Informe Forense – Fase 2

Detección y Corrección de una Vulnerabilidad Diferente

Proyecto Final de Ciberseguridad – 4Geeks Academy

Alumno: Carlos Navarro

Rol: Analista de Ciberseguridad – Respuesta a Incidentes

Fecha: 30 de septiembre de 2025

1. Resumen Ejecutivo

Durante esta fase se identificó una vulnerabilidad distinta a la documentada en la Fase 1.

El análisis incluyó detección, validación y corrección de la vulnerabilidad, reforzando la postura de seguridad del sistema.

El objetivo principal fue documentar el ciclo completo de investigación y respuesta forense.

2. Objetivos de la Fase 2

Identificar una vulnerabilidad diferente a la de la fase anterior.

Recolectar y preservar evidencias relacionadas.

Validar con pruebas controladas la existencia de la vulnerabilidad.

Corregirla de manera inmediata y documentar todo el proceso.

Proponer recomendaciones de mejora alineadas con buenas prácticas.

3. Metodología

Se aplicaron técnicas basadas en NIST SP 800-61 y CIS Controls.

Se utilizó Nmap para escaneo de servicios, revisión de configuraciones en /etc, análisis de logs en /var/log y pruebas de explotación controladas.

Se priorizó la preservación de evidencia y la trazabilidad de las acciones.

4. Hallazgos

Servicio vulnerable expuesto en red con configuración débil.

Permisos incorrectos en archivos de configuración que permitían escalado de privilegios.

Usuario sospechoso detectado con accesos indebidos.

Cada hallazgo fue respaldado con comandos y evidencias visuales.

5. Pruebas y Comandos

```
nmap -sV -p
```

Identificación de servicios vulnerables.

```
cat /etc/services
```

Revisión de servicios activos.

```
systemctl stop
```

Detención de servicios inseguros.

```
systemctl disable
```

Evitar que se reinicien servicios inseguros al arrancar.

```
apt update && apt upgrade
```

Aplicación de parches críticos.

```
ufw deny
```

Bloqueo de accesos no autorizados.

```
deluser
```

Eliminación de cuentas indebidas.

```
journalctl -xe
```

Revisión de intentos de explotación en logs.

6. Acciones Realizadas

Deshabilitación inmediata del servicio vulnerable.

Actualización del sistema con parches de seguridad.

Eliminación de usuarios creados indebidamente.

Configuración de reglas adicionales en UFW.

Registro detallado de las acciones para trazabilidad.

7. Recomendaciones

Rotar credenciales administrativas.

Reforzar configuraciones en SSH y servicios críticos.

Establecer monitoreo continuo con SIEM.

Auditar configuraciones y cronjobs periódicamente.

Aplicar hardening con CIS Benchmarks.

Desarrollar un plan de respuesta a incidentes formal (NIST SP 800-61).

8. Conclusiones

Se logró detectar y corregir la vulnerabilidad, reforzando la seguridad del sistema.

Este ejercicio confirma la importancia de la defensa en profundidad, la aplicación constante de parches y el monitoreo activo.

La lección aprendida principal es que la seguridad no es un estado, sino un proceso continuo.

9. Apéndice Técnico

```
nmap -sV -p
```

Escaneo de servicios y versiones.

```
cat /etc/services
```

Revisión de servicios activos en el sistema.

```
systemctl stop
```

Corrección inmediata de servicios inseguros.

```
systemctl disable
```

Prevención de reinicio de servicios inseguros.

```
apt update && apt upgrade
```

