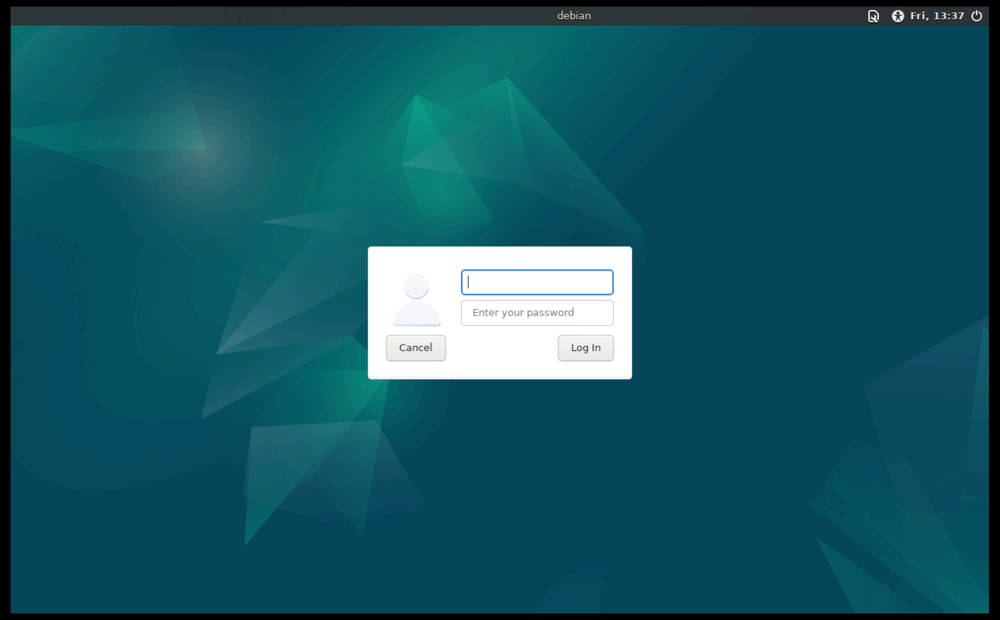
INCIDENTE DE SEGURIDAD

David Huang

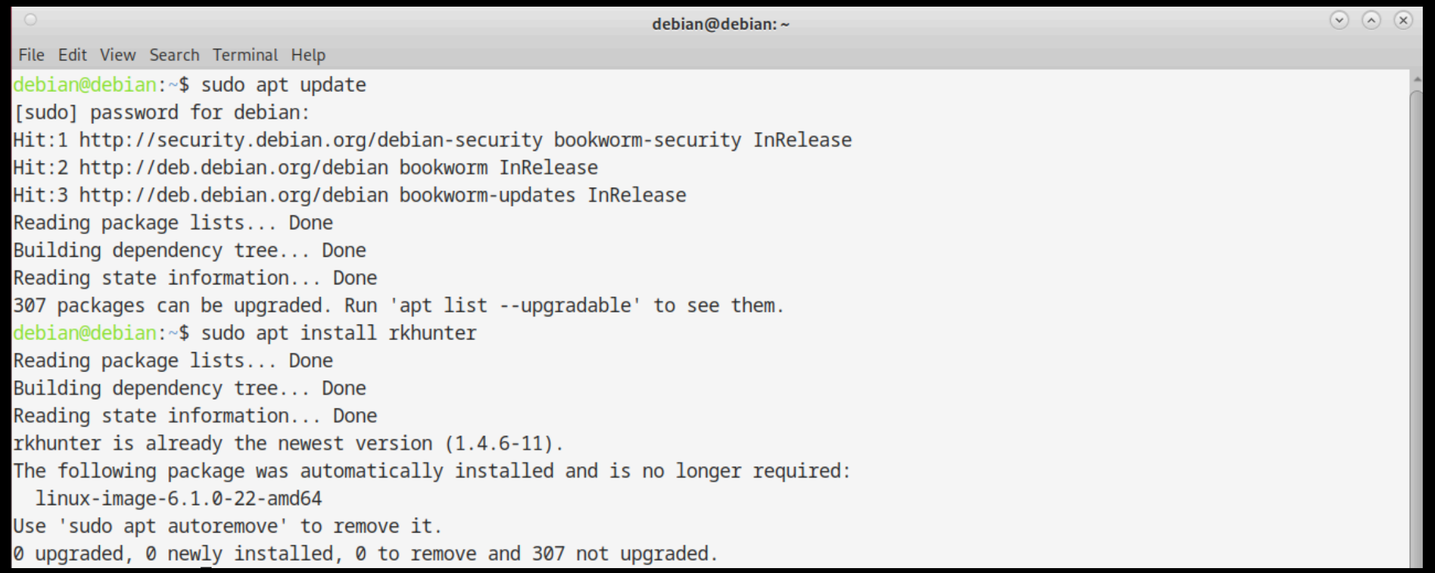


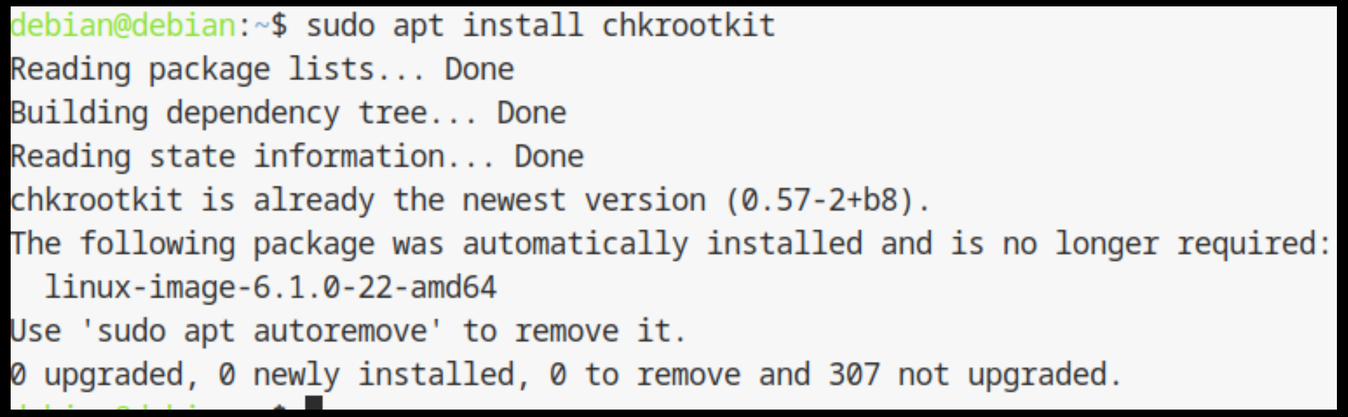
INDICE

- Incidente ocurrido.
  - Reconocimiento de vulnerabilidad.
  - Recolección de evidencias.
- Solución del incidente.
- Investigación de nuevas vulnerabilidades.
  - Vulnerabilidad en el puerto 21.
  - Vulnerabilidad en el puerto 80.
- Recomendaciones sobre la máquina.
- Mejoras a futuro.
  - Organizar un plan de respuestas contra incidentes.
  - Crear backups.
  - Mecanismos para proteger los datos.

Reconocimiento

Herramientas útiles como Rkhunter o Chkrootkit para detectar malware y el uso de journalctl para verificar si han entrado en la máquina.





```
debian@debian:~$ sudo rkhunter --check
```

```
   /usr/bin/lwp-request                                      [ Warning ]
```

```
Checking for suspicious (large) shared memory segments    [ Warning ]
```

```
[17:46:03] Warning: The following suspicious (large) shared memory segments have been found:
[17:46:03]          Process: /usr/bin/mate-panel    PID: 1141    Owner: debian    Size: 4.0MB (configured size allowed: 1.0MB)
[17:46:04]          Process: /usr/bin/caja    PID: 1170    Owner: debian    Size: 32MB (configured size allowed: 1.0MB)
[17:46:04]          Process: /usr/bin/mate-terminal    PID: 554016    Owner: debian    Size: 4.0MB (configured size allowed: 1
.0MB)
[17:46:04]          Process: /usr/bin/mate-screensaver    PID: 1199    Owner: debian    Size: 32MB (configured size allowed: 1
```

```
Checking if SSH root access is allowed                    [ Warning ]
```

```
[13:53:07]   Checking if SSH root access is allowed          [ Warning ]
[13:53:07] Warning: The SSH and rkhunter configuration options should be the same:
[13:53:07]          SSH configuration option 'PermitRootLogin': yes
[13:53:07]          Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': no
```

