Informe Técnico de Seguridad: Análisis de Vulnerabilidades y Acciones Correctivas

Objetivo del Pentesting

Realizar un análisis integral de la seguridad del sistema con el propósito de identificar brechas, vulnerabilidades y configuraciones incorrectas susceptibles de explotación. El enfoque principal fue detectar y mitigar problemas derivados de la actividad del usuario debían ya que accedió mediante un ataque de fuerza bruta al tener una contraseña de seguridad muy débil y en consecuencia la escalamiento de privilegios y realizar modificaciones a su antojo y de manera más conveniente.

Vulnerabilidades Detectadas

Acceso No Autorizado a SSH

- Se detectó el uso de una contraseña débil para acceder al sistema a través del puerto 22.
- Riesgo: Permite acceso remoto no autorizado con privilegios de superusuario (*root*).

Creación de Usuario con Privilegios Elevados

- El usuario debian fue creado con privilegios administrativos (*root* y *sudo*).
- Riesgo: Habilitó la ejecución sin restricciones de comandos críticos en el sistema.

Configuración Insegura en Apache

- Activación de scripts CGI, facilitando la ejecución de comandos en el servidor.
- Riesgo: Posibilidad de ejecución arbitraria de comandos que comprometen la seguridad.

Servicios Innecesarios y Puertos Abiertos

- Presencia de servicios como speech-dispatcher, configurados de manera insegura o detenidos. Los puertos 21 (FTP) y 80 (HTTP) estaban abiertos sin justificación.
- Riesgo: Exposición de servicios innecesarios, aumentando la superficie de ataque.

Falta de Segmentación de Red

- Tráfico interno no segmentado, con una red única para servidores y estaciones de trabajo.
- Riesgo: Alta probabilidad de propagación rápida de amenazas dentro de la red.

Informe de Incidente de Seguridad

Análisis Forense

- **Detección del Ataque:**
  Los registros de SSH evidenciaron accesos exitosos como root mediante credenciales comprometidas.

- **Acciones Maliciosas Detectadas:**
  - **Creación del usuario debían con privilegios administrativos.**
  - **Modificación de servicios y configuraciones de Apache.**
  - **Instalación de WordPress con posibles intenciones de explotación web.**
  - **Uso de scripts CGI para la ejecución de comandos.**

- **Impacto:**
  - **Compromiso de la confidencialidad, integridad y disponibilidad del sistema.**
  - **Posibilidad de escalación de privilegios y explotación de los distintos servicios para su beneficio propio.**

Acciones Correctivas Implementadas

1. **Eliminación del Usuario Comprometido:**

Eliminación del usuario debían y sus privilegios.

```
sudo deluser --remove-home debian

sudo groupdel debian
```

   ○

2. **Reconfiguración de SSH:**

Deshabilitación de acceso mediante contraseña y del inicio de sesión como *root*.

```
sudo nano /etc/ssh/sshd_config

PasswordAuthentication no

PermitRootLogin no

PubkeyAuthentication yes

sudo systemctl restart sshd
```

   ○

3. **Restauración de Apache:**

Desactivación de scripts CGI y restauración de permisos seguros.

```
sudo a2dismod cgi

sudo rm -rf /var/www/html/cgi-bin/*
```

   ○

4. **Cierre de Puertos Innecesarios:**

Restricción de acceso a servicios no esenciales mediante el firewall para bloquear por los puertos que accedió fácilmente UFW.

```
sudo ufw deny 21/tcp

sudo ufw deny 80/tcp
```

    -
5. **Escaneo y Limpieza de Malware:**

Detección y eliminación de archivos maliciosos con herramientas como rkhunter, chkrootkit y ClamAV.
bash

```
sudo rkhunter --check

sudo chkrootkit

sudo clamscan -r /
```

    -
6. **Restauración de Servicios Legítimos:**

    Reactivación de servicios esenciales y eliminación de configuraciones no autorizadas.

