

# **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 reinicen 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

The screenshot shows a terminal window titled "Kali-linux-2025.2-virtualbox-amd64 [Coniendo] - Oracle VirtualBox : 1". The terminal displays the results of an nmap scan and a list of exploit links from vulners.com.

```
> nmap -A -T4 -SV --script vuln 192.168.1.16
Starting Nmap 7.90 ( https://nmap.org ) at 2025-09-29 05:33 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|     Hosts are up (no vulnerable).
Nmap scan report for 192.168.1.16
Host is up (0.0023s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
vulnerabilities (please note: vulns found in /root/.nmap/vulns):
  cpe:/a:openbsd:openssh:8.2p1:
    PACKETSTORM:173661      *EXPLOIT*
F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
CVE-2023-38408  9.8   https://vulners.com/cve/CVE-2023-38408
B8100C0D-3E90-4040-B803-808040000003  9.8   https://vulners.com/githubexploit/B8100C0D-3E90-4040-B803-808040000003 *EXPLOIT*
0F2524AD-5C66-5F3C-075E-80B5379A623  9.8   https://vulners.com/githubexploit/0F2524AD-5C66-5F3C-075E-80B5379A623 *EXPLOIT*
8AD01159-548E-546E-AA87-2DE89F3927EC  9.8   https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
22272290-6700-5C8F-8938-1EEAF04B9FF0  9.8   https://vulners.com/githubexploit/22272290-6700-5C8F-8938-1EEAF04B9FF0 *EXPLOIT*
0221525F-07F5-5798-912D-F4B9E2D1B587  9.8   https://vulners.com/githubexploit/0221525F-07F5-5798-912D-F4B9E2D1B587 *EXPLOIT*
A3887BD-F579-53B1-AA4A-FF49E953E10  8.1   https://vulners.com/githubexploit/A3887BD-F579-53B1-AA4A-FF49E953E10 *EXPLOIT*
4FB01B00-F993-5CAF-B057-D7E49009C1F  8.1   https://vulners.com/githubexploit/4FB01B00-F993-5CAF-B057-D7E49009C1F *EXPLOIT*
CVE-2023-3777-548E-546E-AA87-2DE89F3927EC  8.1   https://vulners.com/githubexploit/CVE-2023-3777-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
C94132FD-1FA5-5342-B0EE-00AFA5EEFFEE3  7.8   https://vulners.com/githubexploit/C94132FD-1FA5-5342-B0EE-00AFA5EEFFEE3 *EXPLOIT*
2E719186-2FED-58AB-A150-762EFBAA523  7.8   https://vulners.com/githubexploit/2E719186-2FED-58AB-A150-762EFBAA523 *EXPLOIT*
