

Informe Técnico de Respuesta a Incidente

Título: Análisis y mitigación de ataque en servidor Linux (debian) con WordPress

Fecha de elaboración: 9 de junio de 2025

Responsable del análisis: Alan Alvarado Ramírez

1. Resumen del incidente

Durante la revisión de los registros del sistema y servicios críticos, se detectó actividad anómala atribuida a un usuario sin privilegios root que intentó ejecutar comandos con sudo, alterando y eliminando procesos y archivos. También se detectaron configuraciones débiles en WordPress, FTP y SSH, así como usuarios MySQL con contraseñas vulnerables.

2. Análisis técnico

1. Detección de comandos sospechosos con SUDO

- Se ejecutó:

`journalctl | grep "sudo" | grep "COMMAND="`
- Resultado: se detectaron intentos de escalación de privilegios y eliminación de procesos por un usuario sin permisos.

```
Applications Places System
debian@debian: /var/log
File Edit View Search Terminal Help
Oct 08 16:08:57 debian sudo[4687]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install vsftpd
Oct 08 16:09:38 debian sudo[4886]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/vsftpd.conf
Oct 08 16:10:37 debian sudo[5045]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart vsftpd
Oct 08 16:12:13 debian sudo[5104]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install openssh-server
Oct 08 16:12:55 debian sudo[5157]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
Oct 08 16:14:16 debian sudo[5335]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart ssh
Oct 08 16:14:59 debian sudo[5376]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install net-tools
Oct 08 16:15:16 debian sudo[5442]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/netstat -tuln
Oct 08 16:16:37 debian sudo[5480]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/ls -l /var/www/html
Oct 08 16:17:59 debian sudo[5532]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod -R 777 /var/www/html
Oct 08 16:20:04 debian sudo[5592]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod 777 /var/www/html/wp-config.php
Oct 08 16:21:23 debian sudo[5646]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/apache2/apache2.conf
Oct 08 16:24:30 debian sudo[5975]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart apache2
```

```
Sep 30 11:57:49 debian sudo[38553]:  debian : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/chown -R www-data:www-data /var/www/html/
Sep 30 11:58:23 debian sudo[38598]:  debian : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/chmod -R 755 /var/www/html/
Sep 30 11:59:38 debian sudo[38666]:  debian : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/mv wp-config-sample.php wp-config.php
Sep 30 12:00:08 debian sudo[38693]:  debian : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/nano wp-config.php
Sep 30 12:05:46 debian sudo[39731]:  debian : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/systemctl restart apache2
Sep 30 12:06:00 debian sudo[39831]:  debian : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/systemctl status apache2
Sep 30 12:11:37 debian sudo[40186]:  debian : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/apt install php libapache2-mod-php php-mysql php-gd php-xml php-mbstring php-curl -y
Sep 30 12:15:25 debian sudo[50261]:  debian : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/nano /etc/apache2/sites-available/000-default.conf
Sep 30 12:18:19 debian sudo[50495]:  debian : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/nano /etc/apache2/sites-available/000-default.conf
Sep 30 12:19:00 debian sudo[50603]:  debian : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/systemctl restart apache2
Sep 30 12:19:23 debian sudo[50659]:  debian : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/nano /var/www/html/info.php
```

2. Revisión de inicios de sesión con SUDO

- Comandos:

journalctl | grep "sudo"
sudo passwd root

- Resultado: confirmación de intentos no autorizados y se cambia la contraseña de root por una más fuerte.

```
debian@debian: ~/Desktop
File Edit View Search Terminal Help
Sep 30 15:37:17 debian sudo[4195]: pam_unix(sudo:session): session closed for user root
Sep 30 15:37:33 debian sudo[4228]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl status m
ariadb
Sep 30 15:37:33 debian sudo[4228]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:07:47 debian sudo[4228]: pam_unix(sudo:session): session closed for user root
Oct 08 16:08:57 debian sudo[4687]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install vsftpd
Oct 08 16:08:57 debian sudo[4687]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:09:02 debian sudo[4687]: pam_unix(sudo:session): session closed for user root
Oct 08 16:09:38 debian sudo[4886]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/vsftpd.c
onf
Oct 08 16:09:38 debian sudo[4886]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:10:12 debian sudo[4886]: pam_unix(sudo:session): session closed for user root
Oct 08 16:10:37 debian sudo[5045]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart
vsftpd
```

```
debian@debian:/var/www/html$ sudo su
root@debian:/var/www/html# passwd
New password:
Retype new password:
passwd: password updated successfully
root@debian:/var/www/html#
```