Medidas Preventivas Aplicadas

1. **Endurecimiento de Seguridad en SSH:**

    Implementación de autenticación basada únicamente en claves públicas.

    Restricción de acceso a usuarios específicos.

2. **Fortalecimiento de Contraseñas:**

Aplicación de políticas de contraseñas robustas mediante herramientas como validate password en MySQL.

```
sudo mysql_secure_installation
```

    -
3. **Firewall y Monitoreo de Red:**

Configuración de reglas estrictas en UFW para permitir únicamente tráfico esencial.

```
sudo ufw allow ssh

sudo ufw allow https

sudo ufw enable
```

    -
4. **Segmentación de la Red:**
    - **Creación de VLANs para separar servidores y estaciones de trabajo.**
    - **Implementación de firewalls internos para filtrar el tráfico entre segmentos.**
5. **Herramientas de Monitoreo:**
    - **Propuesta de implementación de sistemas IDS/IPS para detección de intrusiones en tiempo real.**

Plan de Recuperación en Caso de Incidencia

Objetivo:

Garantizar la continuidad operativa y la rápida recuperación ante futuros incidentes de seguridad, y evitar que cualquier tipo de información de nivel crítico e importante puede llegar a ser algo muy grande y difícil de remediar para ello implementaremos diferente medidas

1. **Identificación del Incidente:**

Monitoreo constante mediante herramientas SIEM e IDS.

2. **Contención:**

Aislar sistemas comprometidos y redirigir tráfico hacia servidores alternativos, y realizar las comprobaciones de los posibles sistemas que se han podido comprometer y causas para luego poder saber como realizar los cambios para recuperar la información.

3. **Erradicación:**

Eliminar malware, limpiar configuraciones afectadas y aplicar parches de seguridad.

4. **Restauración:**

Recuperar sistemas desde copias de seguridad verificadas y realizar pruebas exhaustivas, para ellos podemos realizarlo mediante una en la nube la cual nos garantiza un acceso más rápido y efectivo además de la seguridad que nos da.

5. **Aseguramiento de la Continuidad:**

Implementar redundancia en servicios críticos y configurar mecanismos de failover, añadir diferente metodos de verificación y alertas de los diferente cambios que se están realizan para poder actuar de la manera mas rápida posible.

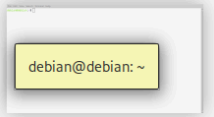
6. **Mejora Continua:**

Capacitación en ciberseguridad, revisiones regulares de seguridad y auditorías periódicas.

Conclusión

Las medidas correctivas implementadas fortalecieron significativamente la seguridad del sistema tras las acciones maliciosas provocadas por el usuario debian. Además, las medidas preventivas y el plan de recuperación mejoran la resistencia de la infraestructura ante futuros incidentes además de las nuevas y diferentes medidas que se pueden realizar para así resolver este de la manera más eficiente

```
sudo mysql -u root -p
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
curl -O https://wordpress.org/latest.tar.gz
tar xzvf latest.tar.gz
sudo cp -a /tmp/wordpress/. /var/www/html/
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
cd /var/www/html/
sudo mv wp-config-sample.php wp-config.php
sudo nano wp-config.php
ip a
sudo systemctl restart apache2
sudo systemctl status apache2
sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring php-curl -y
cd ..
sudo nano /etc/apache2/sites-available/000-default.conf
sudo systemctl restart apache2
sudo nano /var/www/html/info.php
ls /var/www/html
sudo apt install openssh-server -y
sudo systemctl start ssh
sudo systemctl enable ssh
sudo systemctl status ssh
sudo systemctl start apache2
debian@debian:~$ S
```




```
[17:09:40] Rootkits checked : 497
debian@debian:~$ sudo journalctl -u
-- No entries --
debian@debian:~$
```

```
System checks summary
=====================

File properties checks...
    Files checked: 144
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 7

Applications checks...
    All checks skipped

The system checks took: 1 minute and 38 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

debian@debian:~$
```

```
debian@debian:~$ : not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[486], /usr/sbin/NetworkManager[486)
```