23CC97BE-7C95-51B8-9E73-298C4B074432  7.8   https://vulners.com/githubexploit/23CC97BE-7C95-51B8-9E73-298C4B074432 *EXPLOIT*
02130DBE-F683-58BB-B603-353173626208  7.8   https://vulners.com/githubexploit/02130DBE-F683-58BB-B603-353173626208 *EXPLOIT*
SSV-2023-12062  7.5   https://vulners.com/githubexploit/SSV-2023-12062 *EXPLOIT*
CVE-2023-28041  7.5   https://vulners.com/cve/CVE-2023-28041 *EXPLOIT*
1337DAY-ID-26576  7.5   https://vulners.com/ztf/1337DAY-ID-26576 *EXPLOIT*
CVE-2021-28041  7.1   https://vulners.com/cve/CVE-2021-28041 *EXPLOIT*
CVE-2021-41617  7.0   https://vulners.com/cve/CVE-2021-41617 *EXPLOIT*
2848949-FD50-5C47-98EA-479000AD101E  7.0   https://vulners.com/githubexploit/2848949-FD50-5C47-98EA-479000AD101E *EXPLOIT*
PACKETSTORM:189283-548E-546E-AA87-2DE89F3927EC  6.8   https://vulners.com/cve/CVE-2025-189283 *EXPLOIT*
90843289-49EC-5F45-BB96-329B1FB2B254  6.8   https://vulners.com/githubexploit/90843289-49EC-5F45-BB96-329B1FB2B254 *EXPLOIT*
85FCD6C6-9A03-597E-AB4F-F4AAC04F8D0  6.8   https://vulners.com/githubexploit/85FCD6C6-9A03-597E-AB4F-F4AAC04F8D0 *EXPLOIT*
1337DAY-ID-39918  6.8   https://vulners.com/ztf/1337DAY-ID-39918 *EXPLOIT*
D10404BF-ED22-58BB-A9B2-3C562FEB00  6.5   https://vulners.com/githubexploit/D10404BF-ED22-58BB-A9B2-3C562FEB00 *EXPLOIT*
CVE-2023-28041  6.5   https://vulners.com/cve/CVE-2023-28041 *EXPLOIT*
C07A0B46-2488-5787-B375-C761F4750A2  6.5   https://vulners.com/githubexploit/C07A0B46-2488-5787-B375-C761F4750A2 *EXPLOIT*
A8BCDD03E-67CC-51CC-97FB-A80CACB6B08C  6.5   https://vulners.com/githubexploit/A8BCDD03E-67CC-51CC-97FB-A80CACB6B08C *EXPLOIT*
65B15AA1-2A8D-53C1-9499-69EBA3619F1C  6.5   https://vulners.com/githubexploit/65B15AA1-2A8D-53C1-9499-69EBA3619F1C *EXPLOIT*
5325A906-132B-590C-B0EF-0CB105252732  6.5   https://vulners.com/gitee/5325A906-132B-590C-B0EF-0CB105252732 *EXPLOIT*
530326CF-6A83-5643-AA16-73DC8CB44742  6.4   https://vulners.com/githubexploit/530326CF-6A83-5643-AA16-73DC8CB44742 *EXPLOIT*
CVE-2020-16145  5.9   https://vulners.com/cve/CVE-2020-16145 *EXPLOIT*
CVE-2020-16145  5.9   https://vulners.com/cve/CVE-2020-16145 *EXPLOIT*
CVE-2016-20012  5.3   https://vulners.com/cve/CVE-2016-20012 *EXPLOIT*
CVE-2025-32728  4.3   https://vulners.com/cve/CVE-2025-32728 *EXPLOIT*
```