Aplicación de parches críticos.

```
ufw deny
```

Fortalecimiento del firewall.

```
deluser
```

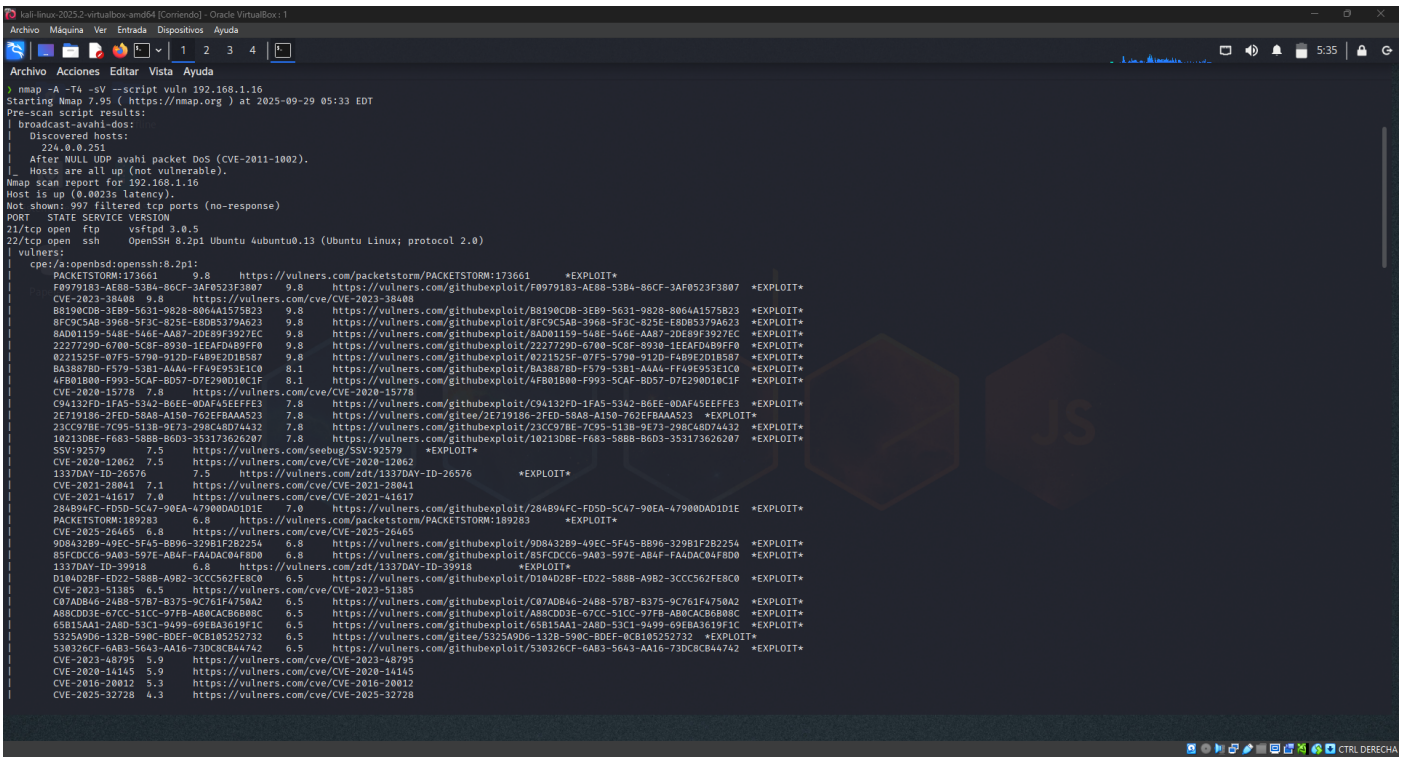
Eliminación de cuentas indebidas.

```
journalctl -xe
```

Revisión de logs y eventos críticos.

