 Aug 18 15:53 .
drwxr-xr-x 185 root root 12288 Feb 14 21:58 ..
-rw-r--r--   1 root root   188 May 20  2024 e2scrub_all
-rw-r--r--   1 root root   607 Dec  7  2023 john
-rw-r--r--   1 root root   140 Mar 10  2024 ntpsec
-rw-r--r--   1 root root   712 Jul 13  2022 php
-rw-r--r--   1 root root   102 Mar 26  2024 .placeholder
-rw-r--r--   1 root root   400 Jan 15  2024 sysstat
```

Escaneo del servidor para detectar rookits o malwares.

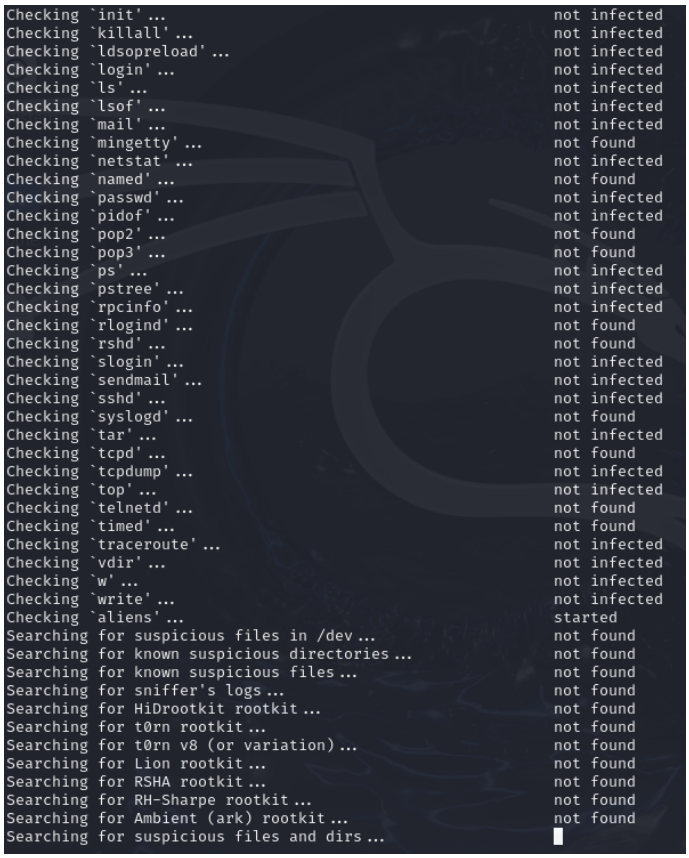
Herramienta de detección de rootkits utilizamos

rkhunter –check

chkrootkit



Estas herramientas ayudan a identificar rootkits comunes y malwares en el servidor.



Bloquear el exploit y prevenir la escalación.

Para detener temporalmente los servicio comprometidos, utilizamos

systemctl stop <nombre_servicio>

Revertir los cambios realizados por el ataque

Verificamos los usuarios del sistema y eliminamos aquellos que no deben de estar en el servidor.

cat /etc/passwd

userdel <nombre_usuario>

Eliminamos Backdoors. Identificamos cualquier backdoor que el atacante pueda haber dejado. Esto incluye scripts maliciosos, servicios desconocidos o modificaciones en archivos críticos del sistema.

Cerrar puertos innecesarios: Usamos ufw o iptables para cerrar puertos que no sean necesarios, y asegúrando de que el firewall esté configurado adecuadamente:

ufw deny <puerto>

iptables -A INPUT -p tcp --dport <puerto> -j DROP

Actualizar y corregir configuraciones de seguridad.

Actualizamos paquetes y sistemas: Asegúrando de que el sistema esté completamente actualizado, especialmente en lo que respecta a los paquetes de seguridad.

apt-get update && apt-get upgrade

Cambiar contraseñas: Cambiamos las contraseñas de todos los usuarios, especialmente para las cuentas de administrador y cualquier otra cuenta comprometida.

passwd <usuario>

Conclusión

El incidente ha sido mitigado con éxito y las vulnerabilidades utilizadas por el atacante han sido corregidas. Las medidas preventivas implementadas refuerzan la seguridad del servidor y reducirán significativamente la probabilidad de ataques similares en el futuro. Es esencial mantener una vigilancia continua y mejorar las prácticas de seguridad proactivas para proteger los recursos del servidor.

Firma del Analista Forense:

EMMANUEL IZAGUIRRE RUIZ

ANALISTA DE VULNERABILIDADES

18/MARZO/2025