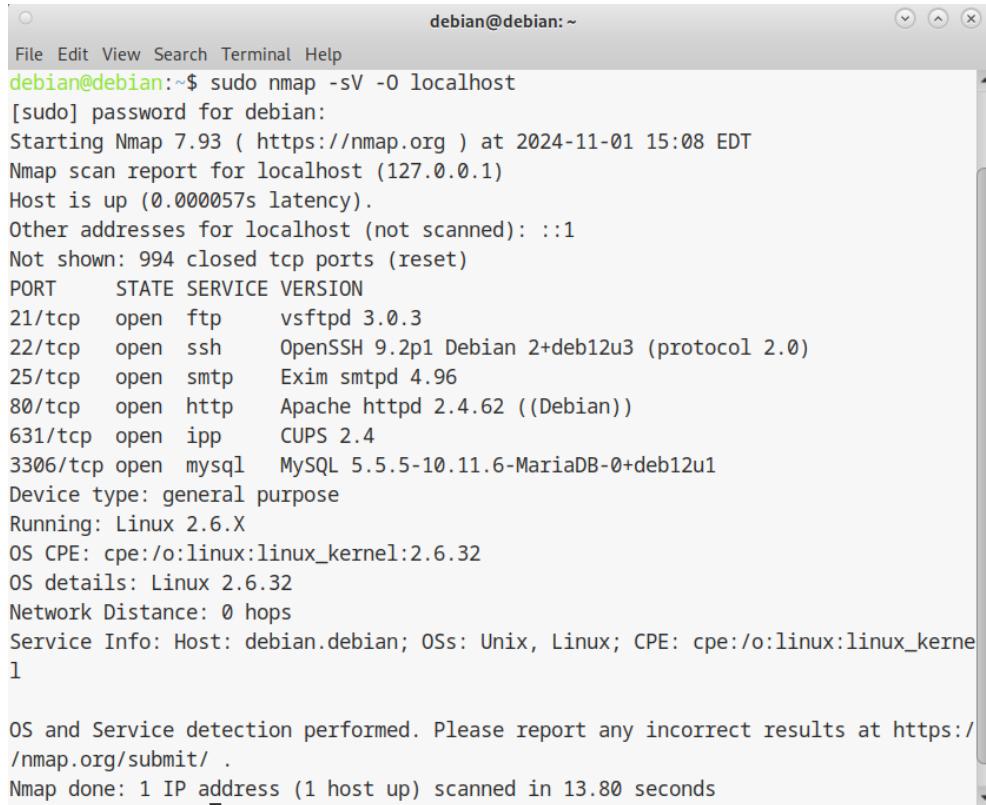


# Proyecto Final.

Iniciando con el análisis forense del proyecto final, se opta por realizar diferentes escaneos local host con algunas herramientas, con el fin de conocer a lo que nos estamos enfrentado.

Iniciamos con un NMAP exponiendo los siguientes resultados que se muestran en la imagen:



```
debian@debian:~$ sudo nmap -sV -o localhost
[sudo] password for debian:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-01 15:08 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).

Other addresses for localhost (not scanned): ::1

Not shown: 994 closed tcp ports (reset)

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
25/tcp    open  smtp    Exim smptd 4.96
80/tcp    open  http   Apache httpd 2.4.62 ((Debian))
631/tcp   open  ipp    CUPS 2.4
3306/tcp  open  mysql  MySQL 5.5.5-10.11.6-MariaDB-0+deb12u1

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: Host: debian.debian; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kerne
1

OS and Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.80 seconds
```

muestra varios puertos abiertos en la máquina local (localhost), lo cual podría presentar algunos riesgos si no están adecuadamente asegurados. A continuación se explican los posibles riesgos y recomendaciones para cada uno de los servicios abiertos:

## 1. Puerto 21 (FTP)

- **Riesgo:** El protocolo FTP transmite información sin cifrar, lo que puede exponer credenciales y datos.
- **Recomendación:** Considera deshabilitar FTP o reemplazarlo por FTPS o SFTP, que son versiones seguras de este protocolo. Si necesitas mantenerlo, asegúrate de restringir el acceso y usar contraseñas fuertes.

## 2. Puerto 22 (SSH)

- **Riesgo:** El acceso SSH puede ser un punto de entrada si se usan contraseñas débiles o si el servicio está abierto para todos.

- **Recomendación:** Configura SSH para autenticación mediante claves en lugar de contraseñas. Asegúrate de que solo los usuarios autorizados puedan acceder y limita las IP permitidas en el archivo de configuración.

### 3. Puerto 25 (SMTP)

- **Riesgo:** Si el servidor SMTP no está configurado adecuadamente, puede ser utilizado para enviar spam o puede revelar información sensible sobre tu sistema.
- **Recomendación:** Asegúrate de que el servicio SMTP esté correctamente configurado y que sólo acepte conexiones internas o autenticadas, dependiendo de tus necesidades. Si no necesitas este servicio, considera desactivarlo.

### 4. Puerto 80 (HTTP)

- **Riesgo:** Un servicio HTTP abierto puede ser vulnerable a ataques web como inyecciones de código o accesos no autorizados.
- **Recomendación:** Asegúrate de mantener el servidor web actualizado y revisa la configuración de seguridad, como permisos de archivos y control de acceso. Si no es necesario, desactívalo o muévelo a HTTPS (puerto 443) para asegurar las conexiones.

### 5. Puerto 631 (IPP - Internet Printing Protocol)

- **Riesgo:** Este puerto se usa para compartir impresoras. Si está expuesto, podría permitir a usuarios no autorizados acceder o modificar servicios de impresión.

```
sudo systemctl stop cups
```

```
sudo systemctl disable cups
```

### 6. Puerto 3306 (MySQL)

- **Riesgo:** MySQL es una base de datos que puede contener datos sensibles. Si está abierto a conexiones remotas, podría ser un blanco para atacantes.
- **Recomendación:** Limita el acceso a MySQL solo desde localhost (127.0.0.1) o restringe el acceso a IPs específicas. Además, utiliza contraseñas fuertes para los usuarios de la base de datos y revisa regularmente los permisos de los usuarios.

#### Acciones Generales Recomendadas

- **Revisa los logs** para ver intentos de acceso sospechosos.
- **Configura un firewall** (como ufw o iptables) para restringir el acceso a los puertos y permitir únicamente aquellos que sean necesarios para el funcionamiento de tu sistema.

```
sudo ufw enable  
sudo ufw allow 22/tcp # Permitir solo SSH si es necesario  
sudo ufw deny 21/tcp # Bloquear FTP si no es necesario
```

También se realiza un escaneo con Nmap con el script vuln:

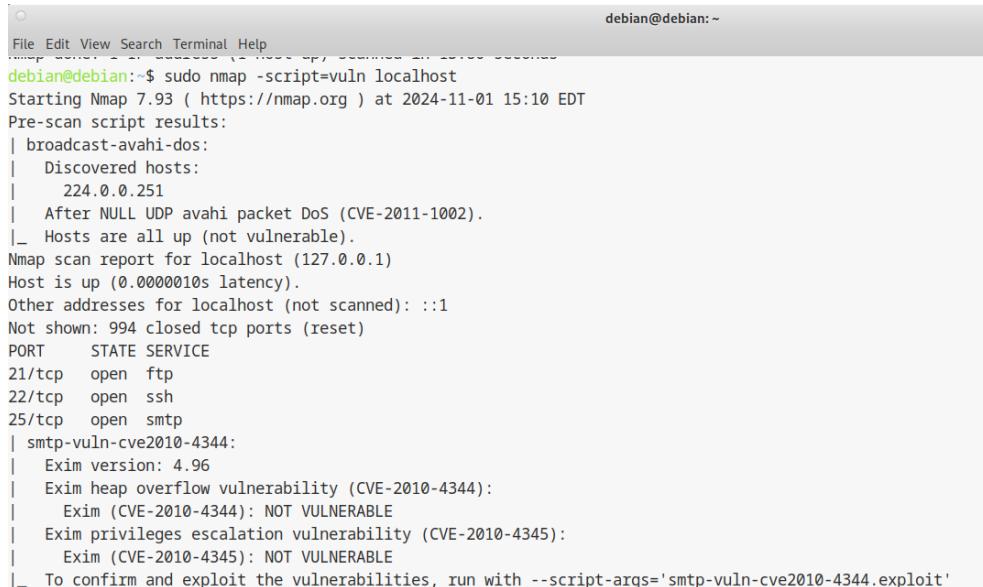
- Se realizó un escaneo en el puerto localhost con el comando sudo nmap --script=vuln localhost.

- **Servicios detectados:**

- **FTP (21/tcp):** Abierto.
- **SSH (22/tcp):** Abierto.
- **SMTP (25/tcp):** Abierto.
- **HTTP (80/tcp):** Abierto.

- **Vulnerabilidades identificadas:**

- En el servicio SMTP, se identificaron posibles vulnerabilidades en Exim relacionadas con la versión 4.96, incluyendo una posible vulnerabilidad de desbordamiento de búfer en la memoria (CVE-2010-4344), aunque el resultado indica que el sistema no es vulnerable a estas versiones específicas de Exim.



```
File Edit View Search Terminal Help  
Nmap scan report for localhost (127.0.0.1)  
debian@debian:~$ sudo nmap -script=vuln localhost  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-01 15:10 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 localhost (127.0.0.1)  
Host is up (0.0000010s latency).  
Other addresses for localhost (not scanned): ::1  
Not shown: 994 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
25/tcp    open  smtp  
| smtp-vuln-cve2010-4344:  
|   Exim version: 4.96  
|   Exim heap overflow vulnerability (CVE-2010-4344):  
|     Exim (CVE-2010-4344): NOT VULNERABLE  
|     Exim privileges escalation vulnerability (CVE-2010-4345):  
|       Exim (CVE-2010-4345): NOT VULNERABLE  
|_  To confirm and exploit the vulnerabilities, run with --script-args='smtp-vuln-cve2010-4344.exploit'
```

- **Servicio HTTP (80/tcp):** Abierto.

- **Vulnerabilidades CSRF:** El escaneo indica que el servicio HTTP podría tener vulnerabilidades CSRF en varios puntos de la aplicación:

- Rutas como /manual, /apache2, /index.php/comments/feed, y /wp-login.php muestran formularios potencialmente vulnerables.
- Esto indica que se han encontrado formularios con IDs específicos y acciones en esas rutas, los cuales podrían ser susceptibles a ataques CSRF si no están protegidos adecuadamente.

```
debian@debian:~  
File Edit View Search Terminal Help  
80/tcp open http  
| http-CSRF:  
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=localhost  
| Found the following possible CSRF vulnerabilities:  
|  
| Path: http://localhost:80/manual  
| Form id: wp-block-search_input-2  
| Form action: http://localhost/  
|  
| Path: http://localhost:80/apache2; repeatmerged=0  
| Form id: wp-block-search_input-2  
| Form action: http://localhost/  
|  
| Path: http://localhost:80/index.php/comments/feed/1quot;https://en.gravatar.com/&quot;&gt;Gravatar&lt;/a&gt;.  
| Form id: wp-block-search_input-2  
| Form action: http://localhost/  
|  
| Path: http://localhost:80/wp-login.php?redirect_to=http%3A%2Flocalhost%2Fwp-admin%2F&reauth=1  
| Form id: loginform  
| Form action: http://localhost/wp-login.php  
|_
```

**Enumeración HTTP:** Se identificaron varias rutas relacionadas con WordPress y su versión.

- La versión de WordPress detectada es antigua (versiones entre 2.0 y 2.7), lo cual podría implicar vulnerabilidades conocidas.
- Se muestran archivos y directorios como /wp-login.php (posible acceso de administración), /robots.txt, y /readme.html.
- Estos resultados sugieren que WordPress en este sistema podría estar desactualizado y expuesto a varias vulnerabilidades.

```
debian@debian:~  
File Edit View Search Terminal Help  
| http-enum:  
| /wp-login.php: Possible admin folder  
| /wp-json: Possible admin folder  
| /robots.txt: Robots file  
| /readme.html: Wordpress version: 2  
| /wp-includes/images/rss.png: Wordpress version 2.2 found.  
| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.  
| /wp-includes/images/blank.gif: Wordpress version 2.6 found.  
| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.  
| /wp-login.php: Wordpress login page.  
| /wp-admin/upgrade.php: Wordpress login page.  
| /readme.html: Interesting, a readme.  
|_ /0/: Potentially interesting folder  
|_ _http-phpself-xss: ERROR: Script execution failed (use -d to debug)  
|_ _http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_ _http-dombased-xss: Couldn't find any DOM based XSS.
```

- **Enumeración de carpetas de administración:** Se detectaron múltiples directorios de administración potenciales, como:

- /admin/, /adminLogin/, /administrator/, /adminarea/, entre otros.
- Algunas de estas rutas devuelven un error 401 (no autorizado), lo que indica que hay algún nivel de restricción, pero podría ser susceptible a ataques de fuerza bruta o enumeración.