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

## Evidencia 2

```
Kali-Linux-2025.2-virtualbox-amd64 [Conected] - Oracle VM VirtualBox: 1
Archivo Máquina Ver Entrada Dispositivos Ayuda
[ ] | 1 2 3 4 [ ]
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
User-agent-header: Apache/2.4.41 (Ubuntu)
http-csrf: Couldn't find any CSRF vulnerabilities.
http-dombased-xss: Couldn't find any DOM based XSS.
vulners:
cpe:/a:apache:http_server:2.4.41:
PACKETSTORM:116334 9.8 https://vulners.com/packetstorm/PACKETSTORM:116334 *EXPLOIT*
PACKETSTORM:121031 9.8 https://vulners.com/packetstorm/PACKETSTORM:121031 *EXPLOIT*
HTTPPD:07C072933AA065A80A3E3C0C172FFC1569 9.8 https://vulners.com/httpd/HTTPPD:07C072933AA065A80A3E3C0C172FFC1569
HTTPPD:A1BBCCE110E077FBF446004F00B09293 9.8 https://vulners.com/httpd/HTTPPD:A1BBCCE110E077FBF446004F00B09293
HTTPPD:A09F9CCEBE087C39EDAA480FEAEFFE9D 9.8 https://vulners.com/httpd/HTTPPD:A09F9CCEBE087C39EDAA480FEAEFFE9D
HTTPPD:9BCBEC3C14201AFC4B0F36F15CB40C0F8 9.8 https://vulners.com/httpd/HTTPPD:9BCBEC3C14201AFC4B0F36F15CB40C0F8
HTTPPD:9AD76A782F4E66676719E36B64777A7A 9.8 https://vulners.com/httpd/HTTPPD:9AD76A782F4E66676719E36B64777A7A
HTTPPD:9B0A66676719E36B64777A8E 9.8 https://vulners.com/httpd/HTTPPD:9B0A66676719E36B64777A8E
EDB-ID:51193 9.8 https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
D5084D51-5C0F-5CBA-BC26-ACF2E33F8E52 9.8 https://vulners.com/githubexploit/D5084D51-5C0F-5CBA-BC26-ACF2E33F8E52 *EXPLOIT*
CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474
CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474
CVE-2023-25690 9.8 https://vulners.com/cve/CVE-2023-25690
CVE-2023-25681 9.8 https://vulners.com/cve/CVE-2023-25681
CVE-2022-23943 9.8 https://vulners.com/cve/CVE-2022-23943
CVE-2022-22720 9.8 https://vulners.com/cve/CVE-2022-22720
CVE-2021-44790 9.8 https://vulners.com/cve/CVE-2021-44790
CVE-2021-39275 9.8 https://vulners.com/cve/CVE-2021-39275
CVE-2021-39275 9.8 https://vulners.com/cve/CVE-2021-39275
CVE-2021-39275 9.8 https://vulners.com/cve/CVE-2021-39275
CVE-2022-11964 9.8 https://vulners.com/cve/CVE-2022-11964
CNVD-2022-51061 9.8 https://vulners.com/cnvd/CNVD-2022-51061
CNVD-2022-03225 9.8 https://vulners.com/cnvd/CNVD-2022-03225
CNVD-2021-102386 9.8 https://vulners.com/cnvd/CNVD-2021-102386
6A4A540A8-0918-58EA-8F60-987F97B27A0C 9.8 https://vulners.com/githubexploit/6A4A540A8-0918-58EA-8F60-987F97B27A0C *EXPLOIT*
5C0F8966-90C1-5EBF-98EF-F5BFDFEE0D 9.8 https://vulners.com/githubexploit/5C0F8966-90C1-5EBF-98EF-F5BFDFEE0D *EXPLOIT*
3F1370A7-5C45-88B3-10B8397B00 9.8 https://vulners.com/githubexploit/3F1370A7-5C45-88B3-10B8397B00 *EXPLOIT*
1337DAY-1D-39214 9.8 https://vulners.com/zdt/1337DAY-1D-39214 *EXPLOIT*
1337DAY-1D-38427 9.8 https://vulners.com/zdt/1337DAY-1D-38427 *EXPLOIT*
1337DAY-1D-34882 9.8 https://vulners.com/zdt/1337DAY-1D-34882 *EXPLOIT*
HTTPPD:50980A8BC51879000A561AC4F0B8E0A0 9.1 https://vulners.com/httpd/HTTPPD:50980A8BC51879000A561AC4F0B8E0A0
HTTPPD:2C27652E2E8B87000A561AC4F0B8E0A1 9.1 https://vulners.com/httpd/HTTPPD:2C27652E2E8B87000A561AC4F0B8E0A1
F1D02000-5455-5E45-8000-92214F 9.1 https://vulners.com/githubexploit/F1D02000-5455-5E45-8000-92214F *EXPLOIT*
E606D7F4-5FA2-5907-B30E-56706F6ECD89 9.1 https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-56706F6ECD89 *EXPLOIT*
DBA19443-2A37-5592-8955-F61a504AAf45 9.1 https://vulners.com/githubexploit/DBA19443-2A37-5592-8955-F61a504AAf45 *EXPLOIT*
CVE-2025-23048 9.1 https://vulners.com/cve/CVE-2025-23048
CVE-2024-40898 9.1 https://vulners.com/cve/CVE-2024-40898
CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475
CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475
CVE-2022-22721 9.1 https://vulners.com/cve/CVE-2022-22721
CNVD-2022-51060 9.1 https://vulners.com/cnvd/CNVD-2022-51060
CNVD-2022-41638 9.1 https://vulners.com/cnvd/CNVD-2022-41638
B5E74010-A082-5ECE-AB37-623A5B33FE7D 9.1 https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D *EXPLOIT*
```

