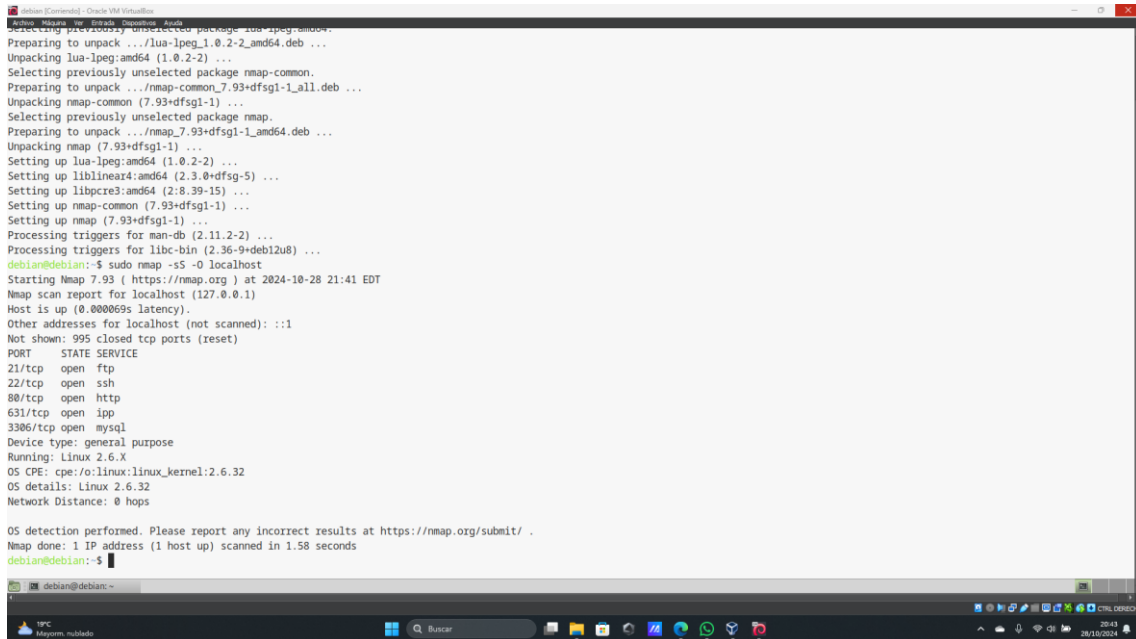


Proyecto Final Ciberseguridad

Fase 1: Análisis Forense.

Objetivo: Lleva a cabo un análisis forense para bloquear el exploit, corregir la vulnerabilidad y evitar que el atacante escale.

Identificación de servicios que han sido comprometidos:



```
debian@debian:~$ sudo apt-get install nmap
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-2_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-2) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.93+dfsg1-1_all.deb ...
Unpacking nmap-common (7.93+dfsg1-1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.93+dfsg1-1_amd64.deb ...
Unpacking nmap (7.93+dfsg1-1) ...
Setting up lua-lpeg:amd64 (1.0.2-2) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up libpcre3:amd64 (2.8.39-15) ...
Setting up nmap-common (7.93+dfsg1-1) ...
Setting up nmap (7.93+dfsg1-1) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u8) ...
debian@debian:~$ sudo nmap -sS -O localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-28 21:41 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000069s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
3306/tcp  open  mysql
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
debian@debian:~$
```

1. 21/tcp open ftp

- **Riesgos:**
 - FTP (File Transfer Protocol) no cifra la información, por lo que las credenciales y datos transferidos pueden ser interceptados fácilmente en texto claro, facilitando ataques de *sniffing*.
 - El puerto 21 es un objetivo común para ataques de fuerza bruta, que buscan adivinar credenciales mediante múltiples intentos.

Recomendaciones:

- **Deshabilitar FTP** si no es absolutamente necesario. Considera usar SFTP (Secure FTP) o FTPS para transferencias seguras, ya que estos protocolos cifran la información.
- **Restringir el acceso** al servicio, limitando la conexión solo a IPs de confianza y aplicando listas de control de acceso (ACL).
- **Configurar autenticación segura:** Establece contraseñas fuertes y, si es posible, autenticación de dos factores para evitar ataques de fuerza bruta.

2. 22/tcp open ssh

- **Riesgos:**
 - SSH (Secure Shell) es relativamente seguro, pero si las configuraciones no son adecuadas, puede ser vulnerable a ataques de fuerza bruta y de diccionario.
 - Los atacantes pueden intentar obtener acceso mediante credenciales débiles o por configuraciones permisivas de autenticación.
- **Recomendaciones:**
 - **Configurar autenticación basada en llaves** en lugar de contraseñas, lo que aumenta la seguridad del acceso.
 - **Cambiar el puerto predeterminado (22)** por otro menos común para reducir los intentos automatizados de acceso no autorizado.
 - **Limitar los intentos de conexión** fallidos y configurar *fail2ban* o herramientas similares para bloquear IPs después de varios intentos.