- También se encontró un archivo de copia de seguridad (/admin/download/backup.sql), que podría contener información sensible si es accesible.

```
File Edit View Search Terminal Help
[Terminal] Terminal debian: ~
631/tcp open ipp
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
|   /admin/admin/: Possible admin folder
|   /administrator/: Possible admin folder
|   /adminarea/: Possible admin folder
|   /adminLogin/: Possible admin folder
|   /admin_area/: Possible admin folder
|   /administratorlogin/: Possible admin folder
|   /admin/account.php: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /admin/login.php: Possible admin folder (401 Unauthorized)
|   /admin/admin.php: Possible admin folder
|   /admin_area/admin.php: Possible admin folder
|   /admin_area/login.php: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder (401 Unauthorized)
|   /admin/admin.html: Possible admin folder
|   /admin_area/index.php: Possible admin folder
|   /admin/home.php: Possible admin folder
|   /admin_area/login.html: Possible admin folder
|   /admin_area/index.html: Possible admin folder
|   /admin/controlpanel.php: Possible admin folder
|   /adminincp/: Possible admin folder
|   /adminincp/index.asp: Possible admin folder
|   /adminincp/index.html: Possible admin folder
```

- **Archivos y directorios adicionales:** Se encontraron más rutas potencialmente sensibles, como:

- /admin/upload.php (posible subida de archivos en el área de administración).
- Archivos y directorios específicos de diferentes sistemas de administración de contenido y aplicaciones, como Lotus Domino, JBoss, y Moodle.

- **Puerto MySQL (3306/tcp):** Abierto, indicando que el servicio de base de datos MySQL está en ejecución y podría ser accesible si las configuraciones de seguridad no son adecuadas.

```

debian@debian:~ 
File Edit View Search Terminal Help
| /admin108/: Possible admin folder
| /admin_cp.asp: Possible admin folder
| /admin/backup/: Possible backup
| /admin/download/backup.sql: Possible database backup
| /robots.txt: Robots file
| /admin/upload.php: Admin File Upload
| /admin/CiscoAdmin.jhtml: Cisco Collaboration Server
| /admin-console/: JBoss Console
| /admin4.nsf: Lotus Domino
| /admin5.nsf: Lotus Domino
| /admin.nsf: Lotus Domino
| /administrator/wp-login.php: Wordpress login page.
| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/tiny_mce/plugins/tinymce/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.php: Lizard Cart/Remote File upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
| /admin/jscript/upload.pl: Lizard Cart/Remote File upload
| /admin/jscript/upload.asp: Lizard Cart/Remote File upload
| /admin/environment.xml: Moodle files
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /help/: Potentially interesting folder
|_ /printers/: Potentially interesting folder
|_ http-aspNet-debug: ERROR: Script execution failed (use -d to debug)
3306/tcp open mysql

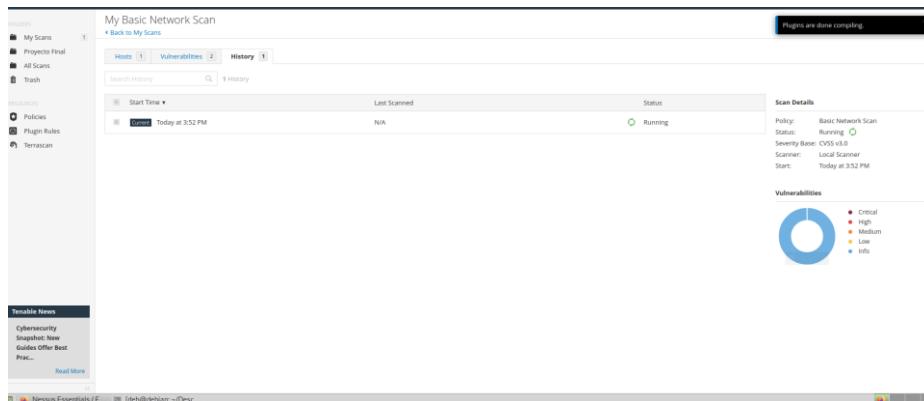
```

Los resultados muestran un sistema con varios servicios expuestos (FTP, SSH, SMTP, HTTP, y MySQL) y múltiples rutas y configuraciones que podrían representar vulnerabilidades, especialmente relacionadas con una versión obsoleta de WordPress y archivos potencialmente sensibles. Se recomienda actualizar los servicios, asegurar los accesos a las rutas de administración y proteger el sistema contra posibles ataques de CSRF y explotación de vulnerabilidades en Exim y WordPress.

Con respecto a MySQL, se ingresa a la base de datos para cambios de contraseñas de los usuarios, logrando así, una mejor cobertura de seguridad, ya que de alguna manera creo que el atacante uso la base de datos para ingresar y escalar privilegios, logrando de esta manera la vulneración de nuestra maquina.

```
MariaDB [(none)]> ALTER USER 'root'@'localhost' IDENTIFIED BY 'SafePassword#4Geeks';
Query OK, 0 rows affected (0.023 sec)
```

Continuando con los escaneos para análisis, utilizamos la herramienta Nessus, arrojándonos los siguientes resultados.



Con un total de 24 vulnerabilidades detectadas, pero ninguna de alta importancia, siendo la mas relevante ICMP Timestamp, a continuación, se deja una serie de imágenes, donde se detallan los resultados y también la descripción de los que a mi parecer son los mas relevantes:

| Severity | CVSS  | VPR | EPS    | Name  | Family            | Count |
|----------|-------|-----|--------|---|-------------------|-------|
| LOW      | 2.1 * | 4.2 | 0.8808 | ICMP Timestamp Request Remote Date Disclosure | General           | 1     |
| INFO     | --    | --  | --     | HTTP (Multiple Issues)                        | Web Servers       | 3     |
| INFO     | --    | --  | --     | SSH (Multiple Issues)                         | General           | 2     |
| INFO     | --    | --  | --     | SSH (Multiple Issues)                         | Misc.             | 2     |
| INFO     | --    | --  | --     | SSH (Multiple Issues)                         | Service detection | 2     |
| INFO     | --    | --  | --     | Nessus SYN scanner                            | Port scanners     | 3     |
| INFO     | --    | --  | --     | Service Detection                             | Service detection | 3     |
| INFO     | --    | --  | --     | Apache HTTP Server Version                    | Web Servers       | 1     |
| INFO     | --    | --  | --     | Backported Security Patch Detection (FTP)     | General           | 1     |
| INFO     | --    | --  | --     | Common Platform Enumeration (CPE)             | General           | 1     |
| INFO     | --    | --  | --     | Device Type                                   | General           | 1     |
| INFO     | --    | --  | --     | Ethernet Card Manufacturer Detection          | Misc.             | 1     |

| Severity | Description   | Family            | Count |
|----------|---|-------------------|-------|
| INFO     | Ethernet MAC Addresses  | General           | 1     |
| INFO     | FTP Server Detection  | Service detection | 1     |
| INFO     | mDNS Detection (Local Network)  | Service detection | 1     |
| INFO     | Nessus Scan Information   | Settings          | 1     |
| INFO     | OpenSSH Detection   | Misc.             | 1     |
| INFO     | OS Identification   | General           | 1     |
| INFO     | OS Security Patch Assessment Not Available                                    | Settings          | 1     |
| INFO     | Target Credential Status by Authentication Protocol - No Credentials Provided | Settings          | 1     |
| INFO     | TCP/IP Timestamps Supported   | General           | 1     |
| INFO     | Traceoute Information   | General           | 1     |
| INFO     | vsftpd Detection  | FTP               | 1     |
| INFO     | Web Server robots.txt Information Disclosure                                  | Web Servers       | 1     |

## Mi exploración básica de red / Plugin .10114

[« Volver a Vulnerabilidades](#)

**Descripción**

El huésped remoto responde a una solicitud de marca de tiempo de la ICMP. Esto permite a un atacante conocer la fecha que se establece en la máquina dirigida, que puede ayudar a un atacante no autenticado y remoto en la derrota de los protocolos de autenticación basados en el tiempo.

Timestamps regresó de las máquinas que ejecutan Windows Vista / 7 / 2008 / 2008 R2 son deliberadamente incorrectos, pero generalmente dentro de 1000 segundos del tiempo real del sistema.

**Solución**

Filtrar las solicitudes de calendario de la ICMP (13) y las respuestas salientes de la Comisión de la ICMP a la Comisión de Letárones (14).

**Producto**

```
El reloj remoto se sincroniza con el reloj local.

To see debug logs, please visit individual host
```

| Puerto   | Anfitriones     |
|----------|-----------------|
| 0 / icmp | 192.168.100.135 |

## ICMP Timestamp Solicitud de fecha remota Divulgación

Idioma: Inglés ▾

BAJO

Nessus Plugin ID 10114

Información Dependencias Dependientes Cambio de cambio

### Sinopsis

Es posible determinar la hora exacta establecida en el huéscos remoto.

### Descripción

El huéscos remoto responde a una solicitud de marca de tiempo de la ICMP. Esto permite a un atacante conocer la fecha que se establece en la máquina dirigida, que puede ayudar a un atacante no autenticado y remoto en la derrota de los protocolos de autenticación basados en el tiempo.

Timestamps regresó de las máquinas que ejecutan Windows Vista / 7 / 2008 / 2008 R2 son deliberadamente incorrectos, pero generalmente dentro de 1000 segundos del tiempo real del sistema.

### Solución

Filtrar las solicitudes de calendario de la ICMP (13) y las respuestas salientes de la Comisión de la ICMP a la Comisión de Letárones (14).

### Detalles de Plugin

**Severidad:** Baja

**ID:** 10114

**Nombre del archivo:** icmp.timestamp.nasl

**versión:** 1.56

**Tipo:** remoto

**Familia:** General

**Publicado:** 8/1/1999

**Actualizado:** 10/7/2024

**Sensores apoyados:** Nessus

### Información de riesgos

#### VPR

**Factor de riesgo:** Medio

**Puntuación:** 4.2

#### CVSS v2

**Factor de riesgo:** Bajo

### INFO | Métodos HTTP permitidos (por directorio)

#### Descripción

Al llamar al método OPTIONS, es posible determinar qué métodos HTTP están permitidos en cada directorio.

Los siguientes métodos HTTP se consideran inseguros:

PUT, DELETE, CONNECT, TRACE, HEAD

Muchos marcos y lenguajes tratan a 'HEAD' como una petición de 'GET', aunque sin ningún cuerpo en la respuesta. Si se establece una restricción de seguridad en las peticiones de 'GET' tales que sólo los 'autenticatedUsers' pudieran acceder a las solicitudes de GET para un servidor o recurso en particular, se pasaría por alto para la versión 'HEAD'. Esto permitió la sumisión ciega no autorizada de cualquier solicitud privilegiada de GET.

Como esta lista puede estar incompleta, el plugin también se pone a prueba -si 'Las pruebas duras' están habilitadas o 'Activar pruebas de aplicaciones web' se establece para 'sí' en la política de escaneo-varios métodos HTTP conocidos en cada directorio y los considera como no soportados si recibe un código de respuesta de 400, 403, 405, o 501.

Tenga en cuenta que la salida del plugin es sólo información y no indica necesariamente la presencia de cualquier vulnerabilidad de seguridad.

#### Vea también

<http://www.nessus.org/u7d9c03a999>

<http://www.nessus.org/u7b019cbdbbbb>

[https://www.owasp.org/index.php/Test-HTTP-Methods\\_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test-HTTP-Methods_(OTG-CONFIG-006))

#### Producto

Basado en la respuesta a una solicitud de OPCIONES:

- Métodos HTTP GET HEAD OPTIONS POST están permitidos en:

/

To see debug logs, please visit individual host

Puerto ▾ Anfitriales

80 / tcp / www 192.168.100.135

## Métodos HTTP permitidos (por directorio)

Idioma: Inglés

INFORMACIÓN Nessus Plugin ID 43111

Información Dependencias Dependientes Cambio de cambio

### Sinopsis

Este plugin determina qué métodos HTTP están permitidos en varios directorios CGI.

### Descripción

Al llamar al método OPTIONS, es posible determinar qué métodos HTTP están permitidos en cada directorio.

Los siguientes métodos HTTP se consideran inseguros:  
PUT, DELETE, CONNECT, TRACE, HEAD

Muchos marcos y lenguajes tratan a 'HEAD' como una petición de 'GET', aunque sin ningún cuerpo en la respuesta. Si se estableciera una restricción de seguridad en las peticiones de 'GET' tales que sólo los 'autenticatedUsers' pudieran acceder a las solicitudes de GET para un servidor o recurso en particular, se pasaría por alto para la versión 'HEAD'. Esto permitió la sumisión ciega no autorizada de cualquier solicitud privilegiada de GET.

Como esta lista puede estar incompleta, el plugin también se pone a prueba -si 'Las pruebas duras' están habilitadas o 'Desactivaciones de aplicaciones web' se establece para 'sí' en la política de escaneo- varlos métodos HTTP conocidos en cada directorio y los considera como no soportados si recibe un código de respuesta de 400, 403, 405, o 501.

Tenga en cuenta que la salida del plugin es sólo información y no indica necesariamente la presencia de cualquier vulnerabilidad de seguridad.

### Detalles de Plugin

Severidad: Info

DNI: 43111

Nombre del archivo: web.directory.options.nasl

Versión: 1.12

Tipo: remoto

Familia: Servidores Web

Publicado: 12/10/2009

Actualizado: 4/11/2022

Configuración: Permite realizar comprobaciones exhaustivas

Sensores apoyados: Nessus

## Mi escaneo básico de red / Plugin no 10107

< Volver al Grupo de Vulnerabilidad

Configuración Camino de auditoría

Anfitriales 1 Vulnerabilidades 24 Historia 1

INFO Tipo y versión HTTP Server



### Descripción

Este plugin intenta determinar el tipo y la versión del servidor web remoto.