3. Búsqueda de rootkits

- Herramientas y comandos utilizados:

chkrootkit
rkhunter --check

- Resultado: no se encontraron rootkits activos.

```
debian@debian: ~/Desktop
File Edit View Search Terminal Help
Searching for Adore LKM... not tested
Searching for sebek LKM (Adore based)... not tested
Searching for knark LKM rootkit... not found
Searching for for hidden processes with chkproc... not found
Searching for for hidden directories using chkdirs... not found
Checking 'lkm'... finished
Checking 'revokedcs'... not found
Checking 'sniffer'... WARNING

WARNING: Output from ifpromisc:
lo: not promise and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[492])

Checking 'w55808'... not found
Checking 'wtet'... not found
Checking 'scalper'... not found
Checking 'slapper'... not found
Checking 'z2'... not found
Checking 'chkutmp'... not found
Checking 'OSX_RSPLUG'... not tested
debian@debian:~/Desktop$ sudo chkrootkit
```

```
debian@debian:~$ sudo rkhunter --check
[sudo] password for debian:
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables [ None found ]
Checking for preloaded libraries [ None found ]
Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
Checking for prerequisites [ OK ]
/usr/sbin/adduser [ OK ]
/usr/sbin/chroot [ OK ]
/usr/sbin/cron [ OK ]
/usr/sbin/depmod [ OK ]
/usr/sbin/fsck [ OK ]
/usr/sbin/insmod [ OK ]
```

4. Análisis de WordPress (wp-config.php)

- Se detectó una contraseña débil del usuario wordpressuser.
- Acción tomada:
 - Cambio del usuario y contraseña en wp-config.php.
 - Refuerzo de la contraseña con criterios seguros.

```
debian@debian: /var/www/html
GNU nano 7.2 wp-config.php
* @package WordPress
*/

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wordpressuser' );

/** Database password */
define( 'DB_PASSWORD', '123456' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```

define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wpusernew' );

/** Database password */
define( 'DB_PASSWORD', 'Jh7yt5GG13' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

```

5. Revisión de privilegios en MySQL

- Comando:

SHOW GRANTS FOR 'wordpressuser'@'localhost';

- Resultado: el usuario tenía ALL PRIVILEGES sobre la base de datos.
- Acción: el usuario fue eliminado.

```

MariaDB [(none)]> SELECT User, Host, plugin FROM mysql.user;
+-----+-----+-----+
| User          | Host      | plugin                |
+-----+-----+-----+
| mariadb.sys   | localhost | mysql_native_password |
| root          | localhost | mysql_native_password |
| mysql         | localhost | mysql_native_password |
| wordpressuser | localhost | mysql_native_password |
| user          | localhost | mysql_native_password |
+-----+-----+-----+
5 rows in set (0.101 sec)

MariaDB [(none)]> SHOW GRANTS FOR 'wordpress'@'localhost';
ERROR 1141 (42000): There is no such grant defined for user 'wordpress' on host 'localhost'
MariaDB [(none)]> SHOW GRANTS FOR 'wordpressuser'@'localhost';
+-----+-----+-----+
| Grants for wordpressuser@localhost |
+-----+-----+-----+
| GRANT USAGE ON *.* TO 'wordpressuser'@'localhost' IDENTIFIED BY PASSWORD '*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9' |
| GRANT ALL PRIVILEGES ON 'wordpress'.* TO 'wordpressuser'@'localhost' |
+-----+-----+-----+
2 rows in set (0.003 sec)

MariaDB [(none)]>

```

```
MariaDB [(none)]> SELECT User , Host FROM mysql.user;
+-----+-----+
| User      | Host      |
+-----+-----+
| mariadb.sys | localhost |
| mysql      | localhost |
| root       | localhost |
| user       | localhost |
| wordpressuser | localhost |
+-----+-----+
5 rows in set (0.026 sec)

MariaDB [(none)]> DROP USER 'wordpressuser'@'localhost';
Query OK, 0 rows affected (0.079 sec)

MariaDB [(none)]> SELECT User, Host FROM mysql.user WHERE User = 'wordpressuser';
Empty set (0.006 sec)
```

6. Auditoría de hashes de contraseñas MySQL

- Comando:

```
SELECT User, Host, plugin, authentication_string FROM mysql.user;
```