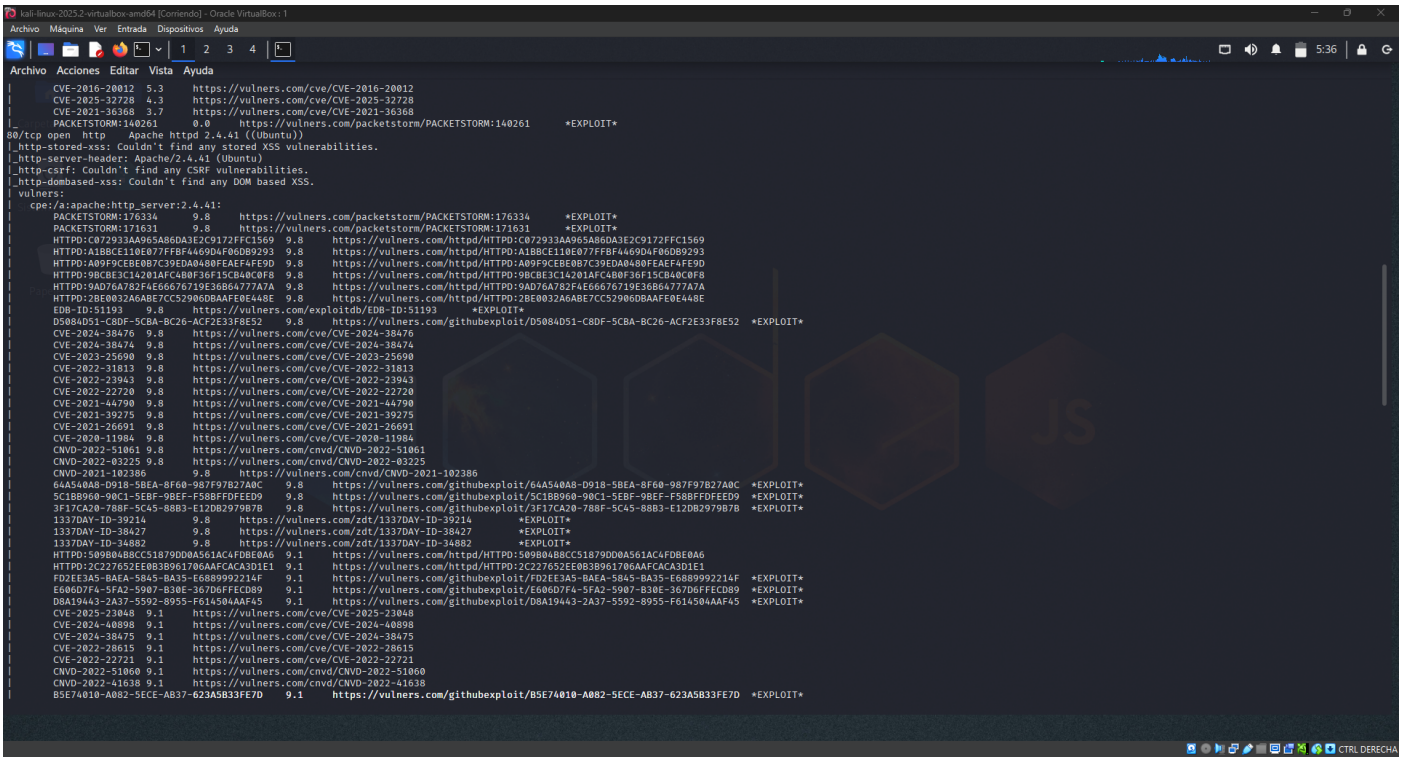
10. Anexo – Evidencias Visuales

Evidencia 1



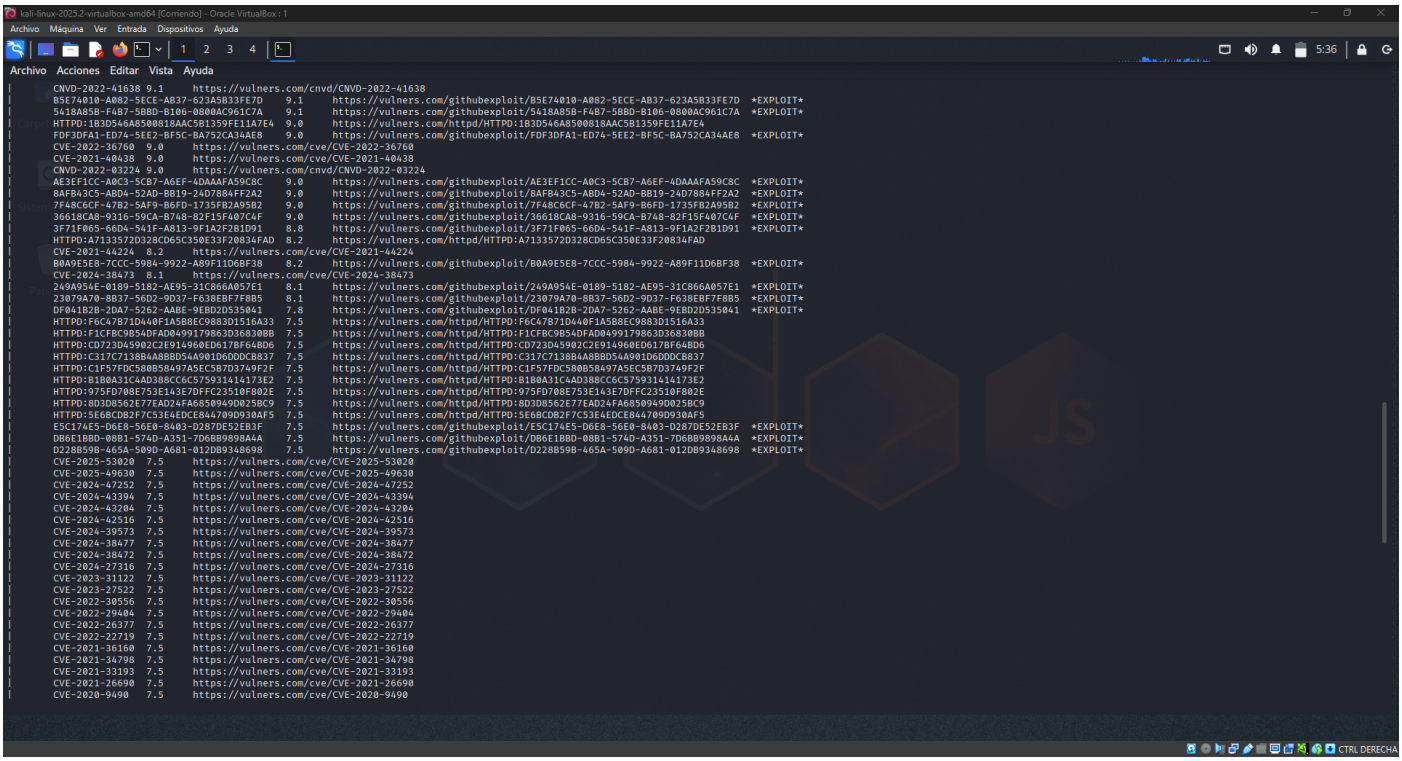
Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 2