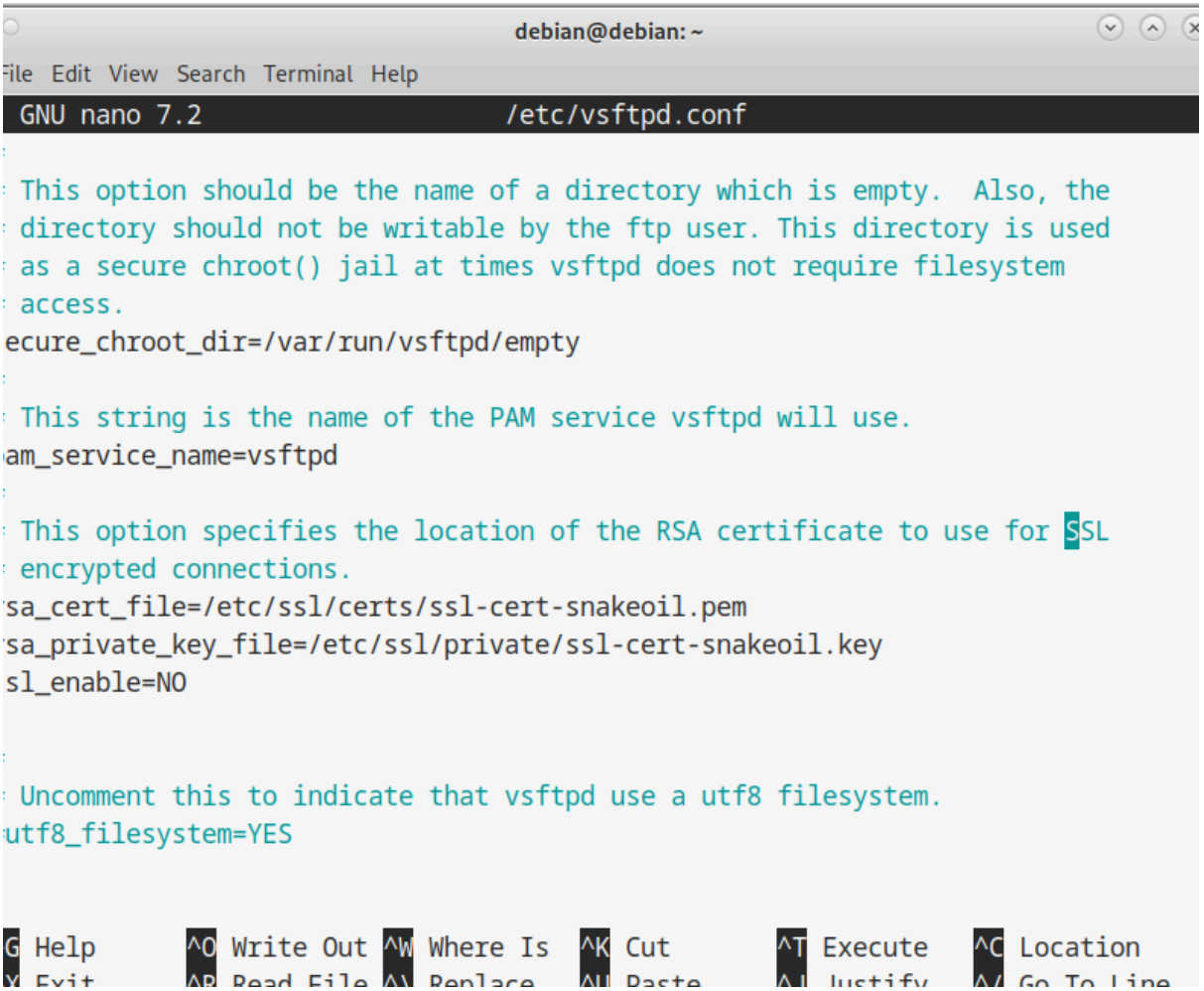
```
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0057s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.94 seconds
debian@debian:~$
```

```
debian@debian:~$ ps aux | grep sniffer
debian    147500  0.0  0.1   6332  2044 pts/4    S+   17:03   0:00 grep sniffer
```