3. 80/tcp open ipp

- **Riesgos:**
 - El puerto 80 a menudo se utiliza para HTTP y en este caso también para el Protocolo de Impresión en Internet (IPP), que puede exponer información de impresoras o de documentos sensibles en red.
 - El tráfico HTTP no está cifrado, por lo que es susceptible a *sniffing*, ataques *MITM* (Man-in-the-Middle) y divulgación de información.
 - Si el servicio está configurado incorrectamente o expuesto a Internet, podría permitir a los atacantes explorar y potencialmente controlar impresoras u obtener detalles de red.
- **Recomendaciones:**
 - **Cambiar a HTTPS** (puerto 443) y habilitar el cifrado SSL/TLS si es posible para IPP, o usar otro método de gestión de impresoras que no exponga información en texto claro.
 - **Restringir el acceso** al servicio IPP limitándolo a dispositivos de red confiables y deshabilitar el puerto 80 si no es necesario.

4. 3306/tcp open mysql

- **Riesgos:**
 - MySQL, si está expuesto, puede ser vulnerable a ataques de fuerza bruta y otros tipos de ataques que exploten la base de datos.
 - Las configuraciones predeterminadas de MySQL pueden permitir accesos sin suficiente restricción de IPs, aumentando el riesgo de acceso no autorizado.
 - Las bases de datos que contienen información sensible pueden ser un objetivo atractivo para atacantes.
- **Recomendaciones:**
 - **Restringir el acceso** de MySQL solo a localhost si es posible (127.0.0.1), para evitar conexiones remotas innecesarias.
 - **Establecer contraseñas fuertes** para todas las cuentas de MySQL, en especial la cuenta root.
 - **Utilizar cifrado** en conexiones de red MySQL para proteger la información sensible en tránsito, y considerar cifrar la información almacenada.

5. 631/tcp - HTTP (CUPS - Common UNIX Printing System)

- **Riesgos:**
 - CUPS expuestos podría permitir a atacantes visualizar o manipular tareas de impresión, así como acceder a información potencialmente confidencial.
 - Es vulnerable a configuraciones incorrectas, lo que podría permitir acceso no autorizado.
- **Recomendaciones:**
 - **Deshabilitar CUPS** si no es necesario.
 - Restringir el acceso al puerto 631 solo a direcciones locales o seguras mediante el firewall.
 - Actualizar CUPS a la última versión disponible y verificar que se aplica una autenticación adecuada para el acceso remoto.

Identificación de archivos sospechosos, procesos en ejecución y cualquier modificación inusual en el sistema.

Buscamos archivos modificados recientemente, esto nos ayuda a detectar archivos que hayan sido creados o modificados en un periodo específico.

Utilizamos el comando **find / -type f -mtime -7 -ls**; Esto lista archivos modificados en los últimos 7 días.

```

debian@debian:~$ find / -type f -mtime -7 -ls
1443571 4 -rw-r--r-- 1 root root 2002 Oct 30 23:34 /etc/passwd
1442922 4 drwxr-xr-x 2 root root 1066 Oct 30 23:34 /etc/shadow
1441869 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/ppp/ip-up.d
1444077 0 lrwxrwxrwx 1 root root 15 Oct 30 23:34 /etc/rc6.d/K01exim4 -> ../init.d/exim4
1441810 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/apt/apt.conf.d
1441996 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/cron.weekly
1441822 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/alternatives
1443813 4 -rw-r--r-- 1 root root 14 Oct 30 23:34 /etc/mailname
1441900 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/init.d
1442391 4 drwxr-xr-x 5 root root 4096 Oct 30 22:40 /etc/cups
1444000 4 -rw-r--r-- 1 root root 381 Oct 30 22:40 /etc/cups/subscriptions.conf
1443955 4 -rw-r--r-- 1 root root 671 Oct 30 20:48 /etc/cups/subscriptions.conf.0
1442393 4 drwxr-xr-x 2 root root 4096 Oct 30 22:43 /etc/cups/ssl
find: '/etc/cups/ssl': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
1441864 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/rc1.d
1444076 0 lrwxrwxrwx 1 root root 15 Oct 30 23:34 /etc/rc1.d/K01exim4 -> ../init.d/exim4
1441868 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/rc5.d
1444074 0 lrwxrwxrwx 1 root root 15 Oct 30 23:34 /etc/rc5.d/S01exim4 -> ../init.d/exim4
1443994 4 -rw-r--r-- 1 root root 797 Oct 30 23:34 /etc/gshadow
1441863 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/rc0.d
1444075 0 lrwxrwxrwx 1 root root 15 Oct 30 23:34 /etc/rc0.d/K01exim4 -> ../init.d/exim4
1441866 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/rc3.d
1444072 0 lrwxrwxrwx 1 root root 15 Oct 30 23:34 /etc/rc3.d/S01exim4 -> ../init.d/exim4
1443579 4 -rw-r--r-- 1 root root 78 Oct 30 20:47 /etc/resolv.conf
1441865 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/rc2.d
1444070 0 lrwxrwxrwx 1 root root 15 Oct 30 23:34 /etc/rc2.d/S01exim4 -> ../init.d/exim4
1444086 64 -rw-r--r-- 1 root root 62894 Oct 30 23:34 /etc/ld.so.cache
1444069 4 -rw-r--r-- 1 root root 948 Oct 30 23:34 /etc/group
1441915 4 drwxr-xr-x 2 root root 4096 Oct 30 23:34 /etc/systemd/system/timers.target.wants
1444078 0 lrwxrwxrwx 1 root root 36 Oct 30 23:34 /etc/systemd/system/timers.target.wants/exim4-base.timer -> /lib/systemd/system/exim4-base.t
imer
find: '/etc/ssl/private': Permission denied
find: '-': No such file or directory
find: 'type': No such file or directory
debian@debian:~$ find / -type f -mtime -7 -ls