Rkhunter

Se utiliza la herramienta para ayudar a la detección de malware o vulnerabilidades.

```
debian@debian:~$ sudo chkrootkit
```

```
Searching for suspicious files and dirs...                    WARNING

WARNING: The following suspicious files and directories were found:
/usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.vscodeignore
/usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.gitignore
/usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.vscode
/usr/lib/ruby/vendor_ruby/rubygems/ssl_certs/.document
/usr/lib/ruby/vendor_ruby/rubygems/tsort/.document
/usr/lib/ruby/vendor_ruby/rubygems/optparse/.document
/usr/lib/libreoffice/share/.registry
```

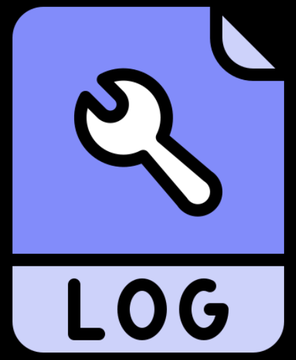
```
Checking `sniffer'...                                         WARNING

WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[528])
```

Chkrootkit

Se utiliza la herramienta para ayudar a la detección de rootkits.

Journalctl

Es la herramienta de línea de comandos utilizada para consultar y mostrar los registros (logs) del sistema en sistemas Linux.




```
debian@debian:~$ sudo journalctl -u ssh | grep "Accepted"
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
```

Evidencias

```
debian@debian:~$ sudo journalctl -u ssh | grep "Accepted"
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
```

```
# Authentication:

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

- La máquina virtual debian sufrió un ataque por el puerto 22.
- Con una mala configuración del SSH, da una vulnerabilidad de escalada de privilegios.

Solución

- Cambio en el fichero de la autenticación del puerto 22.
- Aplicar un firewall “ufw” para la ayuda contra la vulnerabilidad conocida.

```
debian@debian:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
debian@debian:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
debian@debian:~$ sudo ufw allow from 192.168.1.130 to any port 22 proto tcp
Rules updated
debian@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

```
# Authentication:

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

Investigación

Se usa la herramienta de Nmap para analizar los puertos, Netstat y Nikto. Gracias a la máquina Kali nos ayudará a la investigación.

```
debian@debian:~$ sudo nmap -sV -p- 10.0.2.12
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-24 12:39 EST
Nmap scan report for 10.0.2.12
Host is up (0.0000010s latency).
Not shown: 65532 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)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
```

```
debian@debian:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      545/cupsd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      579/sshd: /usr/sbin
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      669/mariadbd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      3060/exim4
tcp6       0      0 ::1:631                 :::*                    LISTEN      545/cupsd
tcp6       0      0 :::80                   :::*                    LISTEN      670/apache2
tcp6       0      0 :::21                   :::*                    LISTEN      556/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      579/sshd: /usr/sbin
tcp6       0      0 ::1:25                  :::*                    LISTEN      3060/exim4
udp        0      0 0.0.0.0:51166           0.0.0.0:*                           507/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           507/avahi-daemon: r
udp6       0      0 :::5353                 :::*                                507/avahi-daemon: r
udp6       0      0 :::55573                :::*                                507/avahi-daemon: r
debian@debian:~$ sudo nano /etc/ssh/sshd_config
```

Vsftpd (puerto 21)

El puerto 21 tiene un acceso autorizado con un acceso llamado “anonymous”.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.12
Connected to 10.0.2.12.
220 (vsFTPd 3.0.3)
Name (10.0.2.12:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               close           fget            lpage           modtime         pdir            rcvbuf          sendport        type
$               cr              form            lpwd            more            pls             recv            set             umask
account         debug           ftp             ls              mput            pmlsd           reget           site            unset
append          delete          gate            macdef          mreget          preserve        remopts         size            usage
ascii           dir             get             mdelete         msend           progress        rename          sndbuf          user
bell            disconnect      glob            mdir            newer           prompt          reset           status          verbose
binary          edit            hash            mget            nlist           proxy           restart         struct          xferbuf
bye             epsv            help            mkdir           nmap            put             rhelp           sunique         ?
case            epsv4           idle            mls             ntrans          pwd             rmdir           system
cd              epsv6           image           mlsd            open            quit            rstatus         tenex
cdup            exit            lcd             mlst            page            quote           runique         throttle
chmod           features        less            mode            passive         rate            send            trace
```

Apache (puerto 80)

Gracias a la herramienta Nikto se ha encontrado varias vulnerabilidades en la página web.