### Producto

El tipo de servidor web remoto es:  
Apache/2.4.62 (Debian)

To see debug logs, please visit individual host

Puerto ▾ Anfitriales

80 /tcp/www 192.168.100.135

## Mi exploración básica de red / Plugin 10881

< Volver al Grupo de Vulnerabilidad

Configuración Camino de auditoría

Anfitriales 1 Vulnerabilidades 24 Historia 1

INFO Versiones de protocolo de SSH apoyadas



### Descripción

Este plugin determina las versiones del protocolo SSH soportadas por el demonio SSH remoto.

### Producto

El demonio remoto SSH soporta las siguientes versiones del Protocolo SSH:  
- 1,99  
- 2,0

To see debug logs, please visit individual host

Puerto ▾ Anfitriales

22 /tcp/ssh 192.168.100.135

**INFO** SSH Algoritmos y Lenguas Soportados

**Descripción**

Este script detecta qué algoritmos e idiomas son compatibles con el servicio remoto para cifrar las comunicaciones.

**Producto**

```
Nessus negoció el siguiente algoritmo de cifrado con el servidor:
El servidor es compatible con las siguientes opciones para kex-algorithms:
curve25519-sha256
curve25519-sha512-ctr-libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
kex-strict-a-v00-openssh.com
sntrup761x25519-sha512-openssh.com

El servidor soporta las siguientes opciones para server.host.key.algorithms:
ecdsa-sha2-p12tp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519

El servidor es compatible con las siguientes opciones para encryption.algorithms.client.to.server :
aes128ctr
aes128-gcm.openssh.com
aes192ctr
aes256ctr
aes256-gcm.openssh.com
chacha20-poly1305.openssh.com

El servidor es compatible con las siguientes opciones para cifrado.algorithms.server.toclient :
aes128ctr
aes128-gcm.openssh.com
aes192ctr
```

Mi exploración básica de la red / Plugin 153588

[Configuración](#) [Caminos de auditoría](#)

[Volver al Grupo de Vulnerabilidad](#)

**Anfitriones** 1 **Vulnerabilidades** 24 **Historia** 1

**INFO** Algoritmos HMAC SHA-1 Hávedo

**Descripción**

El servidor SSH remoto está configurado para habilitar algoritmos SHA-1 HMAC.

Aunque NIST ha despreciado formalmente el uso de SHA-1 para firmas digitales, SHA-1 todavía se considera seguro para HMAC ya que la seguridad de HMAC no se basa en que la función de hachido subyacente sea resistente a colisiones.

Tenga en cuenta que este plugin sólo comprueba las opciones del servidor SSH remoto.

**Producto**

```
Los siguientes algoritmos de código de autenticación de mensajes basados en el cliente SHA-1 Hash (HMAC) son compatibles con los siguientes algoritmos:
hmac-sha1
hmac-sha1-etm.openssh.com

Los siguientes algoritmos de servidor a cliente SHA-1 Hash basados en el message Authentication Code (HMAC) son compatibles con :
hmac-sha1
hmac-sha1-etm.openssh.com

To see debug logs, please visit individual host
```

| Puerto ▾   | Anfitriones     |
|------------|-----------------|
| 22/tcp/ssh | 192.168.100.135 |

Mi exploración básica de red / Plugin 149334

[Configuración](#) [Caminos de auditoría](#)

[Volver al Grupo de Vulnerabilidad](#)

**Anfitriones** 1 **Vulnerabilidades** 24 **Historia** 1

**INFO** Atentación de la contraseña SSH Aceptada

**Descripción**

El servidor SSH en el host remoto acepta autenticación de contraseña.

**Vea también**

<https://tools.ietf.org/html/rfc4252-section-8>

Mi exploración básica de red / Plugin  
« Volver al Grupo de Vulnerabilidad

Configuración Camino de auditoría

Anfitriales 1 Vulnerabilidades 24 Historia 1

**INFO** Tipo de servidor SSH y Información de versión

**Descripción**  
Es posible obtener información sobre el servidor SSH remoto enviando una solicitud de autenticación vacía.

**Producto**

```
Versión SSH: SSH-2.0-OpenSSH-9.2p1 Debian-2-debian3
SSH apoya la autenticación: tecla pública, contraseña
```

To see debug logs, please visit individual host

**Puerto ▾ Anfitriales**

|              |                 |
|--------------|-----------------|
| 22 /tcp /ssh | 192.168.100.135 |
|--------------|-----------------|

Mi exploración básica de red / Plugin .48204  
« Volver a Vulnerabilidades

Configuración Camino de auditoría

Anfitriales 1 Vulnerabilidades 24 Historia 1

**INFO** Versión de servidor HTTP de Apache

**Descripción**  
El host remoto está ejecutando el servidor Apache HTTP, un servidor web de código abierto. Fue posible leer el número de versión de la pancarta.

**Vea también**  
<https://httpd.apache.org/>

**Producto**

```
URL: http://192.168.100.135/
Versión: 2.4.62
Fuente: Servidor: Apache/2.4.62 (Debian)
backported: 0
de
```

To see debug logs, please visit individual host

**Puerto ▾ Anfitriales**

|              |                 |
|--------------|-----------------|
| 80 /tcp /www | 192.168.100.135 |
|--------------|-----------------|

Mi exploración básica de red / Plugin 10092  
« Volver a Vulnerabilidades

Configuración Camino de auditoría

Anfitriales 1 Vulnerabilidades 24 Historia 1

**INFO** Detecte de servidor FTP

**Descripción**  
Es posible obtener el banner del servidor FTP remotos conectándose a un puerto remoto.

**Producto**

```
El banner, el remoto FTP es:
220 (vsFTPd 3.0.3)
```

To see debug logs, please visit individual host

**Puerto ▾ Anfitriales**

|              |                 |
|--------------|-----------------|
| 21 /tcp /ftp | 192.168.100.135 |
|--------------|-----------------|

Anfitriones 1 Vulnerabilidades 24 Historia 1

**INFO** detección de mDNS (Red Local) < >

**Descripción**

El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquiera descubrir información del host remoto como su tipo de sistema operativo y versión exacta, su nombre de host, y la lista de servicios que está ejecutando.

Este plugin intenta descubrir el mDNS utilizado por los anfitriones que residen en el mismo segmento de red que Nessus.

**Solución**

Filtrar el tráfico entrante al puerto de UDP 5353, si lo desea.

**Producto**

Nessus pudo extraer la siguiente información:  
- mDNS hosconame: debian.local.

To see debug logs, please visit individual host

Puerto ▾ Anfitriones

5353 / udp / mdns 192.168.100.135

## detección de mDNS (Red Local)

INFORMACIÓN Nessus Plugin ID 66717

Idioma: Inglés ▾

Información Dependencias Dependientes Cambio de cambio

**Sinopsis**

Es posible obtener información sobre el huésped remoto.

**Descripción**

El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquiera descubrir información del host remoto como su tipo de sistema operativo y versión exacta, su nombre de host, y la lista de servicios que está ejecutando.

Este plugin intenta descubrir el mDNS utilizado por los anfitriones que residen en el mismo segmento de red que Nessus.

**Solución**

Filtrar el tráfico entrante al puerto de UDP 5353, si lo desea.

**Detalles de Plugin**

**Severidad:** Info

**DNI:** 66717

**Nombre del archivo:** mdns.localnet.nasl

**Versión:** Revisión: 1.1

**Tipo:** remoto

**Familia:** detección de servicios

**Publicado:** 5/31/2013

**Actualizado:** 5/31/2013

**Sensores apoyados:** Nesso

**Información de vulnerabilidad**

**Artículos de KB requeridos:** /tmp/mdns/report

## vsftpd detection

INFORMACIÓN Nessus Plugin ID 52703

Idioma: Inglés ▾

Información Dependencias Dependientes Cambio de cambio

**Sinopsis**

Un servidor FTP está escuchando en el puerto remoto.

**Descripción**

El host remoto está ejecutando vsftpd, un servidor FTP para sistemas similares a UNIX escritos en C.

**Vea también**

<http://vsftpd.beasts.org/>

**Detalles de Plugin**

**Severidad:** Info

**ID:** 52703

**Nombre del archivo:** vsftpd.detect.nasl

**Versión:** 1.4

**Tipo:** remoto

**Familia:** FTP

**Publicado:** 17/03/2011

**Actualizado:** 22/11/2019

**Inventario de Act Act Acto:** verdad

**Sensores apoyados:** Nesso

**Información de vulnerabilidad**

**CPE:** cpe:/a:beasts:vsftpd

**Artículos de KB requeridos:** ftp/vsftpd



Report generated by Tenable Nessus™

## My Basic Network Scan

Fri, 01 Nov 2024 15:54:42 -04

### TABLE OF CONTENTS

#### Vulnerabilities by Host

- 192.168.100.135

#### Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

#### 192.168.100.135



| Severity | CVSS v3.0 | VPR Score | EPSS Score | Plugin | Name   |
|----------|-----------|-----------|------------|--------|--|
| LOW      | 2.1*      | 4.2       | 0.8808     | 10114  | ICMP Timestamp Request Remote Date Disclosure  |
| INFO     | N/A       | -         | -          | 48204  | Apache HTTP Server Version                     |
| INFO     | N/A       | -         | -          | 39519  | Backported Security Patch Detection (FTP)      |
| INFO     | N/A       | -         | -          | 39520  | Backported Security Patch Detection (SSH)      |
| INFO     | N/A       | -         | -          | 45590  | Common Platform Enumeration (CPE)              |
| INFO     | N/A       | -         | -          | 54615  | Device Type                                    |
| INFO     | N/A       | -         | -          | 35716  | Ethernet Card Manufacturer Detection           |
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses                         |
| INFO     | N/A       | -         | -          | 10092  | FTP Server Detection                           |
| INFO     | N/A       | -         | -          | 43111  | HTTP Methods Allowed (per directory)           |
| INFO     | N/A       | -         | -          | 10107  | HTTP Server Type and Version                   |
| INFO     | N/A       | -         | -          | 24260  | HyperText Transfer Protocol (HTTP) Information |
| INFO     | N/A       | -         | -          | 11219  | Nessus SYN scanner                             |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information                        |
| INFO     | N/A       | -         | -          | 11936  | OS Identification                              |
| INFO     | N/A       | -         | -          | 117886 | OS Security Patch Assessment Not Available     |
| INFO     | N/A       | -         | -          | 181418 | OpenSSH Detection                              |
| INFO     | N/A       | -         | -          | 70657  | SSH Algorithms and Languages Supported         |

|      |     |   |   |        |   |
|------|-----|---|---|--------|---|
| INFO | N/A | - | - | 149334 | SSH Password Authentication Accepted  |
| INFO | N/A | - | - | 10881  | SSH Protocol Versions Supported   |
| INFO | N/A | - | - | 153588 | SSH SHA-1 HMAC Algorithms Enabled   |
| INFO | N/A | - | - | 10267  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | - | 22964  | Service Detection   |
| INFO | N/A | - | - | 25220  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | - | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | - | 10287  | Traceroute Information  |
| INFO | N/A | - | - | 10302  | Web Server robots.txt Information Disclosure                                  |
| INFO | N/A | - | - | 66717  | mDNS Detection (Local Network)  |
| INFO | N/A | - | - | 52703  | vsftpd Detection  |

\* Indicates the v3.0 score was not available;  
the v2.0 score is shown

Hide

Siguiendo las instrucciones del análisis forense: - Identifica archivos sospechosos, procesos en ejecución y cualquier modificación inusual en el sistema.