```

Buscamos permisos inusuales, archivos con permisos *suid* o *sgid* podrían ser explotables si se alteraron sin autorización para esto usamos el comando **find / -perm /6000 -type f 2>/dev/null**

```

debian@debian:~$ find / -perm /6000 -type f 2>/dev/null
/usr/sbin/exim4
/usr/sbin/unix_chkpwd
/usr/sbin/pppd
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/fusemount3
/usr/bin/expiry
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/ntfs-3g
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/chage
/usr/bin/dotlockfile
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/crontab
debian@debian:~$

```

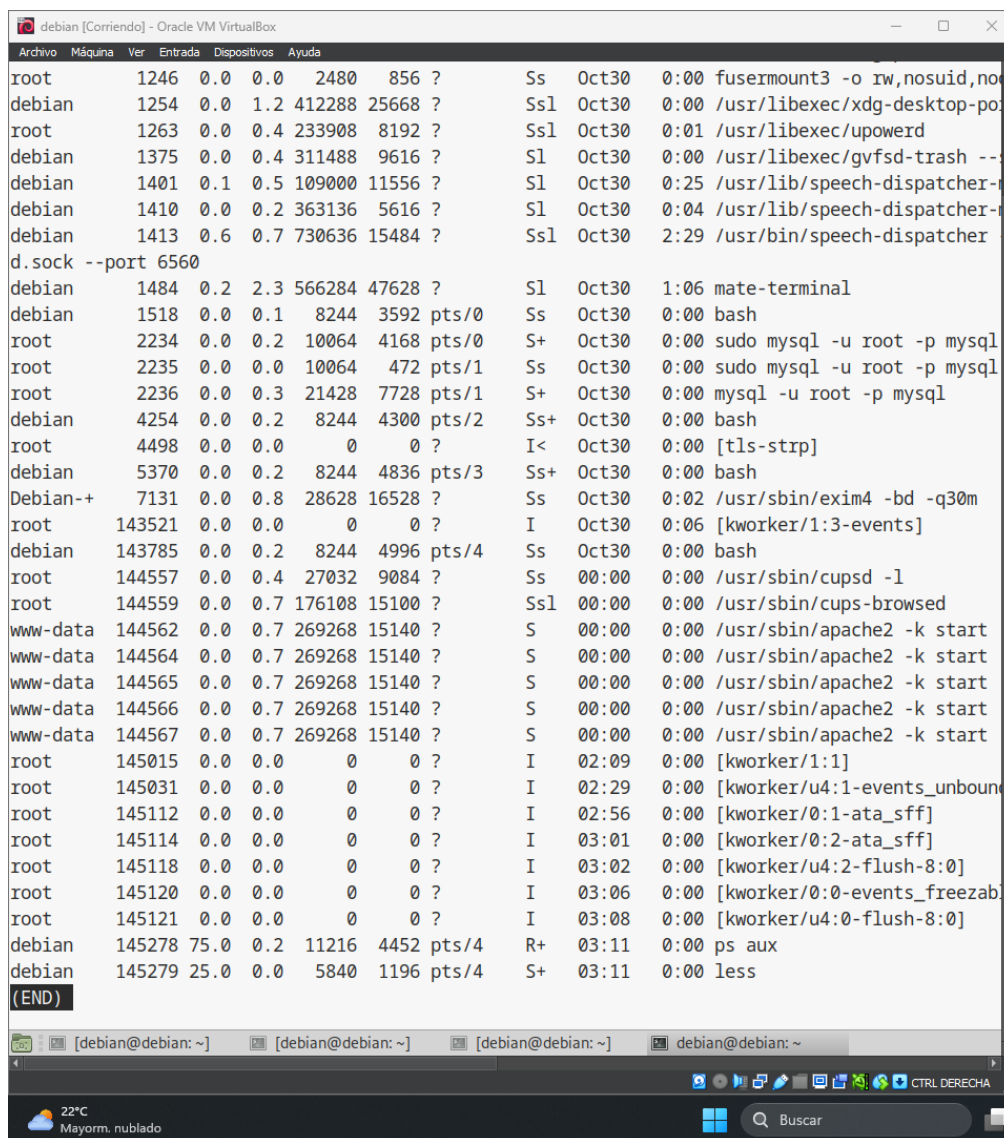
La lista que obtuvimos muestra archivos que tienen los bits de Setuid o Setgid activados, como **/usr/bin/sudo**, **/usr/bin/passwd**, y **/usr/bin/chage**. Estos son archivos que podrían usarse para ejecutar comandos con privilegios elevados, lo que los convierte en posibles objetivos para el escalamiento de privilegios.