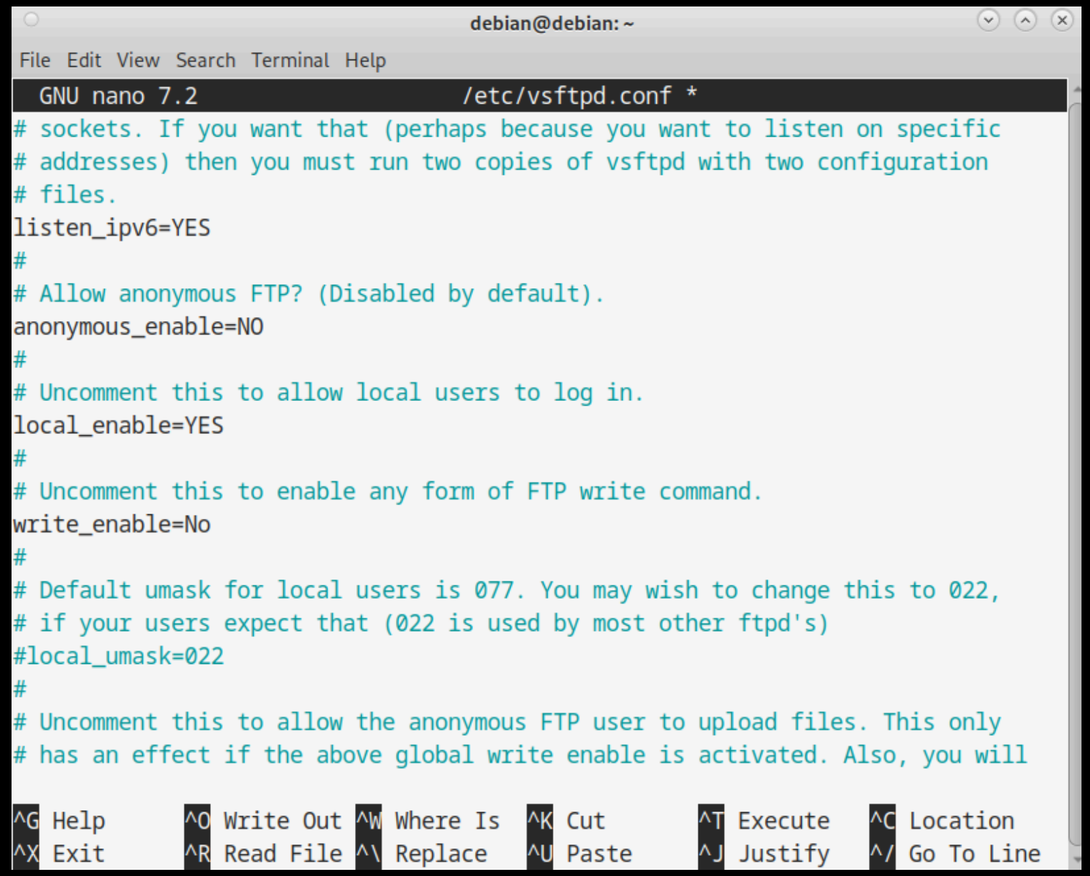
```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.0.2.12
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.12
+ Target Hostname:    10.0.2.12
+ Target Port:        80
+ Start Time:         2026-01-24 15:56:03 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Opt
ions
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /FalHqZTx.de: Drupal Link header found with value: <http://localhost/index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupa
l.org/
+ /FalHqZTx.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 623573d915b52, mtime: gzip. See: http://cve.mitre.org/cg
i-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/: A Wordpress installation was found.
+ /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.
+ /wp-login.php: Wordpress login found.
+ 8106 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2026-01-24 15:59:04 (GMT-5) (181 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Recomendaciones en el puerto 21

- Deshabilitar el acceso anónimo del puerto vsftpd.
- Aplicar un firewall para contrarrestar las vulnerabilidades.