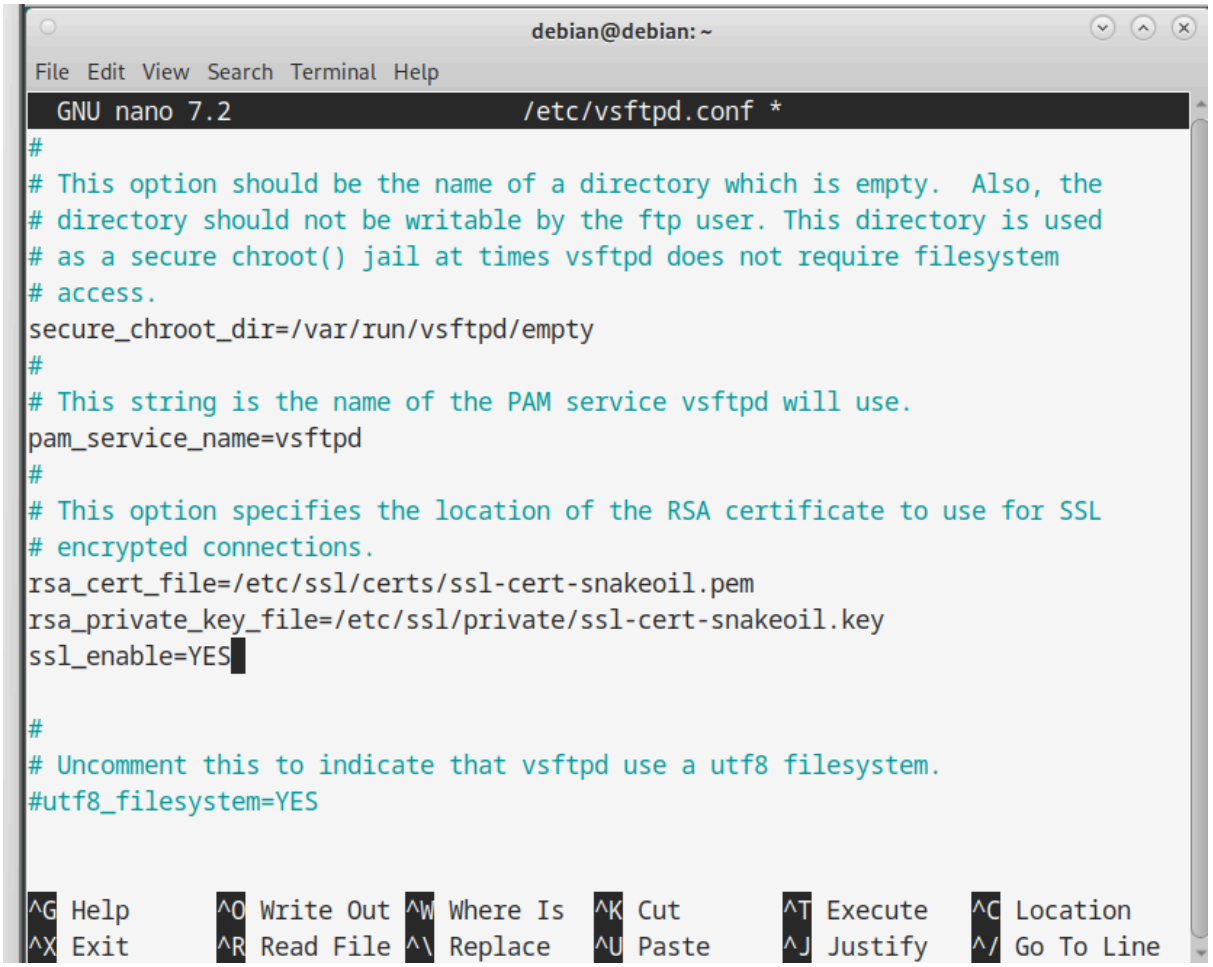
```
total 120
drwx------ 14 debian debian  4096 Jan 30 12:36 .
drwxr-xr-x  3 root   root    4096 Jul 31  2024 ..
-rw-------  1 debian debian  2192 Sep 30 15:35 .bash_history
-rw-r--r--  1 debian debian   220 Jul 31  2024 .bash_logout
-rw-r--r--  1 debian debian  3526 Jul 31  2024 .bashrc
drwxr-xr-x 13 debian debian  4096 Jan 30 15:45 .cache
drwxr-xr-x 10 debian debian  4096 Jan 30 16:41 .config
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Desktop
-rw-r--r--  1 debian debian    35 Jul 31  2024 .dmrc
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Documents
drwxr-xr-x  2 debian debian  4096 Jan 30 14:53 Downloads
-rw-r--r--  1 debian debian  5290 Jul 31  2024 .face
lrwxrwxrwx  1 debian debian     5 Jul 31  2024 .face.icon -> .face
-rw-------  1 debian debian    20 Jan 30 12:36 .lesshst
drwx------  3 debian debian  4096 Jul 31  2024 .local
drwx------  4 debian debian  4096 Jul 31  2024 .mozilla
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Music
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Pictures
-rw-r--r--  1 debian debian   807 Jul 31  2024 .profile
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Public
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Templates
drwxr-xr-x  2 debian debian  4096 Jul 31  2024 Videos
-rw-------  1 debian debian    51 Jan 30 12:31 .Xauthority
-rw-------  1 debian debian 20259 Jan 30 16:39 .xsession-errors
-rw-------  1 debian debian  4362 Jan 29 13:50 .xsession-errors.old
```

```
Applications  Places  System                                   Fri Jan 31, 10:29
                                  debian@debian: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 7.2                          /etc/ssh/sshd_config *
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

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

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
debian@debian: ~   debian@debian: ~
```