Para mejorar la seguridad, podemos:

- Revisar estos archivos y decidir si es seguro que tengan estos permisos.
- Usar herramientas como **chmod** para ajustar los permisos si encuentras alguno que no debería tener Setuid o Setgid.

Revisión de procesos en ejecución

Usamos el comando **ps aux** para revisar procesos en ejecución el mismo observa procesos desconocidos o ejecutándose desde ubicaciones sospechosas.



```
debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root      1246  0.0  0.0  2480  856  ?      Ss   Oct30  0:00 fusermount3 -o rw,nosuid,no
debian    1254  0.0  1.2  412288 25668  ?      Ssl  Oct30  0:00 /usr/libexec/xdg-desktop-po
root      1263  0.0  0.4  233908 8192  ?      Ssl  Oct30  0:01 /usr/libexec/upowerd
debian    1375  0.0  0.4  311488 9616  ?      Sl   Oct30  0:00 /usr/libexec/gvfsd-trash --
debian    1401  0.1  0.5  109000 11556  ?      Sl   Oct30  0:25 /usr/lib/speech-dispatcher-
debian    1410  0.0  0.2  363136 5616  ?      Sl   Oct30  0:04 /usr/lib/speech-dispatcher-
debian    1413  0.6  0.7  730636 15484  ?      Ssl  Oct30  2:29 /usr/bin/speech-dispatcher
d.sock --port 6560
debian    1484  0.2  2.3  566284 47628  ?      Sl   Oct30  1:06 mate-terminal
debian    1518  0.0  0.1  8244  3592 pts/0   Ss   Oct30  0:00 bash
root      2234  0.0  0.2  10064  4168 pts/0   S+   Oct30  0:00 sudo mysql -u root -p mysql
root      2235  0.0  0.0  10064  472 pts/1    Ss   Oct30  0:00 sudo mysql -u root -p mysql
root      2236  0.0  0.3  21428  7728 pts/1    S+   Oct30  0:00 mysql -u root -p mysql
debian    4254  0.0  0.2  8244  4300 pts/2    Ss+  Oct30  0:00 bash
root      4498  0.0  0.0  0  0 ?      I<   Oct30  0:00 [tls-strp]
debian    5370  0.0  0.2  8244  4836 pts/3    Ss+  Oct30  0:00 bash
Debian++  7131  0.0  0.8  28628 16528  ?      Ss   Oct30  0:02 /usr/sbin/exim4 -bd -q30m
root      143521 0.0  0.0  0  0 ?      I    Oct30  0:06 [kworker/1:3-events]
debian    143785 0.0  0.2  8244  4996 pts/4    Ss   Oct30  0:00 bash
root      144557 0.0  0.4  27032  9084 ?      Ss   00:00 0:00 /usr/sbin/cupsd -l
root      144559 0.0  0.7  176108 15100 ?      Ssl  00:00 0:00 /usr/sbin/cups-browsed
www-data  144562 0.0  0.7  269268 15140 ?      S    00:00 0:00 /usr/sbin/apache2 -k start
www-data  144564 0.0  0.7  269268 15140 ?      S    00:00 0:00 /usr/sbin/apache2 -k start
www-data  144565 0.0  0.7  269268 15140 ?      S    00:00 0:00 /usr/sbin/apache2 -k start
www-data  144566 0.0  0.7  269268 15140 ?      S    00:00 0:00 /usr/sbin/apache2 -k start
www-data  144567 0.0  0.7  269268 15140 ?      S    00:00 0:00 /usr/sbin/apache2 -k start
root      145015 0.0  0.0  0  0 ?      I    02:09 0:00 [kworker/1:1]
root      145031 0.0  0.0  0  0 ?      I    02:29 0:00 [kworker/u4:1-events_unbound
root      145112 0.0  0.0  0  0 ?      I    02:56 0:00 [kworker/0:1-ata_sff]
root      145114 0.0  0.0  0  0 ?      I    03:01 0:00 [kworker/0:2-ata_sff]
root      145118 0.0  0.0  0  0 ?      I    03:02 0:00 [kworker/u4:2-flush-8:0]
root      145120 0.0  0.0  0  0 ?      I    03:06 0:00 [kworker/0:0-events_freezabl
root      145121 0.0  0.0  0  0 ?      I    03:08 0:00 [kworker/u4:0-flush-8:0]
debian    145278 75.0 0.2  11216  4452 pts/4    R+   03:11 0:00 ps aux
debian    145279 25.0 0.0  5840  1196 pts/4    S+   03:11 0:00 less
(END)
```