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

```
 kali-linux-2025.2-virtualbox-amd64 [Conected] - Oracle VirtualBox : 1
Archivo Máquina Ver Entrada Dispositivos Ayuda
[ 1 2 3 4 ] [ ]
Archivo Acciones Editar Vista Ayuda
D86E1B80-08B1-5740-A351-700BB898A4A 7.5 https://vulners.com/githubexploit/D86E1B80-08B1-5740-A351-700BB898A4A *EXPLOIT*
D228B598-465A-509D-A681-0120B9348698 7.5 https://vulners.com/githubexploit/D228B598-465A-509D-A681-0120B9348698 *EXPLOIT*
CVE-2025-53020 7.5 https://vulners.com/cve/CVE-2025-53020*
CVE-2025-49630 7.5 https://vulners.com/cve/CVE-2025-49630
CVE-2024-47252 7.5 https://vulners.com/cve/CVE-2024-47252
CVE-2024-43394 7.5 https://vulners.com/cve/CVE-2024-43394
CVE-2024-43395 7.5 https://vulners.com/cve/CVE-2024-43395
CVE-2024-42516 7.5 https://vulners.com/cve/CVE-2024-42516
CVE-2024-39573 7.5 https://vulners.com/cve/CVE-2024-39573
CVE-2024-38477 7.5 https://vulners.com/cve/CVE-2024-38477
CVE-2024-38472 7.5 https://vulners.com/cve/CVE-2024-38472
CVE-2024-27316 7.5 https://vulners.com/cve/CVE-2024-27316
CVE-2024-27317 7.5 https://vulners.com/cve/CVE-2024-27317
CVE-2023-27522 7.5 https://vulners.com/cve/CVE-2023-27522
CVE-2022-30556 7.5 https://vulners.com/cve/CVE-2022-30556
CVE-2022-29404 7.5 https://vulners.com/cve/CVE-2022-29404
CVE-2022-26377 7.5 https://vulners.com/cve/CVE-2022-26377
CVE-2022-22719 7.5 https://vulners.com/cve/CVE-2022-22719
CVE-2022-19700 7.5 https://vulners.com/cve/CVE-2022-19700
CVE-2021-34798 7.5 https://vulners.com/cve/CVE-2021-34798
CVE-2021-33193 7.5 https://vulners.com/cve/CVE-2021-33193
CVE-2021-26690 7.5 https://vulners.com/cve/CVE-2021-26690
CVE-2020-9490 7.5 https://vulners.com/cve/CVE-2020-9490
CVE-2020-13950 7.5 https://vulners.com/cve/CVE-2020-13950
CVE-2020-10877 7.5 https://vulners.com/cve/CVE-2020-10877
CVE-2006-20001 7.5 https://vulners.com/cve/CVE-2006-20001
CNVD-2025-16614 7.5 https://vulners.com/cnvd/CNVD-2025-16614
CNVD-2024-20839 7.5 https://vulners.com/cnvd/CNVD-2024-20839
CNVD-2023-93320 7.5 https://vulners.com/cnvd/CNVD-2023-93320
CNVD-2023-80549 7.5 https://vulners.com/cnvd/CNVD-2023-80549
CNVD-2023-80548 7.5 https://vulners.com/cnvd/CNVD-2023-80548
CNVD-2022-41639 7.5 https://vulners.com/cnvd/CNVD-2022-41639
CNVD-2022-03223 7.5 https://vulners.com/cnvd/CNVD-2022-03223
CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 7.5 https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 *EXPLOIT*
BD3652A9-D066-57BA-9943-4E3497046389 7.5 https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E3497046389 *EXPLOIT*
BD088442-6E5F-57A1-B139-B2C90A90 7.5 https://vulners.com/githubexploit/BD088442-6E5F-57A1-B139-B2C90A90 *EXPLOIT*
AE66531EB-3C47-5C56-88A6-E0485A090656 7.5 https://vulners.com/githubexploit/AE66531EB-3C47-5C56-88A6-E0485A090656 *EXPLOIT*
AE0F66C8-7319-5637-82F7-80AF72D14629 7.5 https://vulners.com/githubexploit/AE0F66C8-7319-5637-82F7-80AF72D14629 *EXPLOIT*
9814661A-35A4-50B7-BB25-A1040F365C81 7.5 https://vulners.com/githubexploit/9814661A-35A4-50B7-BB25-A1040F365C81 *EXPLOIT*
45D13B4D-BEC6-552A-91EA-8816914CA7F4 7.5 https://vulners.com/githubexploit/45D13B4D-BEC6-552A-91EA-8816914CA7F4 *EXPLOIT*
40640718-C53D-547C-8769-9E63E3D00395 7.5 https://vulners.com/githubexploit/40640718-C53D-547C-8769-9E63E3D00395 *EXPLOIT*
1FF407A0-0083-593F-925F-76518333 7.5 https://vulners.com/githubexploit/1FF407A0-0083-593F-925F-76518333 *EXPLOIT*
135CA58D-4E52-5EEE-8898-203C62700916 7.5 https://vulners.com/githubexploit/135CA58D-4E52-5EEE-8898-203C62700916 *EXPLOIT*
1337DAY-ID-35422 7.5 https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*
CVE-2025-49812 7.4 https://vulners.com/cve/CVE-2025-49812
HTTPD:D6605F45690EBE2B48CC81E6388EE8 7.3 https://vulners.com/http/HTTPD:D6605F45690EBE2B48CC81E6388EE8
CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709
CVE-2023-38708 7.3 https://vulners.com/cve/CVE-2023-38708
CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395
CVE-2024-24795 6.3 https://vulners.com/cve/CVE-2024-24795
HTTPD:5FF2D6B5108115FFCB65394908D36345 6.1 https://vulners.com/http/HTTPD:5FF2D6B5108115FFCB65394908D36345
CVE-2020-1927 6.1 https://vulners.com/cve/CVE-2020-1927
```