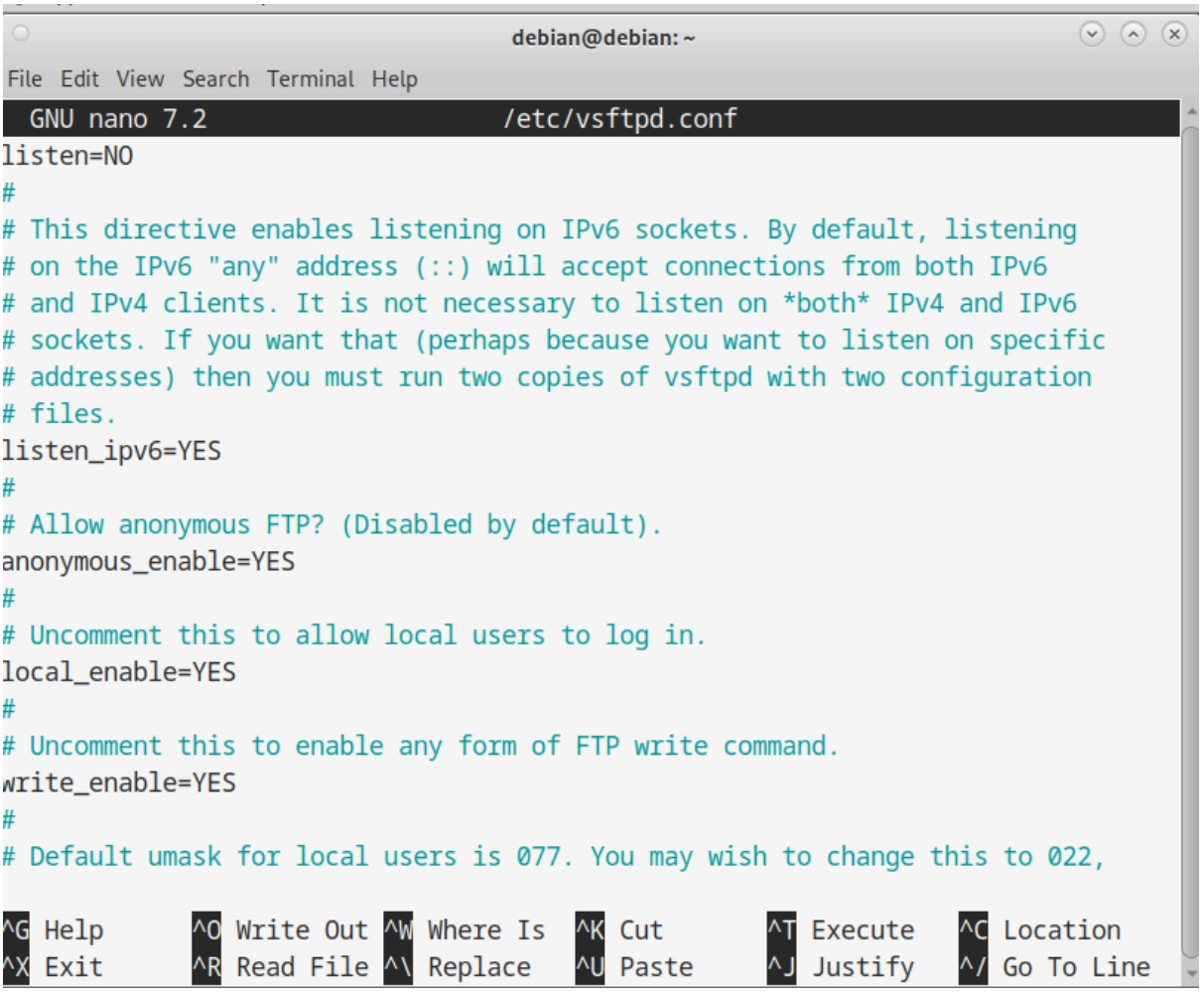
```
debian@debian:~$ sudo find / -type f -name ".sh*"
find: '/run/user/1000/doc': Permission denied
find: '/run/user/1000/gvfs': Permission denied
```