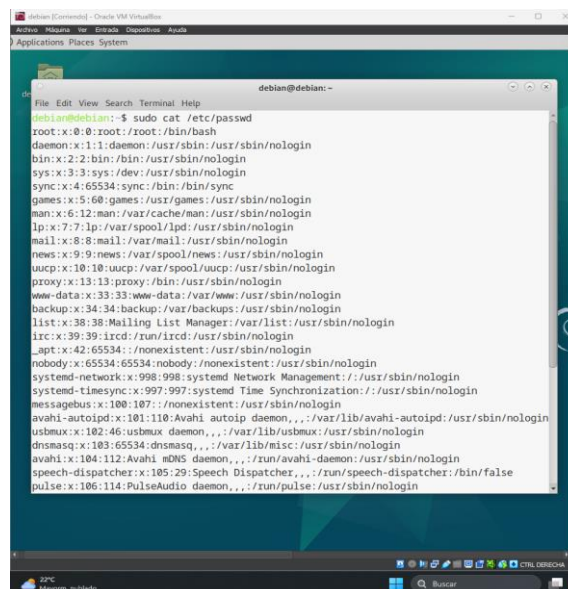
La salida de **ps aux** nos proporciona una visión general de los procesos en ejecución en tu sistema. Al comprender esta información, se puede identificar problemas de rendimiento, optimizar recursos y mantener tu sistema estable.

Recomendaciones

1. **Monitoreo Regular:** Utiliza herramientas como `top` o `htop` para monitorear los procesos en tiempo real y detectar cualquier anomalía.
2. **Identificación de Procesos Desconocidos:** Si encuentras procesos que no reconoces, busca información en línea o en la documentación de tu distribución para determinar su función y si son necesarios.
3. **Optimización de Servicios:** Si algunos servicios consumen demasiados recursos, puedes intentar ajustar sus configuraciones o reiniciarlos.
4. **Limpieza de Procesos Zombis:** Los procesos zombis son procesos terminados que aún no han sido eliminados por sus padres. Utiliza el comando `ps aux | grep Z` para identificarlos y eliminarlos.
5. **Análisis de Logs:** Revisa los logs del sistema para buscar mensajes de error o advertencias que puedan indicar problemas.
6. **Actualizaciones del Sistema:** Mantén tu sistema operativo y las aplicaciones actualizados para corregir vulnerabilidades y mejorar el rendimiento.

Comprobación de usuarios y permisos.