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

## Evidencia 5

```
 kali-linux-2025-2-virtualbox-amd64 [Conected] - Oracle VM VirtualBox : 1
Archivo Máquina Ver Entrada Dispositivos Ayuda
Archivo Acciones Editar Vista Ayuda
CDC791CD-A414-5ABE-A897-7CF43C1D2029 7.5 https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CF43C1D2029 *EXPLOIT*
BD3652A0-BD66-9941-4E34970463B9 7.5 https://vulners.com/githubexploit/BD3652A0-BD66-9941-4E34970463B9 *EXPLOIT*
B020842-6F17-5772-B12D-B5BE30FA5540 7.5 https://vulners.com/githubexploit/B020842-6F17-5772-B12D-B5BE30FA5540 *EXPLOIT*
A6687F08-B033-5AE7-8AF5-DE799491DA2F 7.5 https://vulners.com/githubexploit/A6687F08-B033-5AE7-8AF5-DE799491DA2F *EXPLOIT*
A66531EB-3C47-5C56-B8A6-E04B54E9D656 7.5 https://vulners.com/githubexploit/A66531EB-3C47-5C56-B8A6-E04B54E9D656 *EXPLOIT*
A0F26BC8-7319-5637-82F7-80AF72D14629 7.5 https://vulners.com/githubexploit/A0F26BC8-7319-5637-82F7-80AF72D14629 *EXPLOIT*
9B1E9840-5A8D-4501-8890-9E63E83D0B55 7.5 https://vulners.com/githubexploit/9B1E9840-5A8D-4501-8890-9E63E83D0B55 *EXPLOIT*
45013BA0-BEC6-592A-91EA-981B914CA7F4 7.5 https://vulners.com/githubexploit/45013BA0-BEC6-592A-91EA-981B914CA7F4 *EXPLOIT*
40879618-C556-547C-8769-9E63E83D0B55 7.5 https://vulners.com/githubexploit/40879618-C556-547C-8769-9E63E83D0B55 *EXPLOIT*
1F6E0709-D403-564E-925F-3177657C053E 7.5 https://vulners.com/githubexploit/1F6E0709-D403-564E-925F-3177657C053E *EXPLOIT*
135C45BD-4652-5EEE-8890-203C62709016 7.5 https://vulners.com/githubexploit/135C45BD-4652-5EEE-8890-203C62709016 *EXPLOIT*
1337DAY-ID-35422 7.5 https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*
CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709
HTTPD:0x64D9F45690E8E82B48CC1E1F6388EE8 7.3 https://vulners.com/httpd/HTTPD:0x64D9F45690E8E82B48CC1E1F6388EE8
CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709
CVE-2020-35452 7.3 https://vulners.com/cve/CVE-2020-35452
CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395
CVE-2024-24795 6.3 https://vulners.com/cve/CVE-2024-24795
HTTPD:0x64D9F45690E8E82B48CC1E1F6388EE8 6.3 https://vulners.com/httpd/HTTPD:0x64D9F45690E8E82B48CC1E1F6388EE8
CVE-2020-1927 6.1 https://vulners.com/cve/CVE-2020-1927
CVE-2023-45802 5.9 https://vulners.com/cve/CVE-2023-45802
HTTPD:8900BFAC5C32A54AB9D565F59C8AC1D08 5.5 https://vulners.com/httpd/HTTPD:8900BFAC5C32A54AB9D565F59C8AC1D08
CVE-2020-1939 5.5 https://vulners.com/cve/CVE-2020-1939
HTTPD:EB26B6C686524056477E845C9C744 5.3 https://vulners.com/httpd/HTTPD:EB26B6C686524056477E845C9C744
HTTPD:8806CE1EFAA6A57C75AD6277806A64F 5.3 https://vulners.com/httpd/HTTPD:8806CE1EFAA6A57C75AD6277806A64F
HTTPD:7633A8F14E2E3E9990BFD8AAE5C7DAC1 5.3 https://vulners.com/httpd/HTTPD:7633A8F14E2E3E9990BFD8AAE5C7DAC1
HTTPD:5C8B80394DE17D1C29719816CE00F475D 5.3 https://vulners.com/httpd/HTTPD:5C8B80394DE17D1C29719816CE00F475D
CVE-2022-37430 5.3 https://vulners.com/cve/CVE-2022-37430
CVE-2022-28614 5.3 https://vulners.com/cve/CVE-2022-28614
CVE-2022-38640 5.3 https://vulners.com/cve/CVE-2022-38640
CVE-2023-38641 5.3 https://vulners.com/cve/CVE-2023-38641
CVE-2020-1934 5.3 https://vulners.com/cve/CVE-2020-1934
CVE-2019-17567 5.3 https://vulners.com/cve/CVE-2019-17567
CNVD-2023-30859 5.3 https://vulners.com/cnvd/CNVD-2023-30859
CNVD-2023-30859 5.3 https://vulners.com/cnvd/CNVD-2023-30859
CNVD-2023-31089 5.3 https://vulners.com/cnvd/CNVD-2023-31089
MAC Address: 08:00:27:88:E8:88 (PCS SystemTechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 4.19 (97%), Linux 5.0 - 5.14 (97%), OpenWrt 21.02 (Linux 5.4) (97%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (97%), Linux 6.0 (95%), Linux 5.4 - 5.10 (91%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 2.29 ms 192.168.1.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.94 seconds.
took 1m 27s at 05:35:21
CTRL DERECHA
```