- Herramienta de auditoría: hashes.com (ya que mysql usa doble cifrado y john the ripper no puede descifrarlas).
- Resultado: se descifraron varias contraseñas, confirmando que eran débiles.
- Acción: recomendación de fortalecer políticas de contraseñas y rotarlas periódicamente.

```
MariaDB [(none)]> SELECT User, Host, plugin, authentication_string FROM mysql.user;
+-----+-----+-----+-----+
| User      | Host      | plugin                | authentication_string |
+-----+-----+-----+-----+
| mariadb.sys | localhost | mysql_native_password |                       |
| root       | localhost | mysql_native_password | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql      | localhost | mysql_native_password | invalid               |
| user       | localhost | mysql_native_password | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+-----+-----+-----+-----+
4 rows in set (0.019 sec)
```

✓ Encontrado:

```
2470c0c06dee42fd1618bb99005adca2ec9d1e19:password:MYSQL5
```

```
6bb4837eb74329105ee4568dda7dc67ed2ca2ad9:123456:MYSQL5
```

7. Revisión de configuración FTP

- Archivo revisado:

/etc/vsftpd.conf

- Problema: acceso anónimo habilitado.
- Acción: acceso anónimo deshabilitado.

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

8. Revisión de configuración SSH

- Archivo revisado:

/etc/ssh/sshd_config

- Problemas:
 - Autenticación por contraseña habilitada.
 - Login como root habilitado.
- Acción: ambas opciones desactivadas y se migró a autenticación con llave SSH.

```
# Authentication:

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

#PubkeyAuthentication yes
```

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

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

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

9. Actualización del sistema

- Comandos ejecutados:

```
sudo apt update  
sudo apt upgrade -y  
sudo apt full-upgrade
```

- Resultado: sistema actualizado con los últimos parches de seguridad.

```
Removing linux-image-6.1.0-23-amd64 (6.1.99-1) ...  
/etc/kernel/postrm.d/initramfs-tools:  
update-initramfs: Deleting /boot/initrd.img-6.1.0-23-amd64  
/etc/kernel/postrm.d/zz-update-grub:  
Generating grub configuration file ...  
Found background image: /usr/share/images/desktop-base/desktop-grub.png  
Found linux image: /boot/vmlinuz-6.1.0-37-amd64  
Found initrd image: /boot/initrd.img-6.1.0-37-amd64  
Found linux image: /boot/vmlinuz-6.1.0-25-amd64  
Found initrd image: /boot/initrd.img-6.1.0-25-amd64  
Warning: os-prober will not be executed to detect other bootable partitions.  
Systems on them will not be added to the GRUB boot configuration.  
Check GRUB_DISABLE_OS_PROBER documentation entry.  
done  
debian@debian:/var/www/html$
```

3. Medidas tomadas para mitigar el ataque

- Cierre del acceso SUDO al usuario sospechoso mediante un cambio de contraseña.
- Eliminación del usuario wordpressuser con permisos elevados.

- Reforzamiento de contraseñas en WordPress y MySQL.
- Desactivación del acceso anónimo por FTP y endurecimiento de su configuración.
- Desactivación del login por contraseña y del acceso root por SSH.
- Actualización completa del sistema.

4. Recomendaciones para prevenir futuros ataques

1. Implementar políticas de contraseñas fuertes a nivel de sistema y MySQL, que incluyan:
 - Longitud mínima de 12 caracteres.
 - Uso de mayúsculas, minúsculas, números y símbolos.
 - Cambios obligatorios de forma periódica.
2. Deshabilitar acceso SSH por contraseña y usar exclusivamente autenticación por llave pública.
3. Eliminar usuarios innecesarios en el sistema y en la base de datos.
4. Activar el plugin “validate_password” en MySQL para forzar contraseñas seguras.
5. Auditar regularmente archivos sensibles como wp-config.php, /etc/passwd, /etc/sudoers, etc.
6. Instalar y configurar fail2ban para bloquear intentos de fuerza bruta en SSH, FTP y WordPress.
7. Establecer respaldos automáticos y almacenarlos fuera del servidor.

8. Realizar escaneos periódicos de rootkits y malware con rkhunter y chkrootkit.
9. Revisar periódicamente los servicios en ejecución y cerrar puertos no utilizados.
10. Se debe realizar el control y monitoreo de usuarios privilegiados.