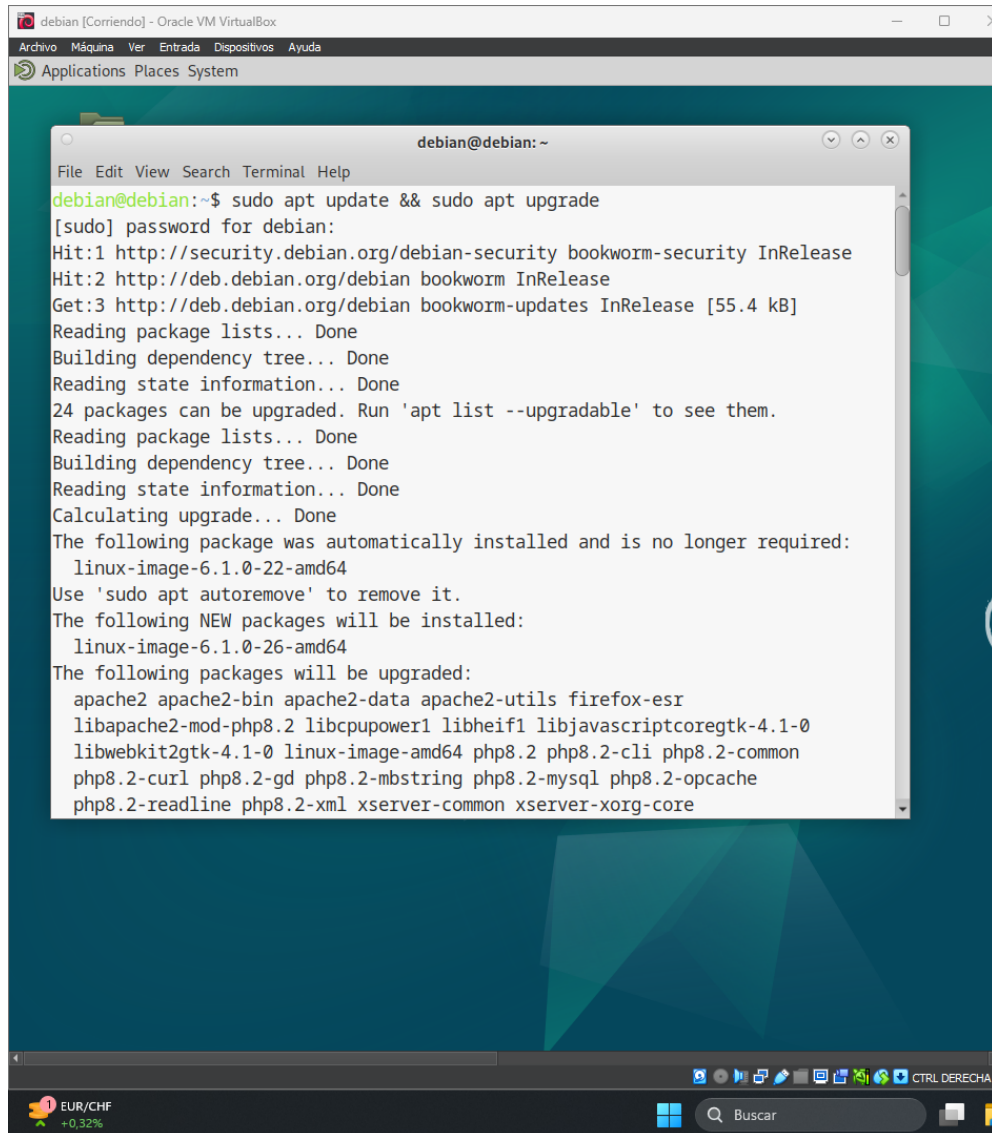
sudo cat /etc/passwd Este comando muestra el contenido del archivo `/etc/passwd`, que contiene información sobre las cuentas de usuario en el sistema. Cada línea en este archivo representa un usuario y contiene varios campos separados por dos puntos (:). Aquí se muestra una descripción de cada campo.



```
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:/usr/sbin:/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
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:irc:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
system-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoipd 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
```

Bloqueo de exploit y prevención de escalación. Detención de los servicios comprometidos temporalmente (`systemctl stop servicio`) en caso de ser necesario.

Actualización del sistema Tener el sistema actualizado es la primera línea de defensa, ya que los parches de seguridad cubren vulnerabilidades conocidas. Ejecutando el comando **sudo apt update && sudo apt upgrade** nos da este resultado:



```
debian [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Applications Places System

debian@debian: ~
File Edit View Search Terminal Help

debian@debian:~$ sudo apt update && sudo apt upgrade
[sudo] password for debian:
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
24 packages can be upgraded. Run 'apt list --upgradable' to see them.
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 libcupower1 libheif1 libjavascriptcoregtk-4.1-0
  libwebkit2gtk-4.1-0 linux-image-amd64 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
```


Evaluación de Seguridad

- **Puertos Abiertos y Expuestos:** Los puertos 21 (FTP), 22 (SSH), 80 (HTTP), 3306 (MySQL/MariaDB), y 631 (IPP) están abiertos y podrían ser potenciales vectores de ataque si no se configuran y aseguran correctamente.
- **Puerto 21 (FTP):** El protocolo FTP no es seguro por defecto, ya que envía datos sin cifrar. Si es necesario, considera reemplazarlo por una alternativa más segura como sftp.
- **Puerto 22 (SSH):** Asegúrate de que SSH esté configurado correctamente para evitar ataques de fuerza bruta. Considera medidas como la autenticación con clave pública y la restricción de acceso a ciertas direcciones IP.
- **Puerto 80 (HTTP):** Si Apache está abierto a internet, asegúrate de que esté configurado y actualizado para evitar vulnerabilidades.
- **Puerto 3306 (MySQL/MariaDB):** Asegúrate de que este puerto no esté expuesto a la red pública a menos que sea necesario. Limita el acceso solo a direcciones IP específicas o accede a la base de datos desde localhost.
- **Puerto 631 (CUPS):** Este servicio de impresión es mejor limitarlo a la red local, ya que podría exponer configuraciones innecesarias si está accesible externamente.