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

## Evidencia 6

The screenshot shows a terminal window titled 'kali-linux-2025.2-virtualbox.amd64 [Conected] - Oracle VM VirtualBox - 1'. The terminal displays the output of a Nikto scan against the IP address 192.168.1.16. The output includes the following details:

```
curl -I http://192.168.1.16
HTTP/1.1 200 OK
Date: Mon, 29 Sep 2025 09:50:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 21 Jun 2025 20:01:12 GMT
ETag: "22-6381a70ec77f21"
Accept-Ranges: bytes
Content-Length: 34
Content-Type: text/html

> nikto -h http://192.168.1.16 -ask no
- Nikto v2.5.0

+ Target IP:      192.168.1.16
+ Target Hostname: 192.168.1.16
+ Target Port:    80
+ Start Time:    2025-09-29 05:50:34 (GMT-4)

+ Server: Apache/2.4.41 (Ubuntu)
+ /: The X-Content-Type-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /: The X-Frame-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allow from: * HTTP Methods: GET, POST, OPTIONS, HEAD
+ 8102 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:    2025-09-29 05:51:41 (GMT-4) (67 seconds)

+ 1 host(s) tested
```

The terminal window has a dark background with light-colored text. It includes standard Linux terminal icons (file, folder, terminal, etc.) in the top bar. The bottom right corner shows system status icons.