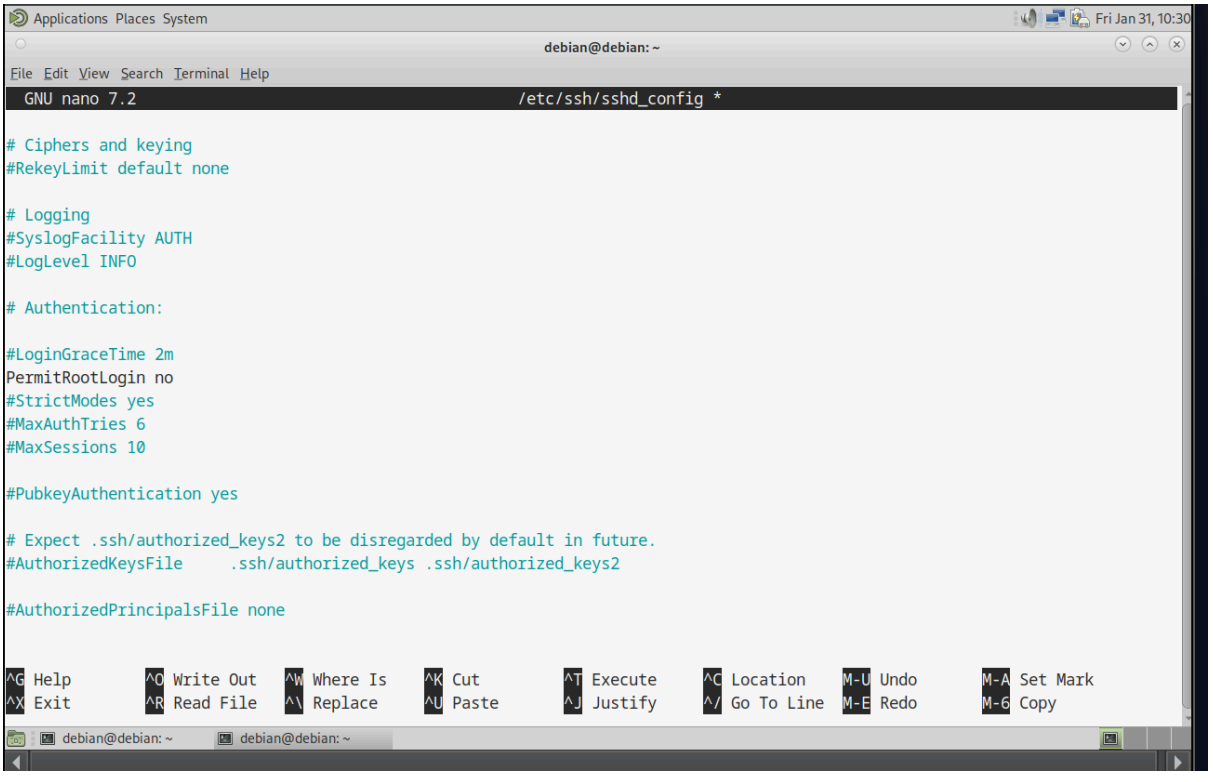



```
debian@debian:~$ sudo chmod -R 755 /var/ftp
chmod: cannot access '/var/ftp': No such file or directory
debian@debian:~$
```




```
MariaDB [(none)]> SELECT user, host, authentication_string FROM mysql.user;
+---------------+-----------+-------------------------------------------+
| User          | Host      | authentication_string                     |
+---------------+-----------+-------------------------------------------+
| mariadb.sys   | localhost |                                           |
| root          | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql         | localhost | invalid                                   |
| wordpressuser | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user          | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+---------------+-----------+-------------------------------------------+
```