Recomendaciones Generales

1. **Firewall:** Considera configurar un firewall (iptables o ufw) para permitir solo las conexiones necesarias y limitar el acceso a los servicios críticos.
2. **Seguridad en SSH:** Usa autenticación de clave pública y desactiva el inicio de sesión con contraseña si es posible.
3. **FTP Seguro:** Considera alternativas seguras para FTP, como sftp o ftps.
4. **Restricción de Base de Datos:** Limita el acceso a MariaDB desde la red, y permite solo conexiones locales o desde direcciones IP específicas.

Identificación de usuarios no autorizados.

```
debian [Comiendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

debian@debian: ~
File Edit View Search Terminal Help
cat: /etc/passwd: No such file or directory
debian@debian:~$ cat /etc/passwd | awk -F: '{print $q}'
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
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:systemd 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
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
```

Búsqueda de backdoors

```
debian [Comiendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

debian@debian: ~
File Edit View Search Terminal Help
/var/cache/debconf/templates.dat
/var/cache/debconf/templates.dat-old
/var/cache/debconf/config.dat
/var/cache/man/da/CACHEDIR.TAG
/var/cache/man/da/index.db
/var/cache/man/sl/CACHEDIR.TAG
/var/cache/man/sl/index.db
/var/cache/man/CACHEDIR.TAG
/var/cache/man/zh_CN/CACHEDIR.TAG
/var/cache/man/zh_CN/index.db
/var/cache/man/sr/CACHEDIR.TAG
/var/cache/man/sr/index.db
/var/cache/man/id/CACHEDIR.TAG
/var/cache/man/id/index.db
/var/cache/man/it/CACHEDIR.TAG
/var/cache/man/it/index.db
/var/cache/man/fr/CACHEDIR.TAG
/var/cache/man/fr/index.db
/var/cache/man/uk/CACHEDIR.TAG
/var/cache/man/uk/index.db
/var/cache/man/cs/CACHEDIR.TAG
/var/cache/man/cs/index.db
/var/cache/man/es/CACHEDIR.TAG
/var/cache/man/es/index.db
/var/cache/man/zh/CACHEDIR.TAG
/var/cache/man/zh/index.db
/var/cache/man/ro/CACHEDIR.TAG
/var/cache/man/ro/index.db
/var/cache/man/ja/CACHEDIR.TAG
/var/cache/man/ja/index.db
/var/cache/man/pt_BR/CACHEDIR.TAG
/var/cache/man/pt_BR/index.db
/var/cache/man/pl/CACHEDIR.TAG
/var/cache/man/pl/index.db
```

Plan de Mitigación.

Primero, se realiza una identificación y evaluación de servicios vulnerables mediante herramientas de análisis como Nmap, verificando los puertos abiertos y los servicios que los ocupan. En este caso, los servicios FTP en el puerto 21, SSH en el puerto 22, IPP en el puerto 80, HTTP en el puerto 631 y MySQL en el puerto 3306 requieren evaluación. El siguiente paso es revisar los registros del sistema en busca de actividades sospechosas, incluyendo intentos de conexión inusuales, fallos de autenticación y cambios inesperados en archivos de configuración. En Debian, se examinan los logs en directorios como `/var/log/auth.log` y `/var/log/syslog`, prestando atención a los accesos SSH y otros intentos de conexión remota no autorizados.

Para mitigar el ataque, se inicia una serie de pasos enfocados en limitar el acceso a estos servicios vulnerables. En primer lugar, se ajustan las configuraciones de firewall utilizando iptables o UFW para restringir el acceso a ciertos puertos únicamente desde direcciones IP de confianza o internas, limitando así la exposición de servicios como FTP y SSH. Para FTP, se puede optar por deshabilitar el servicio temporalmente o restringirlo solo a conexiones internas si no es necesario para usuarios externos. En el caso de SSH, una de las medidas de mitigación es modificar el archivo de configuración (`/etc/ssh/sshd_config`) para deshabilitar el acceso root directo, cambiar el puerto por defecto y habilitar autenticación mediante claves en lugar de contraseñas. Además, se monitorea MySQL restringiendo su acceso solo a localhost si no se requiere acceso remoto, y ajustando los permisos de usuarios y configuraciones de seguridad en la base de datos.