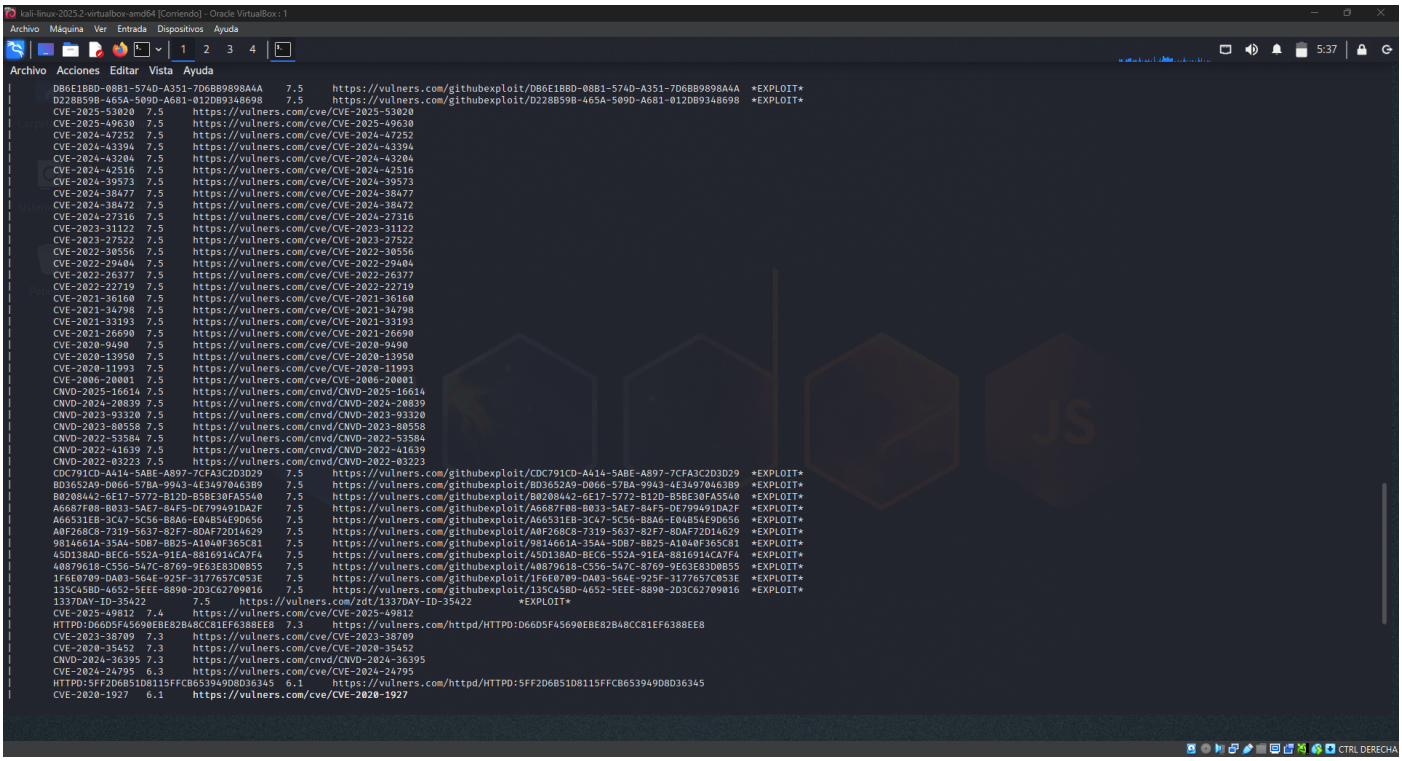
Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 3