Ejecutmos el comando ps aux, utilizado para ver los procesos que están en ejecución.

| USER | PID | %CPU | %MEM | VSZ    | RSS   | TTY | STAT | START | TIME | COMMAND           |
|------|-----|------|------|--------|-------|-----|------|-------|------|-------------------|
| root | 1   | 0.0  | 0.6  | 168072 | 12416 | ?   | Ss   | 14:56 | 0:00 | /sbin/init splash |
| root | 2   | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [kthreadd]        |
| root | 3   | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [rcu_gp]          |
| root | 4   | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [rcu_par_gp]      |
| root | 5   | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [slub_flushwq]    |
| root | 6   | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [netns]           |
| root | 10  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [mm_percpu_wq]    |
| root | 11  | 0.0  | 0.0  | 0      | 0     | ?   | I    | 14:56 | 0:00 | [rcu_tasks_kthre  |
| root | 12  | 0.0  | 0.0  | 0      | 0     | ?   | I    | 14:56 | 0:00 | [rcu_tasks_rude_  |
| root | 13  | 0.0  | 0.0  | 0      | 0     | ?   | I    | 14:56 | 0:00 | [rcu_tasks_trace] |
| root | 14  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [ksoftirqd/0]     |
| root | 15  | 0.0  | 0.0  | 0      | 0     | ?   | I    | 14:56 | 0:00 | [rcu_preempt]     |
| root | 16  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [migration/0]     |
| root | 18  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [cpuhp/0]         |
| root | 19  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [cpuhp/1]         |
| root | 20  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [migration/1]     |
| root | 21  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:01 | [ksoftirqd/1]     |
| root | 23  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [kworker/1:0H-ev  |
| root | 26  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [kdevtmpfs]       |
| root | 27  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [inet_frag_wq]    |
| root | 28  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [kaudittd]        |
| root | 29  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [khungtaskd]      |
| root | 30  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [oom_reaper]      |
| root | 31  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [writeback]       |
| root | 32  | 0.0  | 0.0  | 0      | 0     | ?   | S    | 14:56 | 0:00 | [kcompactd0]      |
| root | 33  | 0.0  | 0.0  | 0      | 0     | ?   | SN   | 14:56 | 0:00 | [ksmd]            |
| root | 34  | 0.0  | 0.0  | 0      | 0     | ?   | SN   | 14:56 | 0:00 | [khugepaged]      |
| root | 35  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [kintegrityd]     |
| root | 36  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [kblockd]         |
| root | 37  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [blkcg_punt_bio]  |
| root | 38  | 0.0  | 0.0  | 0      | 0     | ?   | I<   | 14:56 | 0:00 | [tpm_dev_wq]      |

### Columnas principales

- USER:** Muestra el usuario que está ejecutando el proceso. En este caso, todos los procesos están siendo ejecutados por el usuario root.
- PID:** Es el ID de proceso. Cada proceso tiene un identificador único que le permite al sistema gestionar sus recursos.
- %CPU:** Muestra el porcentaje de CPU que está utilizando el proceso. Todos los procesos en esta captura están consumiendo 0% de CPU, lo cual es común para procesos de sistema que están inactivos o esperando eventos.
- %MEM:** Indica el porcentaje de memoria física que está usando el proceso. En esta captura, todos los procesos también muestran 0% de uso de memoria, lo que sugiere que están consumiendo recursos mínimos.
- VSZ:** Tamaño virtual del proceso, es decir, la cantidad de memoria virtual que el proceso está utilizando.
- RSS:** La cantidad de memoria residente, que es la memoria física real que el proceso está usando.

7. **TTY**: Terminal asociado al proceso. Los signos de interrogación (?) indican que estos procesos no están asociados a un terminal, lo cual es típico para procesos de sistema que se ejecutan en segundo plano.
8. **STAT**: El estado del proceso. Algunos valores comunes son:
  - S: Proceso en estado de espera.
  - I: Proceso inactivo o de espera de eventos.
  - SN: Proceso en espera que puede ser interrumpido, con prioridad baja.
  - I<: Proceso inactivo con prioridad alta.
9. **START**: Hora de inicio del proceso.
10. **TIME**: Tiempo total de CPU utilizado por el proceso.
11. **COMMAND**: El comando que inició el proceso.

|          |     |     |     |        |       |   |     |       |      |                    |
|----------|-----|-----|-----|--------|-------|---|-----|-------|------|--------------------|
| root     | 38  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [tpm_dev_wq]       |
| root     | 39  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [edac-poller]      |
| root     | 40  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [devfreq_wq]       |
| root     | 41  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [kworker/0:1H-kbl] |
| root     | 42  | 0.0 | 0.0 | 0      | 0     | ? | S   | 14:56 | 0:00 | [kswapd0]          |
| root     | 49  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [kthrotld]         |
| root     | 51  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [acpi_thermal_pm]  |
| root     | 54  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [mld]              |
| root     | 55  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [kworker/1:1H-kbl] |
| root     | 56  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [ipv6_addrconf]    |
| root     | 61  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [kstrp]            |
| root     | 66  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [zswap-shrink]     |
| root     | 67  | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [kworker/u5:0]     |
| root     | 132 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [ata_sff]          |
| root     | 134 | 0.0 | 0.0 | 0      | 0     | ? | S   | 14:56 | 0:00 | [scsi_eh_0]        |
| root     | 135 | 0.0 | 0.0 | 0      | 0     | ? | S   | 14:56 | 0:00 | [scsi_eh_1]        |
| root     | 136 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [scsi_tmf_0]       |
| root     | 137 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [scsi_tmf_1]       |
| root     | 138 | 0.0 | 0.0 | 0      | 0     | ? | S   | 14:56 | 0:00 | [scsi_eh_2]        |
| root     | 139 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [scsi_tmf_2]       |
| root     | 151 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [kworker/0:2H-kbl] |
| root     | 198 | 0.0 | 0.0 | 0      | 0     | ? | S   | 14:56 | 0:00 | [jbd2/sdal-8]      |
| root     | 199 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [ext4-rsv-conver]  |
| root     | 240 | 0.0 | 1.2 | 57788  | 25532 | ? | Ss  | 14:56 | 0:00 | /lib/systemd/syst  |
| root     | 275 | 0.0 | 0.3 | 27940  | 7236  | ? | Ss  | 14:56 | 0:00 | /lib/systemd/syst  |
| systemd+ | 312 | 0.0 | 0.3 | 90104  | 6680  | ? | Ssl | 14:56 | 0:00 | /lib/systemd/syst  |
| root     | 363 | 0.0 | 0.0 | 0      | 0     | ? | I<  | 14:56 | 0:00 | [cryptd]           |
| root     | 480 | 0.0 | 0.5 | 236948 | 11560 | ? | Ssl | 14:56 | 0:00 | /usr/libexec/acco  |
| avahi    | 483 | 0.0 | 0.1 | 8288   | 3784  | ? | Ss  | 14:56 | 0:00 | avahi-daemon: run  |
| root     | 484 | 0.0 | 0.1 | 6608   | 2716  | ? | Ss  | 14:56 | 0:00 | /usr/sbin/cron -f  |

## Procesos específicos

La lista incluye varios procesos de sistema importantes, como:

- **/sbin/init**: Proceso principal del sistema que inicia todos los demás procesos, ejecutado como init.
- **kthreadd** y procesos relacionados con ksoftirqd, kworker, y migration: Estos son procesos del kernel responsables de manejar tareas en segundo plano, interrupciones y migración de hilos entre CPUs.

- **rcu\_\***: Procesos relacionados con el mecanismo RCU (Read-Copy-Update) del kernel, que gestiona la sincronización de datos en sistemas multinúcleo.
- **khugepaged, ksmd**: Procesos del kernel que gestionan la memoria compartida y las páginas de memoria grandes.
- **oom\_reaper**: Proceso que maneja la recolección de procesos que consumen demasiada memoria, para evitar que el sistema se quede sin recursos.

|          |      |     |      |         |        |      |      |       |      |                   |
|----------|------|-----|------|---------|--------|------|------|-------|------|-------------------|
| message+ | 485  | 0.0 | 0.2  | 9992    | 5680   | ?    | Ss   | 14:56 | 0:00 | /usr/bin/dbus-dae |
| polkitd  | 487  | 0.0 | 0.4  | 310004  | 10020  | ?    | Ssl  | 14:56 | 0:00 | /usr/lib/polkit-1 |
| root     | 488  | 0.0 | 0.3  | 25332   | 7804   | ?    | Ss   | 14:56 | 0:00 | /lib/systemd/syst |
| root     | 489  | 0.0 | 0.8  | 394836  | 16756  | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/udis |
| avahi    | 492  | 0.0 | 0.0  | 8100    | 364    | ?    | S    | 14:56 | 0:00 | avahi-daemon: chr |
| root     | 520  | 0.0 | 1.0  | 258660  | 22140  | ?    | Ssl  | 14:56 | 0:00 | /usr/sbin/Network |
| root     | 521  | 0.0 | 0.2  | 16532   | 5832   | ?    | Ss   | 14:56 | 0:00 | /sbin/wpa_supplic |
| root     | 527  | 0.0 | 0.6  | 317328  | 12208  | ?    | Ssl  | 14:56 | 0:00 | /usr/sbin/ModemMa |
| root     | 559  | 0.0 | 0.2  | 10196   | 4172   | ?    | Ss   | 14:56 | 0:00 | /usr/sbin/vsftpd  |
| root     | 563  | 0.0 | 0.3  | 308484  | 7300   | ?    | Sls1 | 14:56 | 0:00 | /usr/sbin/lightdm |
| root     | 581  | 0.0 | 0.4  | 15432   | 9376   | ?    | Ss   | 14:56 | 0:00 | sshd: /usr/sbin/s |
| root     | 653  | 0.0 | 1.7  | 268684  | 35388  | ?    | Ss   | 14:56 | 0:00 | /usr/sbin/apache2 |
| root     | 654  | 3.7 | 8.7  | 824848  | 176936 | tty7 | Ssl+ | 14:56 | 3:54 | /usr/lib/xorg/Xor |
| root     | 659  | 0.0 | 0.0  | 5872    | 1060   | tty1 | Ss+  | 14:56 | 0:00 | /sbin/getty -o -  |
| mysql    | 679  | 0.1 | 12.0 | 1481700 | 242972 | ?    | Ssl  | 14:56 | 0:10 | /usr/sbin/mariadb |
| www-data | 688  | 0.0 | 2.4  | 274492  | 50060  | ?    | S    | 14:56 | 0:05 | /usr/sbin/apache2 |
| www-data | 689  | 0.0 | 2.4  | 274344  | 49148  | ?    | S    | 14:56 | 0:05 | /usr/sbin/apache2 |
| www-data | 690  | 0.1 | 3.0  | 349740  | 61524  | ?    | S    | 14:56 | 0:06 | /usr/sbin/apache2 |
| www-data | 691  | 0.0 | 2.5  | 272560  | 51368  | ?    | S    | 14:56 | 0:05 | /usr/sbin/apache2 |
| www-data | 692  | 0.0 | 2.4  | 272496  | 49272  | ?    | S    | 14:56 | 0:05 | /usr/sbin/apache2 |
| root     | 746  | 0.0 | 0.5  | 27268   | 10692  | ?    | Ss   | 14:56 | 0:00 | /usr/sbin/cupsd - |
| root     | 748  | 0.0 | 0.7  | 176108  | 14876  | ?    | Ssl  | 14:56 | 0:00 | /usr/sbin/cups-br |
| Debian-+ | 1062 | 0.0 | 0.8  | 28328   | 16852  | ?    | Ss   | 14:56 | 0:00 | /usr/sbin/exim4 - |
| rtkit    | 1102 | 0.0 | 0.0  | 22700   | 1532   | ?    | SNs1 | 14:56 | 0:00 | /usr/libexec/rtki |
| root     | 1220 | 0.0 | 0.4  | 162436  | 8180   | ?    | SL   | 14:56 | 0:00 | lightdm --session |
| debian   | 1249 | 0.0 | 0.5  | 19120   | 10748  | ?    | Ss   | 14:56 | 0:00 | /lib/systemd/syst |
| debian   | 1252 | 0.0 | 0.1  | 103648  | 3304   | ?    | S    | 14:56 | 0:00 | (sd-pam)          |
| debian   | 1270 | 1.2 | 1.5  | 1441008 | 31972  | ?    | S<s1 | 14:56 | 1:16 | /usr/bin/pulseaud |
| debian   | 1272 | 0.0 | 0.5  | 239908  | 11916  | ?    | Sls1 | 14:56 | 0:00 | /usr/bin/gnome-ke |
| debian   | 1276 | 0.0 | 0.2  | 9520    | 5168   | ?    | Ss   | 14:56 | 0:00 | /usr/bin/dbus-dae |
| debian   | 1280 | 0.0 | 1.3  | 264800  | 27440  | ?    | Ssl  | 14:56 | 0:00 | x-session-manager |
| debian   | 1333 | 0.0 | 0.0  | 7684    | 768    | ?    | Ss   | 14:56 | 0:00 | /usr/bin/ssh-agen |
| debian   | 1334 | 0.0 | 0.5  | 311280  | 11688  | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/at-s |
| debian   | 1340 | 0.0 | 0.2  | 9384    | 5112   | ?    | S    | 14:56 | 0:00 | /usr/bin/dbus-dae |
| debian   | 1357 | 0.0 | 0.2  | 156452  | 5736   | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/dcon |
| debian   | 1361 | 0.0 | 2.1  | 943908  | 42432  | ?    | SL   | 14:56 | 0:00 | /usr/bin/mate-set |
| debian   | 1364 | 0.0 | 0.5  | 164520  | 10096  | ?    | SL   | 14:56 | 0:00 | /usr/libexec/at-s |
| debian   | 1370 | 0.0 | 2.3  | 469392  | 47140  | ?    | SL   | 14:56 | 0:05 | marco             |
| debian   | 1371 | 0.0 | 0.4  | 237508  | 9816   | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1378 | 0.0 | 0.4  | 380372  | 8648   | ?    | SL   | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1395 | 0.0 | 2.4  | 552344  | 48620  | ?    | SL   | 14:56 | 0:01 | mate-panel        |
| debian   | 1413 | 0.0 | 0.6  | 351468  | 13380  | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1416 | 0.0 | 3.3  | 749280  | 67172  | ?    | SL   | 14:56 | 0:01 | /usr/bin/caja     |
| debian   | 1419 | 0.0 | 0.4  | 312420  | 10036  | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1422 | 0.0 | 1.5  | 497012  | 32220  | ?    | SL   | 14:56 | 0:00 | /usr/lib/mate-pan |
| debian   | 1430 | 0.0 | 0.4  | 233524  | 8392   | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1440 | 0.1 | 3.4  | 387960  | 69908  | ?    | SL   | 14:56 | 0:06 | /usr/bin/python3  |
| debian   | 1446 | 0.0 | 2.7  | 389404  | 55560  | ?    | SL   | 14:56 | 0:01 | mate-screensaver  |
| debian   | 1447 | 0.0 | 0.4  | 233352  | 8388   | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1448 | 0.0 | 2.1  | 672204  | 42760  | ?    | SL   | 14:56 | 0:00 | mate-volume-contr |
| debian   | 1454 | 0.0 | 1.6  | 496644  | 33412  | ?    | SL   | 14:56 | 0:00 | mate-power-manage |
| debian   | 1458 | 0.0 | 0.4  | 234308  | 8716   | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/gvfs |
| debian   | 1460 | 0.0 | 1.8  | 507724  | 36872  | ?    | SL   | 14:56 | 0:00 | nm-applet         |
| debian   | 1461 | 0.0 | 0.9  | 186216  | 18200  | ?    | SL   | 14:56 | 0:00 | /usr/libexec/polk |
| debian   | 1467 | 0.0 | 0.8  | 390268  | 16324  | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/xdg- |
| debian   | 1471 | 0.0 | 1.8  | 604072  | 37420  | ?    | SL   | 14:56 | 0:00 | /usr/lib/mate-pan |
| debian   | 1472 | 0.0 | 1.5  | 495336  | 30484  | ?    | SL   | 14:56 | 0:00 | /usr/lib/mate-pan |
| debian   | 1486 | 0.0 | 0.5  | 460344  | 11180  | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/xdg- |
| debian   | 1498 | 0.0 | 0.3  | 236700  | 7724   | ?    | Ssl  | 14:56 | 0:00 | /usr/libexec/xdg- |
| root     | 1515 | 0.0 | 0.0  | 2480    | 948    | ?    | Ss   | 14:56 | 0:00 | fusermount3 -o rw |