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

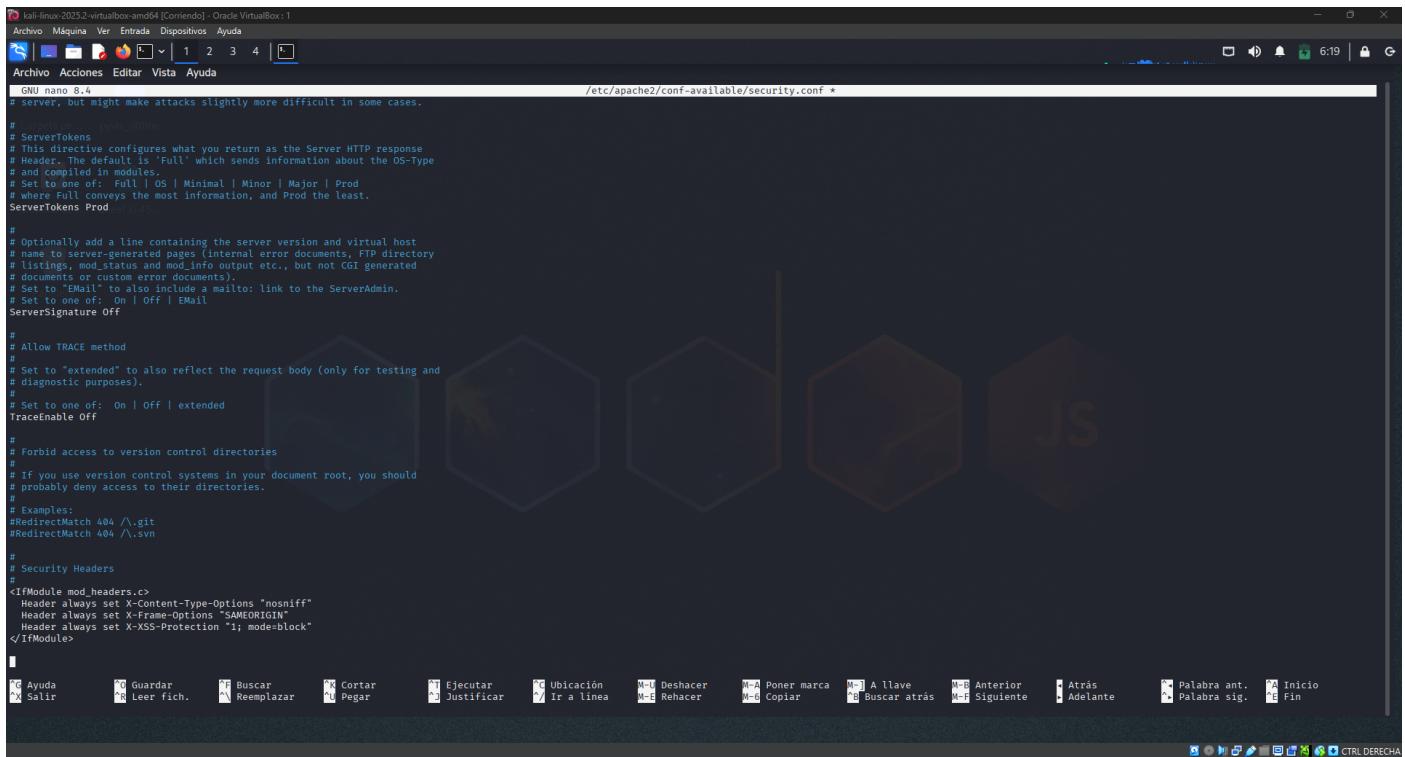
## Evidencia 7

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



```
# GND nano 8.4                                         /etc/apache2/conf-available/security.conf *
# server, but might make attacks slightly more difficult in some cases.
# _ServerTokens
# This directive configures what you return as the Server HTTP response
# Header 'Server'. Set it to 'Full' which sends information about the OS-type
# and compiled modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
ServerTokens Prod

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
ServerSignature Off

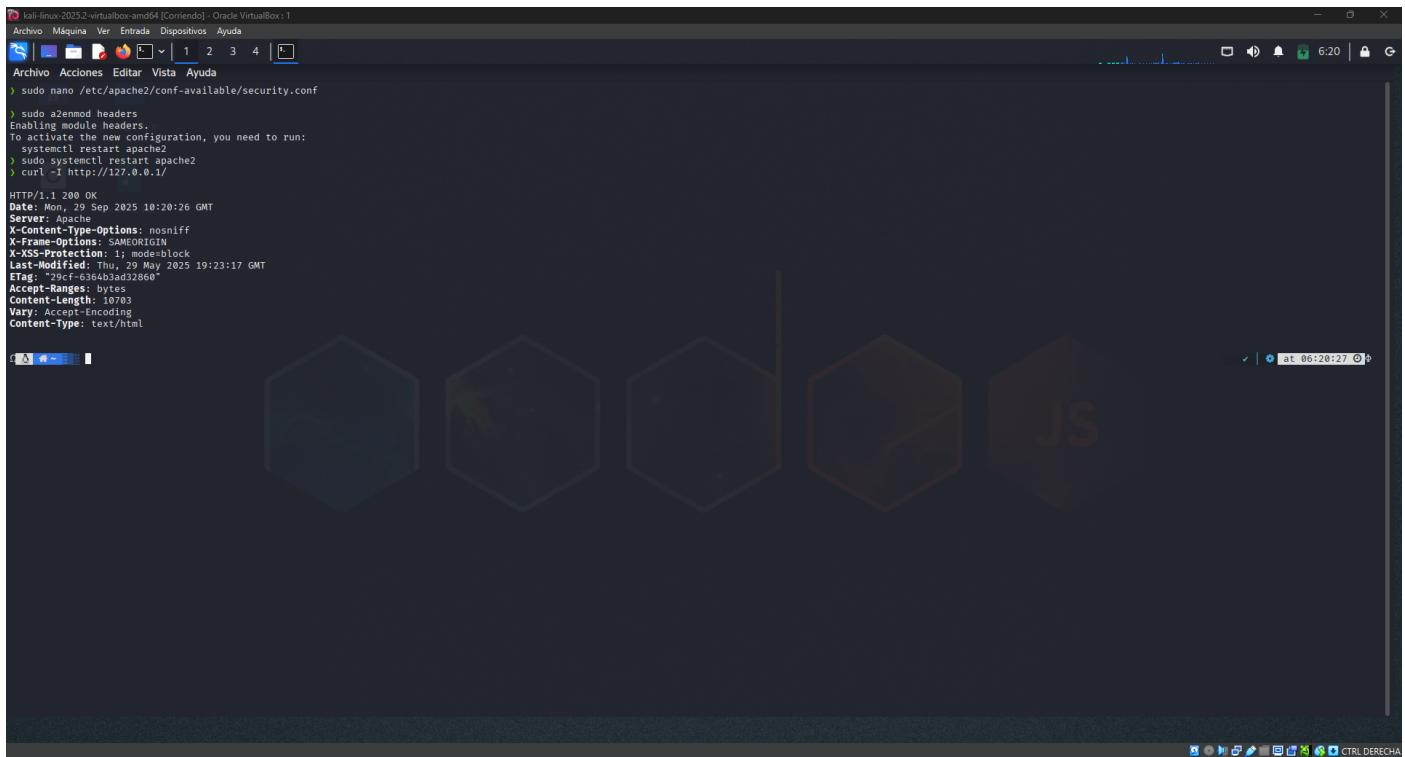
#
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
# diagnostic purposes).
# Set to one of: On | Off | extended
TraceEnable Off

#
# Forbid access to version control directories
#
# If you use version control systems in your document root, you should
# probably deny access to their directories.
#
# Examples:
#RedirectMatch 404 /\.git
#RedirectMatch 404 /\.svn

#
# Security Headers
#
<IfModule mod_headers.c>
    Header always set X-Content-Type-Options "nosniff"
    Header always set X-Frame-Options "SAMEORIGIN"
    Header always set X-XSS-Protection "1; mode=block"
</IfModule>
```

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

## Evidencia 10



Terminal window showing a command being run in a Linux environment:

```
 kali-linux-2025.2-virtualbox-amd64 [Conrado] - Oracle VM VirtualBox : 1
Archivo Máquina Ver Entrada Dispositivos Ayuda
Archivo Acciones Editar Vista Ayuda
> sudo nano /etc/apache2/conf-available/security.conf

> sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
systemctl restart apache2
> sudo systemctl restart apache2
> curl -I http://127.0.0.1/
HTTP/1.1 200 OK
Date: Mon, 29 Sep 2025 10:20:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Last-Modified: Thu, 29 May 2025 19:23:17 GMT
ETag: "29cf-6364b3a3d32860"
Accept-Ranges: bytes
Content-Length: 10703
Vary: Accept-Encoding
Content-Type: text/html
```

The terminal shows the configuration of the Apache headers module and a curl command to test the headers. The curl output indicates a successful 200 OK response with standard security headers.

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