```
debian@debian:~$ sudo ufw allow from 192.168.1.50 to any port 21
Rule added
debian@debian:~$ sufo ufw deny 21
bash: sufo: command not found
debian@debian:~$ sudo ufw deny 21
Rule added
Rule added (v6)
debian@debian:~$
```


```
debian@debian:~$ sudo ufw allow from 192.168.1.50 to any port 21
Rule added
debian@debian:~$ sufo ufw deny 21
bash: sufo: command not found
debian@debian:~$ sudo ufw deny 21
Rule added
Rule added (v6)
debian@debian:~$
```

Recomendaciones en el puerto 80

debian@debian: ~

File Edit View Search Terminal Help

GNU nano 7.2 /etc/apache2/conf-available/security.conf *

```
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

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

#
```

^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

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set X-XSS-Protection "1; mode=block"
```

```
debian@debian:~$ sudo systemctl restart apache2
```

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

```
<FilesMatch "^\.">
        Require all denied
</FilesMatch>
```

```
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
 <Directory /var/www/html>
        <LimitExcept GET POST>
                Require all denied
        </LimitExcept>
</Directory>
```

Recomendaciones

- Actualizar la máquina.
- (Opcional) Eliminación de puertos.
- Aplicar firewalls.
- (Opcional) Añadir un crontab para la actualización del sistema.

```
debian@debian:~$ sudo apt update
[sudo] password for debian:
Hit:1 http://deb.debian.org/debian bookworm InRelease
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources [196 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [292 kB]
Fetched 537 kB in 1s (904 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
debian@debian:~$ sudo apt install-y
```

```
debian@debian:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libdaxctl1 libndctl6 libpmem1 linux-image-6.1.0-22-amd64 linux-image-6.1.0-23-amd64
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  python3-urllib3
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 114 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://security.debian.org/debian-security bookworm-security/main amd64 python3-urllib3 all 1.26.12-1+deb12u3 [114 kB]
Fetched 114 kB in 0s (1,287 kB/s)
apt-listchanges: Reading changelogs...
(Reading database ... 179601 files and directories currently installed.)
Preparing to unpack .../python3-urllib3_1.26.12-1+deb12u3_all.deb ...
Unpacking python3-urllib3 (1.26.12-1+deb12u3) over (1.26.12-1+deb12u2) ...
Setting up python3-urllib3 (1.26.12-1+deb12u3) ...
```

Recomendaciones

- Actualizar la máquina.
- (Opcional) Eliminación de puertos.
- Aplicar firewalls.
- (Opcional) Añadir un crontab para la actualización del sistema.

```
debian@debian:~$ sudo systemctl stop vsftpd
debian@debian:~$ sudo systemctl disable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable vsftpd
Removed "/etc/systemd/system/multi-user.target.wants/vsftpd.service".
debian@debian:~$
```

```
debian@debian:~$ sudo systemctl disable cups
Synchronizing state of cups.service with SysV service script with /lib/systemd/s
ystemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cups
Removed "/etc/systemd/system/sockets.target.wants/cups.socket".
Removed "/etc/systemd/system/multi-user.target.wants/cups.path".
Removed "/etc/systemd/system/multi-user.target.wants/cups.service".
Removed "/etc/systemd/system/printer.target.wants/cups.service".
```