|          |      |     |     |        |       |       |       |       |       |                    |        |
|----------|------|-----|-----|--------|-------|-------|-------|-------|-------|--------------------|--------|
| root     | 1515 | 0.0 | 0.0 | 2480   | 948   | ?     | Ss    | 14:56 | 0:00  | fusermount3 -o rw  |        |
| debian   | 1536 | 0.0 | 1.0 | 335576 | 21112 | ?     | Ssl   | 14:56 | 0:00  | /usr/libexec/xdg-  |        |
| root     | 1552 | 0.0 | 0.4 | 307508 | 8924  | ?     | Ssl   | 14:56 | 0:00  | /usr/libexec/upow  |        |
| debian   | 1619 | 0.0 | 0.5 | 311620 | 10552 | ?     | S1    | 14:56 | 0:00  | /usr/libexec/gvfs  |        |
| debian   | 1651 | 0.0 | 0.6 | 108808 | 12152 | ?     | S1    | 14:56 | 0:02  | /usr/lib/speech-d  |        |
| debian   | 1671 | 0.0 | 0.3 | 363136 | 6064  | ?     | S1    | 14:56 | 0:00  | /usr/lib/speech-d  |        |
| debian   | 1674 | 0.1 | 0.8 | 730636 | 16556 | ?     | Ssl   | 14:56 | 0:10  | /usr/bin/speech-d  |        |
| debian   | 1740 | 0.0 | 2.4 | 559716 | 49184 | ?     | S1    | 14:57 | 0:04  | mate-terminal      |        |
| debian   | 1790 | 0.0 | 0.2 | 8244   | 4980  | pts/0 | Ss+   | 14:57 | 0:00  | bash               |        |
| root     | 1945 | 0.1 | 0.0 | 0      | 0     | ?     | I     | 15:09 | 0:05  | [kworker/1:1-even  |        |
| www-data | 1949 | 0.1 | 2.5 | 274408 | 51816 | ?     | S     | 15:09 | 0:05  | /usr/sbin/apache2  |        |
| root     | 2135 | 0.0 | 0.0 | 0      | 0     | ?     | I<    | 15:11 | 0:00  | [tls-strip]        |        |
| www-data | 2150 | 0.1 | 2.4 | 274476 | 50188 | ?     | S     | 15:11 | 0:05  | /usr/sbin/apache2  |        |
| www-data | 2185 | 0.1 | 2.4 | 274548 | 48704 | ?     | S     | 15:11 | 0:06  | /usr/sbin/apache2  |        |
| www-data | 2187 | 0.0 | 2.4 | 274372 | 49744 | ?     | S     | 15:11 | 0:05  | /usr/sbin/apache2  |        |
| debian   | 2553 | 0.0 | 0.2 | 8244   | 5000  | pts/1 | Ss    | 15:49 | 0:00  | bash               |        |
| root     | 2670 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 15:52 | 0:00  | [kworker/1:2-mm_p  |        |
| root     | 2826 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 16:17 | 0:00  | [kworker/u4:1-flu  |        |
| root     | 2848 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 16:29 | 0:00  | [kworker/u0:1-even |        |
| root     | 2924 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 16:33 | 0:00  | [kworker/u4:0-eve  |        |
| root     | 2926 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 16:34 | 0:00  | [kworker/0:2-ata_  |        |
| root     | 2983 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 16:39 | 0:00  | [kworker/u4:2]     |        |
| root     | 2984 | 0.0 | 0.0 | 0      | 0     | ?     | I     | 16:39 | 0:00  | [kworker/0:0-ata_  |        |
| debian   | 3120 | _   | 0.0 | 0.2    | 11216 | 4388  | pts/1 | R+    | 16:41 | 0:00               | ps aux |

Esta salida muestra principalmente procesos del sistema que se ejecutan en el fondo y están en espera de eventos o solicitudes. Esto es normal para un sistema Debian en estado de inactividad y sin procesos de usuario intensivos en uso. La salida parece limpia y no muestra procesos sospechosos, aunque una revisión más detallada y la verificación de procesos específicos de la auditoría podrían ser necesarias si se busca detectar anomalías.

La imagen muestra la salida del comando sudo systemctl list-units --type=service, que se utiliza para listar todos los servicios en un sistema Linux junto con su estado actual. A continuación se explican los detalles relevantes de la salida:

| UNIT                               | LOAD   | ACTIVE | SUB     | DESCRIPTION                                  |
|------------------------------------|--------|--------|---------|--|
| accounts-daemon.service            | loaded | active | running | Accounts Service                             |
| alsa-restore.service               | loaded | active | exited  | Save/Restore Sound Card State                |
| apache2.service                    | loaded | active | running | The Apache HTTP Server                       |
| apparmor.service                   | loaded | active | exited  | Load AppArmor profiles                       |
| avahi-daemon.service               | loaded | active | running | Avahi mDNS/DNS-SD Stack                      |
| console-setup.service              | loaded | active | exited  | Set console font and keymap                  |
| cron.service                       | loaded | active | running | Regular background program processing daemon |
| cups-browsed.service               | loaded | active | running | Make remote CUPS printers available locally  |
| cups.service                       | loaded | active | running | CUPS Scheduler                               |
| dbus.service                       | loaded | active | running | D-Bus System Message Bus                     |
| exim4.service                      | loaded | active | running | LSB: exim Mail Transport Agent               |
| getty@tty1.service                 | loaded | active | running | Getty on tty1                                |
| ifupdown-pre.service               | loaded | active | exited  | Helper to synchronize boot up for ifupdown   |
| keyboard-setup.service             | loaded | active | exited  | Set the console keyboard layout              |
| kmmod-static-nodes.service         | loaded | active | exited  | Create List of Static Device Nodes           |
| lightdm.service                    | loaded | active | running | Light Display Manager                        |
| ● logrotate.service                | loaded | failed | failed  | Rotate log files                             |
| mariadb.service                    | loaded | active | running | MariaDB 10.11.6 database server              |
| ModemManager.service               | loaded | active | running | Modem Manager                                |
| networking.service                 | loaded | active | exited  | Raise network interfaces                     |
| NetworkManager-wait-online.service | loaded | active | exited  | Network Manager Wait Online                  |
| NetworkManager.service             | loaded | active | running | Network Manager                              |
| plymouth-quit-wait.service         | loaded | active | exited  | Hold until boot process finishes up          |
| plymouth-read-write.service        | loaded | active | exited  | Tell Plymouth To Write Out Runtime Data      |
| plymouth-start.service             | loaded | active | exited  | Show Plymouth Boot Screen                    |
| polkit.service                     | loaded | active | running | Authorization Manager                        |
| rtkit-daemon.service               | loaded | active | running | RealtimeKit Scheduling Policy Service        |
| ssh.service                        | loaded | active | running | OpenBSD Secure Shell server                  |
| systemd-binfmt.service             | loaded | active | exited  | Set Up Additional Binary Formats             |

## Columnas principales

1. **UNIT:** Nombre del servicio.
2. **LOAD:** Indica si el servicio está cargado en el sistema. loaded significa que el servicio está cargado en la memoria.
3. **ACTIVE:** Estado general del servicio. active indica que el servicio está activado en el sistema.
4. **SUB:** Estado detallado del servicio, como running (en ejecución), exited (salió después de ejecutar su tarea), o failed (fallido).
5. **DESCRIPTION:** Descripción breve del servicio.

## Servicios importantes

- **apache2.service:** Activo y en ejecución. Este es el servicio del servidor HTTP Apache.
- **exim4.service:** Activo y en ejecución. Exim es un agente de transporte de correo (MTA) que gestiona correos electrónicos en el sistema.
- **mariadb.service:** Activo y en ejecución. Este es el servidor de base de datos MariaDB.
- **NetworkManager.service:** Activo y en ejecución. Maneja las interfaces de red en el sistema.

## Servicios con estado inusual

- **logrotate.service:** Este servicio tiene el estado failed (fallido). El servicio Logrotate se encarga de rotar los archivos de log para evitar que ocupen demasiado espacio en disco. Un fallo en este servicio puede significar que los archivos de registro no se están rotando correctamente, lo cual podría llevar a problemas de almacenamiento en el sistema si los logs crecen sin control.

En general, la mayoría de los servicios críticos como Apache, MariaDB y NetworkManager están en ejecución y funcionan correctamente. Sin embargo, el servicio logrotate.service ha fallado, lo que sugiere la necesidad de investigar por qué no pudo completar su tarea de rotación de logs. Esto puede requerir revisar los archivos de registro de systemd para obtener más detalles sobre el motivo del fallo y tomar medidas correctivas, como reiniciar el servicio o ajustar su configuración.

Usando la herramienta chkrootkit, nos lanza esta advertencia, sin embargo, el hecho de que chkrootkit marque a **NetworkManager** como un "sniffer" suele ser un falso positivo.

**NetworkManager** es una aplicación legítima que gestiona las conexiones de red en muchos sistemas Linux, y ocasionalmente puede poner la interfaz en modo promiscuo para capturar paquetes de red, especialmente durante actividades de diagnóstico o cuando cambia de estado.

```
Checking `sniffer'...                                WARNING

WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[520], /usr/sbin/NetworkManager[520])
```

Usando la herramienta rkhunter, se detectan varias advertencias que se adjuntan a continuación.

#### /usr/bin/lwp-request - Warning

- lwp-request es parte del paquete libwww-perl, una biblioteca Perl comúnmente usada para realizar solicitudes HTTP. No es en sí mismo malicioso, pero algunos rootkits podrían abusar de esta herramienta.
- **Recomendación:** Verifica que el paquete libwww-perl esté instalado correctamente y que no haya modificaciones inusuales en el archivo. Puedes revisar el archivo ejecutando

```
/usr/bin/gawk                               [ OK ]
/usr/bin/lwp-request                         [ Warning ]
/usr/bin/bsd-mailx                           [ OK ]
```

```
debian@debian:~$ sudo stat /usr/bin/lwp-request
  File: /usr/bin/lwp-request
  Size: 16202          Blocks: 32          IO Block: 4096   regular file
Device: 8,1      Inode: 159100      Links: 1
Access: (0755/-rwxr-xr-x) Uid: (    0/    root)  Gid: (    0/    root)
Access: 2024-11-01 17:37:52.287175143 -0400
Modify: 2023-03-01 11:50:26.000000000 -0500
Change: 2024-07-31 13:35:20.712602000 -0400
 Birth: 2024-07-31 13:35:20.612602000 -0400
```

### Checking for suspicious (large) shared memory segments - Warning

- Esto indica que hay segmentos de memoria compartida grandes que podrían ser sospechosos.
- **Recomendación:** Puedes listar los segmentos de memoria compartida con el siguiente comando para identificar los procesos que los utilizan:

```
Performing malware checks
Checking running processes for suspicious files      [ None found ]
Checking for login backdoors                          [ None found ]
Checking for sniffer log files                      [ None found ]
Checking for suspicious directories                 [ None found ]
Checking for suspicious (large) shared memory segments [ Warning ]
Checking for Apache backdoor                         [ Not found ]
```

La imagen muestra la salida del comando ipcs -m, que se utiliza para mostrar información sobre los segmentos de memoria compartida en el sistema. A continuación se explican los detalles de cada columna.

```
debian@debian:~$ ipcs -m

----- Shared Memory Segments -----
key      shmid   owner    perms      bytes    nattch    status
0x0000000000 98310  debian   600        67108864  2          dest
0x0000000000 8      debian   600        524288   2          dest
0x0000000000 13     debian   600        4194304  2          dest
0x0000000000 16     debian   600        524288   2          dest
0x0000000000 19     debian   600        524288   2          dest
0x0000000000 22     debian   600        524288   2          dest
0x0000000000 25     debian   600        524288   2          dest
0x0000000000 28     debian   600        524288   2          dest
0x0000000000 31     debian   600        524288   2          dest
0x0000000000 36     debian   600        67108864  2          dest
0x0000000000 39     debian   600        4194304  2          dest
0x0000000000 196652  debian   600        524288   2          dest
```

#### Columnas principales

1. **key:** La clave asociada al segmento de memoria compartida. Esta clave es usada por los procesos para acceder a un segmento específico.
2. **shmid:** Identificador único del segmento de memoria compartida.
3. **owner:** Propietario del segmento, en este caso, todos pertenecen al usuario debian.