debian@debian: ~
File Edit View Search Terminal Help
GNU nano 7.2 /etc/vsftpd.conf
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
#
# 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
#
Default umask for local users is 077. You may wish to change this to 022,
^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


Applications Places System
Fri Jan 31, 10:30
debian@debian: ~
File Edit View Search Terminal Help
GNU nano 7.2 /etc/ssh/sshd_config *
Ciphers and keying
#RekeyLimit default none
Logging
#SyslogFacility AUTH
#LogLevel INFO
Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy
debian@debian: ~
debian@debian: ~

```
debian@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a2:21:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82733sec preferred_lft 82733sec
    inet6 fe80::a00:27ff:fea2:2188/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
debian@debian:~$
```

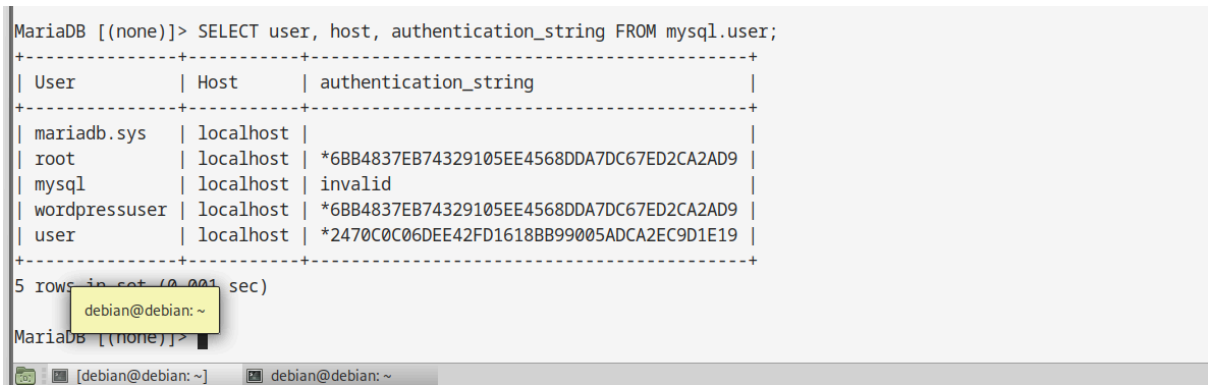
```
debian@debian:~$ nmap -p- 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-31 10:53 EST
Nmap scan report for 10.0.2.15
Host is up (0.000023s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
debian@debian:~$
```

```
# BEGIN WordPress
# The directives (lines) between "BEGIN WordPress" and "END WordPress" are
# dynamically generated, and should only be modified via WordPress filters.
# Any changes to the directives between these markers will be overwritten.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>

# END WordPress
```

```
debian@debian:~$ ls -la /var/www/html/wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 12:02 /var/www/html/wp-config.php
```


```
debian@debian:~$ ls -la /var/www/html/wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 12:02 /var/www/html/wp-config.php
```