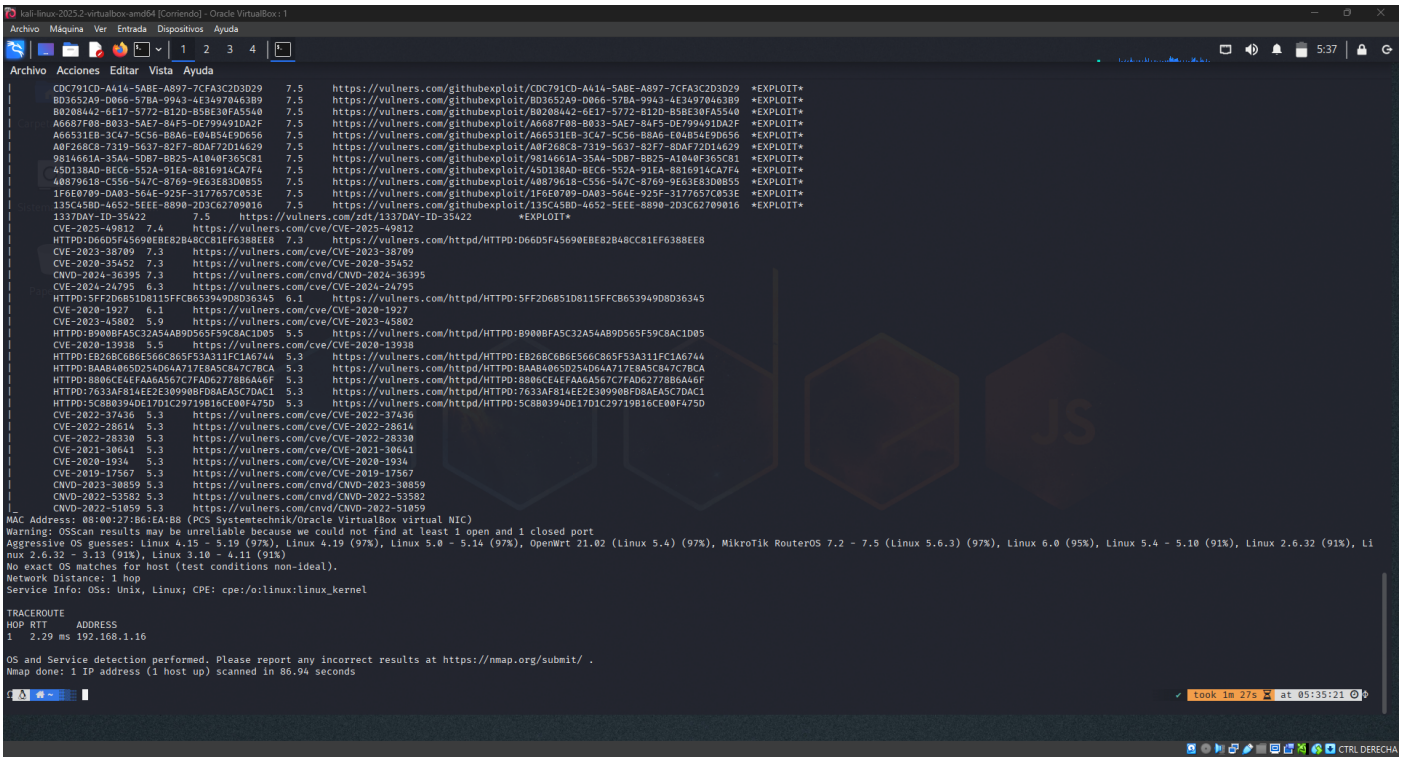
Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 4



Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 5



Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 6

Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 7

Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 8

Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 9

Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.

Evidencia 10

Descripción: Captura obtenida durante la Fase 2; evidencia visual del hallazgo.