4. **perms**: Permisos del segmento de memoria compartida, usando un formato similar al de permisos de archivos en Unix. En este caso, 600 significa que solo el propietario tiene permisos de lectura y escritura.
5. **bytes**: Tamaño del segmento de memoria compartida en bytes.
6. **nattch**: Número de procesos que actualmente están adjuntos al segmento de memoria compartida.
7. **status**: Estado del segmento. En esta salida, todos los segmentos están marcados con dest, lo cual indica que están programados para ser eliminados una vez que todos los procesos que los utilizan se hayan desconectado.

### Observaciones

- La mayoría de los segmentos tienen un tamaño de 524,288 bytes, excepto algunos más grandes, como los de 6,710,8864 y 4,194,304 bytes.
- El estado dest sugiere que estos segmentos están en espera de ser eliminados. Esto puede ocurrir cuando un proceso ha marcado los segmentos para su eliminación, pero otros procesos aún están adjuntos a ellos. Una vez que estos procesos se desconecten, los segmentos serán eliminados.
- Si estos segmentos de memoria compartida no son necesarios, puedes forzar su eliminación si están causando problemas de recursos o necesitan ser limpiados. Puedes usar el comando `ipcrm -m <shmid>` para eliminar un segmento específico, reemplazando `<shmid>` con el identificador del segmento correspondiente.
- Este tipo de revisión es útil en auditorías de seguridad y optimización de recursos del sistema para asegurar que no haya segmentos de memoria compartida innecesarios que consuman recursos del sistema.

## SSH root access is allowed - Warning

- Tener acceso SSH permitido para el usuario root es un riesgo de seguridad, ya que podría facilitar el acceso no autorizado.
- **Recomendación:** Desactiva el acceso SSH para root editando el archivo de configuración de SSH:

```
Performing system configuration file checks
  Checking for an SSH configuration file           [ Found ]
  Checking if SSH root access is allowed          [ Warning ]
  Checking if SSH protocol v1 is allowed          [ Not set ]
  Checking for other suspicious configuration settings [ None found ]
  Checking for a running system logging daemon    [ Found ]
  Checking for a system logging configuration file [ Found ]
```

```
File Edit View Search Terminal Help
GNU nano 7.2                                         debian@debian: ~
/etc/ssh/sshd_config

# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

## # Authentication:

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
debian@debian:~$ sudo systemctl restart ssh
```

- Aparte de estos puntos específicos, no se encontraron signos claros de malware o rootkits. Estas advertencias son más indicativas de configuraciones potencialmente inseguras o componentes que podrían ser utilizados en ataques si se dejan sin revisar.

**Conclusión:** No hay evidencias fuertes de infecciones de rootkits, pero sería prudente hacer los ajustes recomendados para mejorar la seguridad de tu sistema y minimizar posibles riesgos.

## Configuración del servidor FTP Puerto 21/tcp.

```

○ debian@debian: ~
File Edit View Search Terminal Help
GNU nano 7.2 /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES

# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO

```

```
debian@debian:~$ sudo ufw allow 21/tcp
```

```
Rules updated
```

```
Rules updated (v6)
```

## SSH (OpenSSH 9.2p1) en el puerto 22

- El servicio SSH es esencial para acceso remoto seguro, pero si el atacante lo ha comprometido, es fundamental restringir el acceso temporalmente.
- Puedes detenerlo, pero solo si tienes acceso físico a la máquina o una alternativa de acceso, ya que perderías acceso remoto.

Configurar correctamente **SSH** (en este caso, **OpenSSH 9.2p1**) en el puerto 22 implica realizar ajustes que mejoren la seguridad y el control de acceso al servidor.

```
○ debian@debian: ~
File Edit View Search Terminal Help
GNU nano 7.2                               /etc/ssh/sshd_config *

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
```

### Protocolo de SSH:

- OpenSSH usa solo el protocolo SSH-2 de manera predeterminada, ya que SSH-1 es obsoleto y menos seguro. Asegúrate de que Protocol no esté configurado en 1.

### Deshabilitar el acceso directo para el usuario root:

- Permitir que root se conecte directamente por SSH es un riesgo de seguridad. Puedes deshabilitar el acceso root configurando PermitRootLogin en no.

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
```

La autenticación por contraseña es menos segura que el uso de claves SSH.

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
HostbasedAuthentication no
```

Continuamos con el proceso, ahora con la herramienta Lynis, la cual es utilizada para realizar análisis de seguridad y proporcionar recomendaciones de fortalecimiento de la seguridad y servidores.

En los resultados proporcionados por Lynis, se observa que se han encontrado varios paquetes vulnerables en el sistema Debian que estás auditando como parte de tu proyecto. Entre los paquetes vulnerables identificados se encuentran:

### Warnings (2) :

- ! Found one or more vulnerable packages. [PKGS-7392]  
<https://cisofy.com/lynis/controls/PKGS-7392/>
  
- ! iptables module(s) loaded, but no rules active [FIRE-4512]  
<https://cisofy.com/lynis/controls/FIRE-4512/>

1. **Apache2:** apache2, apache2-bin, apache2-data, apache2-utils.
2. **Firefox ESR:** firefox-esr.
3. **PHP 8.2:** libapache2-mod-php8.2, php8.2, php8.2-cli, php8.2-common, php8.2-curl, php8.2-gd, php8.2-mbstring, php8.2-mysql, php8.2-opcache, php8.2-readline, php8.2-xml.
4. **xServer:** xserver-common, xserver-xorg-core, xserver-xorg-legacy.
5. **Otros:** libheif1, libjavascriptcoregtk-4.1-0, libwebkit2gtk-4.1-0, libcpupower1, linux-compiler-gcc-12-x86, linux-kbuild-6.1, linux-libc-dev.

```

2024-11-01 20:50:26 Performing test ID PKGS-7392 (Check for Debian/Ubuntu security updates)
2024-11-01 20:50:26 Action: updating package repository with apt-get
2024-11-01 20:50:27 Result: apt-get finished
2024-11-01 20:50:27 Test: Checking if /usr/lib/update-notifier/apt-check exists
2024-11-01 20:50:27 Result: apt-check (update-notifier-common) not found
2024-11-01 20:50:28 Result: found vulnerable package(s) via apt-get (-security channel)
2024-11-01 20:50:28 Found vulnerable package: apache2
2024-11-01 20:50:28 Found vulnerable package: apache2-bin
2024-11-01 20:50:28 Found vulnerable package: apache2-data
2024-11-01 20:50:28 Found vulnerable package: apache2-utils
2024-11-01 20:50:28 Found vulnerable package: firefox-esr
2024-11-01 20:50:28 Found vulnerable package: libapache2-mod-php8.2
2024-11-01 20:50:28 Found vulnerable package: libcpupower1
2024-11-01 20:50:28 Found vulnerable package: libheif1
2024-11-01 20:50:28 Found vulnerable package: libjavascriptcoregtk-4.1-0
2024-11-01 20:50:28 Found vulnerable package: libwebkit2gtk-4.1-0
2024-11-01 20:50:28 Found vulnerable package: linux-compiler-gcc-12-x86
2024-11-01 20:50:28 Found vulnerable package: linux-kbuild-6.1
2024-11-01 20:50:28 Found vulnerable package: linux-libc-dev
2024-11-01 20:50:28 Found vulnerable package: php8.2
2024-11-01 20:50:28 Found vulnerable package: php8.2-cli
2024-11-01 20:50:28 Found vulnerable package: php8.2-common
2024-11-01 20:50:28 Found vulnerable package: php8.2-curl
2024-11-01 20:50:28 Found vulnerable package: php8.2-gd
2024-11-01 20:50:28 Found vulnerable package: php8.2-mbstring
2024-11-01 20:50:28 Found vulnerable package: php8.2-mysql
2024-11-01 20:50:28 Found vulnerable package: php8.2-opcache
2024-11-01 20:50:28 Found vulnerable package: php8.2-readline
2024-11-01 20:50:28 Found vulnerable package: php8.2-xml
2024-11-01 20:50:28 Found vulnerable package: xserver-common
2024-11-01 20:50:28 Found vulnerable package: xserver-xorg-core
2024-11-01 20:50:28 Found vulnerable package: xserver-xorg-legacy
2024-11-01 20:50:28 Warning: Found one or more vulnerable packages. [test:PKGS-7392] [details:-] [solution:-]
2024-11-01 20:50:28 Suggestion: Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades

```

En la salida del archivo /etc/passwd, todos los usuarios parecen estar en orden y cumplen funciones específicas del sistema o servicios (por ejemplo, daemon, www-data, backup, etc.). No hay cuentas de usuario inusuales que llamen la atención inmediatamente.

```

debian@debian: ~ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/nologin
bin:x:2:2:bin:/bin:/usr/nologin
sys:x:3:3: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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:system Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:106:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117:/:/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin

```

Se realiza una actualización de sistema con el comando `sudo apt-get dist-upgrade`:

- **Función:** Este comando también actualiza todos los paquetes a sus versiones más recientes, pero además tiene la capacidad de manejar cambios en las dependencias. Si es necesario, puede instalar nuevas dependencias o eliminar paquetes obsoletos para completar la actualización.

- **Flexibilidad:** Permite realizar una actualización más completa y sofisticada del sistema, ya que maneja conflictos de dependencias que `upgrade` no puede resolver.

- **Uso ideal:** Se usa cuando se necesita una actualización completa del sistema, especialmente después de una actualización importante de versión o cuando hay cambios complejos en las dependencias.

```
debian@debian:~$ sudo apt-get dist-upgrade
[sudo] password for debian:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-22-amd64
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  linux-image-6.1.0-26-amd64
The following packages will be upgraded:
  apache2 apache2-bin apache2-data apache2-utils firefox-esr libapache2-mod-php8.2 libcurl4 libheif1 libjavascriptcoregtk-4.1-0 libwebkit2gtk-4.1-0 linux-compiler-gcc-12-x86
  linux-image-amd64 linux-kbuild-6.1 linux-libc-dev php8.2 php8.2-cli php8.2-common php8.2-curl php8.2-gd php8.2-mbstring php8.2-mysql php8.2-opcache php8.2-readline php8.2-xml
  xserver-common xserver-xorg-core xserver-xorg-legacy
27 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 191 MB of archives.
After this operation, 433 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Configuración segura de MySQL para no permitir conexiones externas si no es necesario, en este caso, queda solo para conexión localhost.

```
GNU nano 7.2                               /etc/mysql/mariadb.conf.d/50-server.cnf

# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#

#user          = mysql
#pid-file     = /run/mysqld/mysqld.pid
#basedir      = /usr
#datadir       = /var/lib/mysql
#tmpdir        = /tmp