Applications Places System
Fri Jan 31, 10:39
debian@debian: ~
File Edit View Search Terminal Help
GNU nano 7.2 /var/www/html/.htaccess *
BEGIN WordPress
The directives (lines) between "BEGIN WordPress" and "END WordPress" are
dynamically generated, and should only be modified via WordPress filters.
Any changes to the directives between these markers will be overwritten.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
Options -Indexes
</IfModule>
END WordPress
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy
debian@debian: ~
debian@debian: ~


MariaDB [(none)]> SELECT user, host, authentication_string FROM mysql.user;
User	Host	authentication_string
mariadb.sys	localhost	
root	localhost	*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
mysql	localhost	invalid
wordpressuser	localhost	*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
user	localhost	*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
5 rows in set (0.001 sec)
MariaDB [(none)]>
debian@debian: ~
[debian@debian: ~]
debian@debian: ~

```
lariaDB [(none)]> SELECT user, host FROM mysql.user;
+--------------+-----------+
| User         | Host      |
+--------------+-----------+
| mariadb.sys  | localhost |
| mysql        | localhost |
| root         | localhost |
| user         | localhost |
| wordpressuser | localhost |
+--------------+-----------+
 rows in set (0.001 sec)

lariaDB [(none)]>
```

debian@debian: ~

```
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 (0.001 sec)

MariaDB [(none)]> SELECT user, host, authentication_string FROM mysql.use
+---------------+-----------+-------------------------------------------+
| User          | Host      | authentication_string                     |
+---------------+-----------+-------------------------------------------+
| mariadb.sys   | localhost |                                           |
| root          | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql         | localhost | invalid                                   |
| wordpressuser | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user          | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+---------------+-----------+-------------------------------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]>
```

Captura de los pasos usados
Pentesting y vulnerabilidades.

Medidas de seguridad.

```
debian@debian:~$ sudo deluser --remove-home debian
[sudo] password for debian:
Looking for files to backup/remove ...
Removing files ...
Removing crontab ...
Removing user `debian' ...
userdel: user debian is currently used by process 1328
deluser: `/usr/sbin/userdel debian' returned error code 8. Exiting.
debian@debian:~$ sudo grupodel debian
sudo: grupodel: command not found
debian@debian:~$ sudo groupdel debian
groupdel: cannot remove the primary group of user 'debian'
debian@debian:~$ sudo rm -rf /home/debian/.ssh
debian@debian:~$ sudo nano /etc/ssh/sshd_config
debian@debian:~$ sudo systemctl restart sshd
```

```
debian@debian:~$ sudo rm -rf /var/www/html/*
debian@debian:~$ sudo nano /etc/apache2/sities-avaible/000-dafault.conf
debian@debian:~$ sudo systemctl restart apache2
debian@debian:~$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250313_150348'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250313_150348'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250313_150348'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250313_150348'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250313_150348'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250313_150348'

debian@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
debian@debian:~$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
Debian-exim:x:115:124::/var/spool/exim4:/usr/sbin/nologin
debian@debian:~$ sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-image-6.1.0-22-amd64 linux-image-6.1.0-23-amd64
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cracklib-runtime libcrack2 libpwquality-common libpwquality1
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpam-pwquality libpwquality-common
  libpwquality1
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
```