Recomendaciones

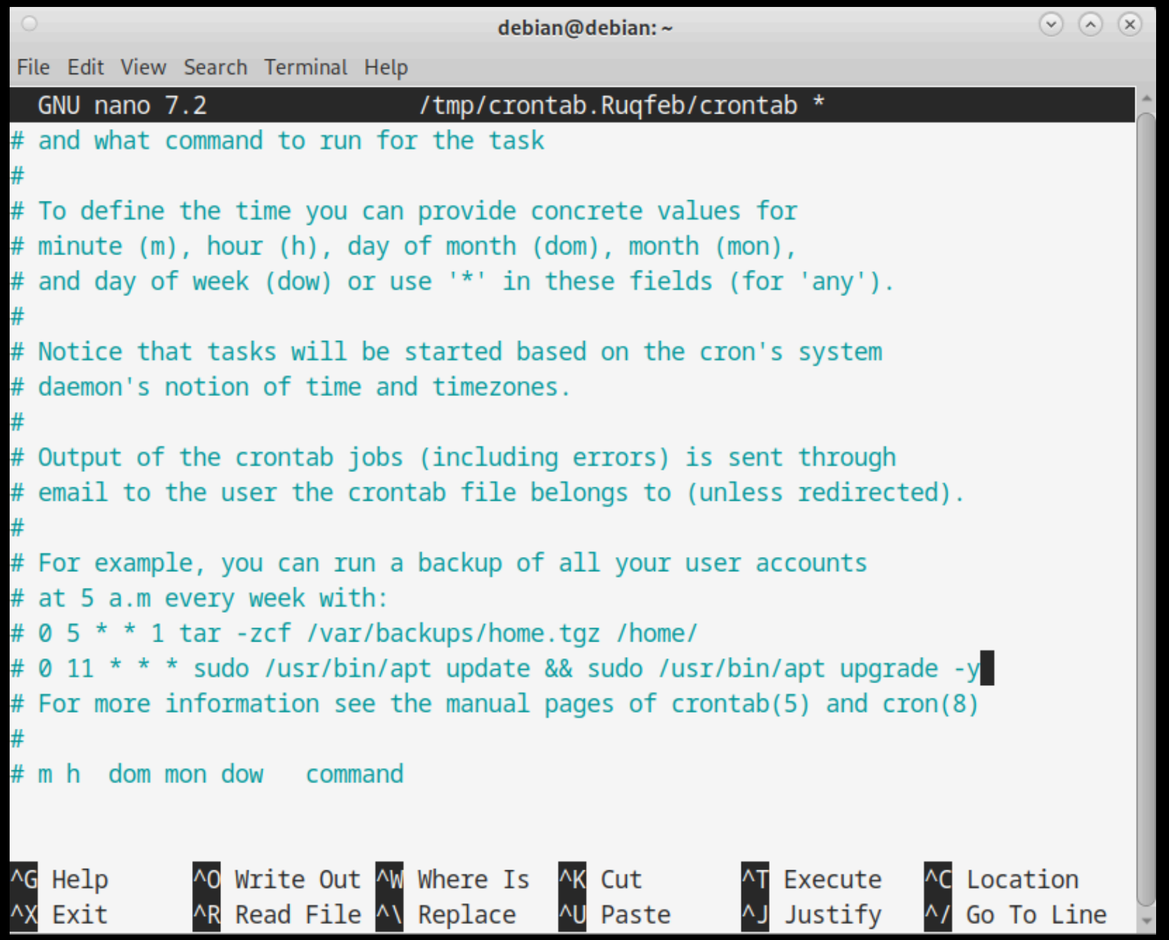
- Actualizar la máquina.
- (Opcional) Eliminación de puertos.
- Aplicar firewalls.
- (Opcional) Añadir un crontab para la actualización del sistema.

```
debian@debian:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
debian@debian:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
debian@debian:~$ sudo ufw allow from 192.168.1.130 to any port 22 proto tcp
Rules updated
debian@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

```
debian@debian:~$ sudo systemctl restart apache2
debian@debian:~$ sudo ufw allow in on lo
Rule added
Rule added (v6)
```

Recomendaciones

- Actualizar la máquina.
- (Opcional) Eliminación de puertos.
- Aplicar firewalls.
- (Opcional) Añadir un crontab para la actualización del sistema.



MEJORA A FUTURO

ORGANIZAR UN PLAN DE RESPUESTAS CONTRA INCIDENTES.

CREAR BACKUPS.

MECANISMOS PARA PROTEGER LOS DATOS.

PLAN DE RESPUESTAS ANTE INCIDENTES

PREVER.

INFORMAR.

RESPONDER.

MITIGAR.

APRENDIZAJE.

CREACIÓN DE BACKUPS

TIPOS DE RESPALDO.

AUTOMATIZACIÓN.

ALMACENAMIENTO.

VERIFICACIÓN.

SEGURIDAD Y CONTROL DE ACCESO.

MECANISMOS PARA PROTEGER LOS DATOS

- SEGUIR LA TRIADA DE LA CIA.
- RESPALDOS PERIÓDICOS.
- CIFRADO DE DATOS.
- IMPLEMENTAR CONTROLES DE ACCESO.

CONCLUSIÓN