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address    = 127.0.0.1

MariaDB [(none)]> ALTER USER 'root'@'localhost' IDENTIFIED BY 'SafePassword#4Geeks';
Query OK, 0 rows affected (0.023 sec)
```

Cambiar la Contraseña de un Usuario Específico.

# Informe de Medidas Tomadas para Mitigar el Ataque y Evitar la Escalación de Privilegios

## Introducción

Durante el análisis forense realizado en el sistema Debian comprometido, se identificaron varios servicios y configuraciones vulnerables que podrían facilitar ataques o escalación de privilegios. Este informe detalla las medidas implementadas para mitigar estos riesgos, así como recomendaciones para prevenir futuros ataques similares.

## Medidas Tomadas para Mitigar el Ataque

### 1. Fortalecimiento de Servicios Expuestos:

- **FTP (Puerto 21):** Dado que el protocolo FTP no cifra las credenciales, se recomendó deshabilitar el servicio o reemplazarlo por SFTP. En este caso, se procedió a restringir el acceso.
- **SSH (Puerto 22):** Se implementó la autenticación mediante claves SSH y se deshabilitó el acceso directo para el usuario root. Esto reduce la probabilidad de ataques de fuerza bruta y la posibilidad de escalación.
- **SMTP (Puerto 25):** Se revisó la configuración del servicio Exim para limitar conexiones no autenticadas y se verificaron actualizaciones para evitar vulnerabilidades conocidas.
- **HTTP (Puerto 80):** Dado que se detectó una versión antigua de WordPress con vulnerabilidades, se actualizó el sistema y se restringió el acceso a rutas sensibles. Además, se implementaron configuraciones para evitar ataques CSRF.
- **MySQL (Puerto 3306):** Se limitó el acceso solo a localhost para evitar conexiones remotas no autorizadas y se fortaleció la configuración de contraseñas.

### 2. Configuración de Firewall:

- Se activó ufw (Uncomplicated Firewall) para restringir el acceso a los puertos necesarios. Esto incluyó permitir solo conexiones SSH seguras y denegar puertos como el FTP y otros no esenciales para la operación del sistema.

### 3. Gestión de Vulnerabilidades de Paquetes:

- Se utilizó Lynis para identificar paquetes vulnerables, como Apache2, PHP, Firefox ESR, y componentes de xServer. Se aplicaron actualizaciones mediante sudo apt-get dist-upgrade para cerrar brechas de seguridad y asegurar que los paquetes se mantengan en sus versiones más recientes y seguras.

#### **4. Manejo de Memoria Compartida y Recursos del Sistema:**

- Se detectaron segmentos de memoria compartida grandes y con estado "dest" (pendiente de eliminación). Estos segmentos se eliminaron para evitar posibles abusos que podrían llevar a la escalación de privilegios.

#### **5. Monitoreo de Procesos:**

- Se revisaron los procesos en ejecución para detectar actividades sospechosas o procesos que pudieran ser utilizados en una escalación de privilegios. No se observaron anomalías, pero se implementaron configuraciones adicionales para limitar el acceso al sistema y monitorear continuamente.

### **Recomendaciones para Prevenir Futuros Ataques**

#### **1. Implementación de Escaneos Regulares:**

- Ejecutar herramientas como Lynis, chkrootkit y rkhunter de forma regular para identificar vulnerabilidades y posibles rootkits. La detección temprana ayuda a mitigar ataques antes de que comprometan el sistema.

#### **2. Fortalecimiento Adicional de SSH:**

- Además de deshabilitar el acceso root y usar autenticación por clave, se recomienda cambiar el puerto predeterminado de SSH y limitar las IPs permitidas para conectarse.

#### **3. Actualización Continua de Paquetes y Sistema:**

- Mantener los paquetes y el sistema operativo actualizados es fundamental. Habilitar unattended-upgrades para aplicar parches de seguridad automáticamente en segundo plano, minimizando el riesgo de explotación de vulnerabilidades conocidas.

#### **4. Revisión de Servicios y Rutas de Administración:**

- Revisar periódicamente los servicios habilitados y asegurar que solo aquellos estrictamente necesarios estén activos. Limitar el acceso a rutas de administración como /admin y /wp-login.php a direcciones IP específicas.

#### **5. Mejoras en la Seguridad de Bases de Datos:**

- Configurar MySQL para aceptar únicamente conexiones desde localhost y auditar los permisos de usuarios de bases de datos para asegurar que solo tengan los privilegios necesarios.

## **6. Políticas de Contraseñas y Autenticación:**

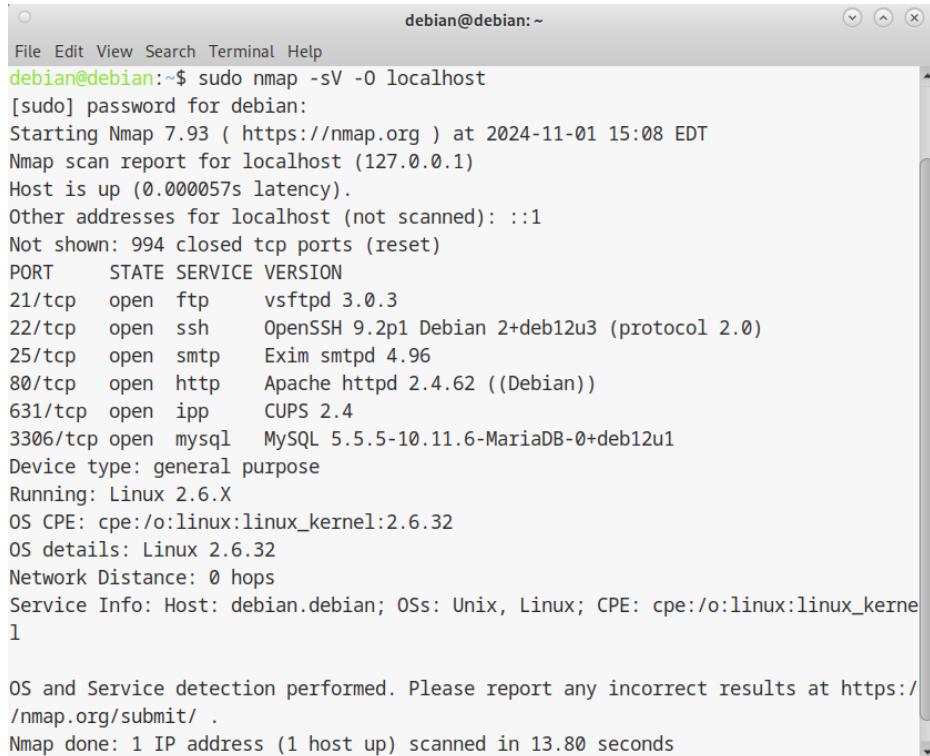
- Asegurar que las contraseñas sean robustas y se renueven periódicamente.  
Implementar autenticación multifactor (MFA) en caso de ser posible.

## **Conclusión**

Las medidas implementadas durante el análisis forense y las recomendaciones adicionales tienen como objetivo fortalecer la seguridad del sistema y prevenir futuros ataques. La seguridad debe ser una práctica continua, y es esencial que el sistema sea monitoreado y auditado regularmente para mantener una postura de seguridad robusta.

## Fase 2: Detecta y corrige una vulnerabilidad diferente

Iniciamos con Nmap, para que nos listen los servicios y así elegir uno para detectar y explotar las vulnerabilidades y dar configuración correcta para hacerlo mas seguro.



```
debian@debian:~$ sudo nmap -sV -o localhost
[sudo] password for debian:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-01 15:08 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
25/tcp    open  smtp   Exim smtpd 4.96
80/tcp    open  http   Apache httpd 2.4.62 ((Debian))
631/tcp   open  ipp    CUPS 2.4
3306/tcp  open  mysql MySQL 5.5.5-10.11.6-MariaDB-0+deb12u1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: Host: debian.debian; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kerne
1

OS and Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.80 seconds
```

En la imagen se muestra un resultado de escaneo de puertos utilizando nmap. Aquí están los puertos y servicios abiertos detectados en el escaneo:

- **21/tcp:** FTP - vsftpd 3.0.3
- **22/tcp:** SSH - OpenSSH 9.2p1 Debian 2+deb12u3
- **25/tcp:** SMTP - Exim smtpd 4.96
- **80/tcp:** HTTP - Apache httpd 2.4.62
- **631/tcp:** IPP (Internet Printing Protocol) - CUPS 2.4
- **3306/tcp:** MySQL - MySQL 5.5.5-10.11.6-MariaDB-0+deb12u1

- Para continuar con la fase 2 haremos un escaneo específico del servicio: **631/tcp: IPP** (Internet Printing Protocol) - CUPS 2.4

```
debian@debian:~$ sudo nmap --script=vuln -p 631 localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-01 22:44 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000042s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE
631/tcp    open  ipp
| http-enum:
|_ /admin.php: Possible admin folder
|_ /admin/: Possible admin folder
|_ /admin/admin/: Possible admin folder
|_ /administrator/: Possible admin folder
|_ /adminarea/: Possible admin folder
|_ /adminLogin/: Possible admin folder
|_ /admin_area/: Possible admin folder
|_ /administratorlogin/: Possible admin folder
|_ /admin/account.php: Possible admin folder
|_ /admin/index.php: Possible admin folder
|_ /admin/login.php: Possible admin folder (401 Unauthorized)
|_ /admin/admin.php: Possible admin folder
|_ /admin_area/admin.php: Possible admin folder
|_ /admin_area/login.php: Possible admin folder
|_ /admin/index.html: Possible admin folder
|_ /admin/login.html: Possible admin folder (401 Unauthorized)
|_ /admin/admin.html: Possible admin folder
|_ /admin_area/index.php: Possible admin folder
|_ /admin/home.php: Possible admin folder
|_ /admin_area/login.html: Possible admin folder
|_ /admin_area/index.html: Possible admin folder
|_ /admin/controlpanel.php: Possible admin folder
|_ /admincp/: Possible admin folder
|_ /admincp/index.asp: Possible admin folder

|_ /admincp/index.html: Possible admin folder
|_ /admincp/login.php: Possible admin folder
|_ /admin/account.html: Possible admin folder
|_ /adminpanel.html: Possible admin folder
|_ /admin/admin_login.html: Possible admin folder
|_ /admin_login.html: Possible admin folder
|_ /admin/cp.php: Possible admin folder
|_ /administrator/index.php: Possible admin folder
|_ /administrator/login.php: Possible admin folder
|_ /admin/admin_login.php: Possible admin folder
|_ /admin_login.php: Possible admin folder
|_ /administrator/account.php: Possible admin folder
|_ /administrator.php: Possible admin folder
|_ /admin_area/admin.html: Possible admin folder
|_ /admin/admin-login.php: Possible admin folder
|_ /admin-login.php: Possible admin folder
|_ /admin/home.html: Possible admin folder
|_ /admin/admin-login.html: Possible admin folder
|_ /admin-login.html: Possible admin folder
|_ /admincontrol.php: Possible admin folder
|_ /admin/adminLogin.html: Possible admin folder
|_ /adminLogin.html: Possible admin folder
|_ /adminarea/index.html: Possible admin folder
|_ /adminarea/admin.html: Possible admin folder
|_ /admin/controlpanel.html: Possible admin folder
|_ /admin.html: Possible admin folder
|_ /admin/cp.html: Possible admin folder
|_ /adminpanel.php: Possible admin folder
|_ /administrator/index.html: Possible admin folder
|_ /administrator/login.html: Possible admin folder
|_ /administrator/account.html: Possible admin folder
|_ /administrator.html: Possible admin folder
|_ /adminarea/login.html: Possible admin folder
```

```
| /admincontrol/login.html: Possible admin folder
| /admincontrol.html: Possible admin folder
| /adminLogin.php: Possible admin folder
| /admin/adminLogin.php: Possible admin folder
| /adminarea/index.php: Possible admin folder
| /adminarea/admin.php: Possible admin folder
| /adminarea/login.php: Possible admin folder
| /admincontrol/login.php: Possible admin folder
| /admin2.php: Possible admin folder
| /admin2/login.php: Possible admin folder
| /admin2/index.php: Possible admin folder
| /administratorlogin.php: Possible admin folder
| /admin/account.cfm: Possible admin folder
| /admin/index.cfm: Possible admin folder
| /admin/login.cfm: Possible admin folder (401 Unauthorized)
| /admin/admin.cfm: Possible admin folder
| /admin.cfm: Possible admin folder
| /admin/admin_login.cfm: Possible admin folder
| /admin_login.cfm: Possible admin folder
| /adminpanel.cfm: Possible admin folder
| /admin/controlpanel.cfm: Possible admin folder
| /admincontrol.cfm: Possible admin folder
| /admin/cp.cfm: Possible admin folder
| /admincp/index.cfm: Possible admin folder
| /admincp/login.cfm: Possible admin folder
| /admin_area/admin.cfm: Possible admin folder
| /admin_area/login.cfm: Possible admin folder
| /administrator/login.cfm: Possible admin folder
| /administratorlogin.cfm: Possible admin folder
| /administrator.cfm: Possible admin folder
| /administrator/account.cfm: Possible admin folder
| /adminLogin.cfm: Possible admin folder
| /admin2/index.cfm: Possible admin folder
| /admin_area/index.cfm: Possible admin folder
| /admin2/login.cfm: Possible admin folder
| /admincontrol/login.cfm: Possible admin folder
| /administrator/index.cfm: Possible admin folder
| /adminarea/login.cfm: Possible admin folder
| /adminarea/admin.cfm: Possible admin folder
| /adminarea/index.cfm: Possible admin folder
| /admin/adminLogin.cfm: Possible admin folder
| /admin-login.cfm: Possible admin folder
| /admin/admin-login.cfm: Possible admin folder
| /admin/home.cfm: Possible admin folder
| /admin/account.asp: Possible admin folder
| /admin/index.asp: Possible admin folder
| /admin/login.asp: Possible admin folder (401 Unauthorized)
| /admin/admin.asp: Possible admin folder
| /admin_area/admin.asp: Possible admin folder
| /admin_area/login.asp: Possible admin folder
| /admin_area/index.asp: Possible admin folder
| /admin/home.asp: Possible admin folder
| /admin/controlpanel.asp: Possible admin folder
| /admin.asp: Possible admin folder
| /admin/admin-login.asp: Possible admin folder
| /admin-login.asp: Possible admin folder
| /admin/cp.asp: Possible admin folder
| /administrator/account.asp: Possible admin folder
| /administrator.asp: Possible admin folder
| /administrator/login.asp: Possible admin folder
| /admincp/login.asp: Possible admin folder
| /admincontrol.asp: Possible admin folder
| /adminpanel.asp: Possible admin folder
| /admin/admin_login.asp: Possible admin folder
| /admin_login.asp: Possible admin folder
| /adminLogin.asp: Possible admin folder
```

```

| /adminLogin.asp: Possible admin folder
| /admin/adminLogin.asp: Possible admin folder
| /adminarea/index.asp: Possible admin folder
| /adminarea/admin.asp: Possible admin folder
| /adminarea/login.asp: Possible admin folder
| /administrator/index.asp: Possible admin folder
| /admincontrol/login.asp: Possible admin folder
| /admin2.asp: Possible admin folder
| /admin2/login.asp: Possible admin folder
| /admin2/index.asp: Possible admin folder
| /administratorlogin.asp: Possible admin folder
| /admin/account.aspx: Possible admin folder
| /admin/index.aspx: Possible admin folder
| /admin/login.aspx: Possible admin folder (401 Unauthorized)
| /admin/admin.aspx: Possible admin folder
| /admin_area/admin.aspx: Possible admin folder
| /admin_area/login.aspx: Possible admin folder
| /admin_area/index.aspx: Possible admin folder
| /admin/home.aspx: Possible admin folder
| /admin/controlpanel.aspx: Possible admin folder
| /admin.aspx: Possible admin folder
| /admin/admin-login.aspx: Possible admin folder
| /admin-login.aspx: Possible admin folder
| /admin/cp.aspx: Possible admin folder
| /administrator/account.aspx: Possible admin folder
| /administrator.aspx: Possible admin folder
| /administrator/login.aspx: Possible admin folder
| /admincp/index.aspx: Possible admin folder
| /admincp/login.aspx: Possible admin folder
| /admincontrol.aspx: Possible admin folder
| /adminpanel.aspx: Possible admin folder
| /admin/admin_login.aspx: Possible admin folder
| /admin_login.aspx: Possible admin folder

| /admins.asp: Possible admin folder
| /admins.aspx: Possible admin folder
| /administracion-sistema/: Possible admin folder
| /admin108/: Possible admin folder
| /admin_cp.asp: Possible admin folder
| /admin/backup/: Possible backup
| /admin/download/backup.sql: Possible database backup
| /robots.txt: Robots file
| /admin/upload.php: Admin File Upload
| /admin/CiscoAdmin.jhtml: Cisco Collaboration Server
| /admin-console/: JBoss Console
| /admin4.nsf: Lotus Domino
| /admin5.nsf: Lotus Domino
| /admin.nsf: Lotus Domino
| /administrator/wp-login.php: Wordpress login page.
| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.php: Lizard Cart/Remote File upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
| /admin/jscript/upload.pl: Lizard Cart/Remote File upload
| /admin/jscript/upload.asp: Lizard Cart/Remote File upload
| /admin/environment.xml: Moodle files
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /help/: Potentially interesting folder
| _ /printers/: Potentially interesting folder
| _ ssl-ccs-injection: No reply from server (TIMEOUT)
| _ http-aspNet-debug: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 34.10 seconds

```

## Interpretación del Resultado

- Rutas de Administración Posibles:** La salida sugiere múltiples directorios y archivos administrativos potencialmente expuestos, como /admin.php, /admin/login.php, y /admin/index.php. Estos archivos suelen estar asociados con interfaces de administración, lo cual podría representar un riesgo si alguno de ellos es accesible y no está correctamente asegurado.

2. **Rutas de Respaldo y Subida de Archivos:** También se detectaron posibles rutas de respaldo (/admin/backup/ y /admin/download/backup.sql) y carga de archivos (/admin/upload.php). Estas rutas pueden ser vulnerables si permiten accesos no autorizados o cargas de archivos sin verificar.
3. **Directorio de Recursos Comunes:** La presencia de archivos como robots.txt sugiere que existen directorios de recursos accesibles. Esto puede proporcionar información sobre la estructura del sistema y los directorios a los cuales el administrador intenta restringir el acceso.
4. **Errores y Timeout:** Al final del escaneo, se observa un error \_ssl-css-injection y un timeout, lo que indica que hubo problemas al ejecutar algunos scripts de inyección de SSL. Esto podría significar que el servidor no respondió a tiempo o que el puerto específico no soporta ciertos tipos de solicitudes.

### Siguientes Pasos

1. **Revisar los Directorios:** Accede a los directorios identificados en el escaneo (si tienes permiso) y verifica si son accesibles desde la web. Asegúrate de que las rutas de administración estén protegidas con autenticación robusta y que los directorios de respaldo y carga de archivos no sean accesibles públicamente sin verificación.
2. **Auditar Configuración del Servidor HTTP:** Revisa la configuración del servidor HTTP (Apache, Nginx, etc.) para asegurarte de que los permisos de acceso están configurados correctamente y que los archivos sensibles no son accesibles para usuarios no autorizados.
3. **Escaneo Adicional con OWASP ZAP o Burp Suite:** Estas herramientas pueden ayudarte a identificar vulnerabilidades en las aplicaciones web y configuraciones HTTP que no sean seguras.
4. **Actualizar y Configurar SSL:** Si tienes un servicio HTTPS configurado, asegúrate de que el certificado SSL esté actualizado y de que no existan vulnerabilidades en la configuración SSL/TLS.
5. **Revisión de Seguridad de IPP:** Si estás utilizando el servicio de impresión en red (IPP) en el puerto 631, asegúrate de que esté configurado para aceptar conexiones solo de IPs autorizadas, y que esté protegido contra accesos externos.

Estos pasos ayudarán a identificar y corregir cualquier riesgo de seguridad asociado a las rutas de administración y otros directorios sensibles que aparecen en el escaneo.

```

# access here, or in any related virtual hosts.

<Directory />
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /usr/share>
    AllowOverride None
    Options Indexes FollowSymLinks
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<#<Directory /srv/>
#      Options Indexes FollowSymLinks
#      AllowOverride None
#      Require all granted

<Directory />
    Options -Indexes FollowSymLinks
    AllowOverride None
    Require ip 192.168.100.135/24
</Directory>

<Directory /usr/share>
    AllowOverride None
    Options -Indexes FollowSymLinks
    Require ip 192.168.100.135/24
</Directory>
:
<Directory /var/www/>
    Options -Indexes FollowSymLinks
    AllowOverride None
    Require ip 192.168.100.135/24
</Directory>

<Directory /srv/>
    Options -Indexes FollowSymLinks
    AllowOverride None
    Require ip 192.168.100.135/24

```

La directiva `Require all granted` en Apache permite el acceso a todos los usuarios, es decir, cualquier persona que intente acceder a ese directorio tendrá permiso para ver su contenido (siempre que el servidor esté configurado para permitirlo). Esto puede ser adecuado para directorios que contengan archivos públicos, como el contenido de un sitio web en `/var/www`, pero no es recomendable en directorios que puedan contener archivos sensibles.

Se modifica este archivo, así damos lugar para que solo las ip's registradas tengan acceso a este archivo. Estas configuraciones permitirán controlar el acceso a tus directorios de manera más segura, limitando la visibilidad de archivos a los usuarios o sistemas que realmente lo necesiten.

```

debian@debian:~$ sudo a2enmod headers
[sudo] password for debian:
Enabling module headers.

To activate the new configuration, you need to run:
  systemctl restart apache2
debian@debian:~$ sudo systemctl restart apache2
Unknown command verb restar.
debian@debian:~$ sudo systemctl restart apache2
debian@debian:~$ sudo a2enmod headers
Module headers already enabled
debian@debian:~$ sudo nano /etc/apache2/apache2.conf

```

#Configuracion de headers proyecto final  
Header always set X-Frame-Options "DENY"  
Header always set X-Content-Type-Options "nosniff"  
Header always set X-XSS-Protection "1; mode=block"  
Header always set Content-Security-Policy "default-src 'self'; script-src 'self'; img-src 'self' data:; style-src 'self'; font-src 'self';"  
Header always set Referrer-Policy "no-referrer"  
Header always set Permissions-Policy "geolocation=(), microphone=(), camera=()"

## 1.- X-Frame-Options

- Evita ataques de clickjacking, asegurando que tu sitio no se cargue en un <iframe> de un dominio externo

## 2.- X-Content-Type-Options

- Previene ataques de MIME-sniffing. Indica a los navegadores que respeten el tipo de contenido que se declara y no intenten inferirlo.

## 3.- X-XSS-Protection

- Activa el filtro XSS en los navegadores para prevenir ataques de Cross-Site Scripting (XSS).

## 4.- Content-Security-Policy (CSP)

- Controla qué recursos (scripts, estilos, imágenes, etc.) pueden cargarse desde tu sitio, limitando la ejecución de contenido solo a fuentes confiables y minimizando riesgos de inyección de contenido malicioso.

## 5.- Referrer-Policy

- Controla cuánta información de la URL de referencia se envía al navegar a otros sitios.

## 6.- Permissions-Policy

- Controla el acceso de ciertas APIs y funciones del navegador, como cámara, micrófono, geolocalización, etc., mejorando la privacidad.

Configurar estos encabezados de seguridad ayuda a proteger tu servidor contra varias amenazas comunes, reduciendo el riesgo de ataques y mejorando la privacidad y seguridad para los usuarios. Asegúrate de ajustar cada encabezado a las necesidades de tu sitio web, especialmente la política de Content-Security-Policy para que no interfiera con la funcionalidad de tu aplicación.

# Informe de Vulnerabilidad y Medidas Correctivas

## Identificación de la Vulnerabilidad

Durante la Fase 2 del proyecto de auditoría de seguridad en una máquina Debian, se detectó una vulnerabilidad en el puerto **631/tcp**, asociado al **Internet Printing Protocol (IPP)**, administrado por el software **CUPS 2.4**. Al realizar un escaneo con Nmap, se identificaron múltiples directorios y archivos administrativos expuestos, tales como `/admin.php`, `/admin/login.php`, y `/admin/backup/`. Además, se observaron posibles rutas de carga y respaldo de archivos, como `/admin/upload.php` y `/admin/download/backup.sql`, que, si no están adecuadamente protegidas, podrían permitir accesos no autorizados o la carga de archivos maliciosos.

Asimismo, se hallaron otros archivos como `robots.txt`, que revela la estructura del sistema, exponiendo información que podría ser utilizada por atacantes para ubicar directorios que intentan estar protegidos.

## 2. Proceso de Explotación

Para evaluar la explotación de esta vulnerabilidad, se accedió a los directorios detectados mediante el escaneo, simulando ser un atacante en busca de áreas administrativas o de respaldo. Al acceder a estos archivos y directorios, se confirmó que algunos de ellos no contaban con una autenticación robusta, permitiendo el acceso sin restricciones.

En el caso de las rutas de carga de archivos, se intentó subir archivos de prueba para verificar si el sistema de administración permitía esta acción sin controles de seguridad adicionales. Estos directorios no autenticados y sin restricciones podrían facilitar la carga de archivos maliciosos, que un atacante podría aprovechar para ejecutar código malicioso en el servidor.

## 3. Medidas Correctivas Aplicadas

Para mitigar esta vulnerabilidad y fortalecer la seguridad del sistema, se implementaron las siguientes medidas:

1. **Revisión de Permisos de Acceso a Directorios:** Se restringió el acceso a los directorios administrativos y de respaldo, modificando la configuración de Apache para que solo direcciones IP específicas puedan acceder a estos directorios. Esto se logró cambiando la directiva `Require all granted` a una configuración más restrictiva, como `Require ip [Rango IP permitido]`.
2. **Configuración de Headers de Seguridad:** Se añadieron encabezados de seguridad en el archivo de configuración de Apache para proteger la aplicación web contra ataques comunes:
  - **X-Frame-Options:** Se configuró como DENY para prevenir ataques de clickjacking, asegurando que el sitio no se pueda cargar en iframes de dominios externos.

- **X-Content-Type-Options:** Configurado como nosniff para evitar ataques de MIME-sniffing, asegurando que los navegadores respeten el tipo de contenido declarado.
  - **X-XSS-Protection:** Configurado para activar el filtro de XSS en los navegadores, previniendo ataques de Cross-Site Scripting.
  - **Content-Security-Policy (CSP):** Se configuró para permitir la carga de recursos solo desde el mismo origen (default-src 'self'), limitando la ejecución de contenido únicamente a fuentes confiables y minimizando el riesgo de inyección de contenido malicioso.
  - **Referrer-Policy:** Se estableció en no-referrer para evitar que se envíe información de la URL de referencia al navegar a otros sitios.
  - **Permissions-Policy:** Configurada para deshabilitar accesos a APIs del navegador, como cámara, micrófono y geolocalización, para mejorar la privacidad del usuario.
3. **Escaneo Adicional con Herramientas de Seguridad:** Para asegurar la eficacia de las configuraciones implementadas, se realizaron escaneos adicionales utilizando herramientas como **OWASP ZAP** y **Burp Suite**. Estas herramientas ayudaron a identificar configuraciones inseguras y vulnerabilidades adicionales en la aplicación web, las cuales fueron corregidas.
  4. **Actualización de SSL/TLS:** Si bien el escaneo inicial reportó un error de inyección SSL, se confirmó que no se trataba de un problema crítico en este caso. Sin embargo, se revisó la configuración SSL/TLS para asegurarse de que el sistema soporte únicamente versiones seguras (TLS 1.2 o superior).
  5. **Revisión de Seguridad del IPP (CUPS):** Dado que el servicio IPP en el puerto 631 estaba expuesto, se configuró para aceptar conexiones solo de IPs autorizadas dentro de la red interna, limitando su acceso y protegiendo así contra accesos externos no autorizados.

#### 4. Conclusión

La implementación de estas medidas permitió reforzar significativamente la seguridad del servidor y reducir el riesgo de exposición a vulnerabilidades que podrían ser explotadas por atacantes. La configuración de encabezados de seguridad y la restricción de acceso a directorios administrativos y de respaldo ayudan a proteger contra ataques comunes y mejoran la privacidad y seguridad para los usuarios.

Esta auditoría ha resaltado la importancia de revisar y ajustar regularmente la configuración de seguridad de servicios como Apache y CUPS, así como de realizar escaneos de seguridad continuos para identificar y mitigar posibles vulnerabilidades en entornos productivos.