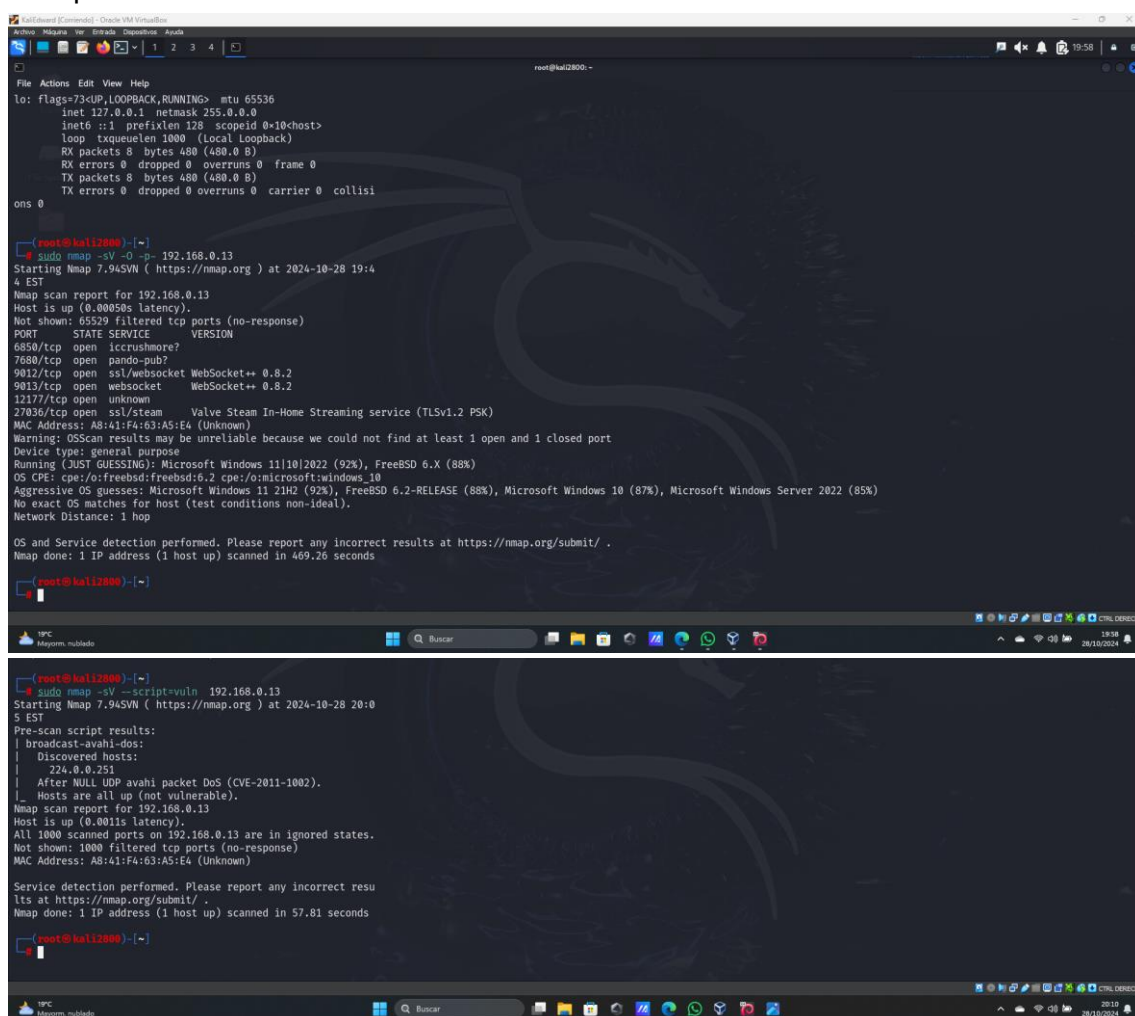
Para prevenir futuros ataques de la misma índole, se recomienda establecer un cronograma de actualizaciones periódicas, asegurando que tanto el sistema operativo Debian como los servicios y paquetes instalados estén en sus versiones más recientes y seguras. Es importante realizar escaneos de vulnerabilidades regulares con herramientas como OpenVAS o Nessus, lo que permite detectar y corregir vulnerabilidades antes de que puedan ser explotadas. Además, es recomendable fortalecer la autenticación en SSH configurando un límite en el número de intentos de autenticación, o incluso habilitando la autenticación de múltiples factores.

Fase 2: Detecta y corrige una vulnerabilidad diferente.

Objetivo: Escanear, detectar y explotar una vulnerabilidad diferente a la explotada anteriormente y crear un informe que explique todo el proceso.

1. Realizamos un escaneo completo del sistema usando herramientas como Nmap.

Usamos Nmap para realizar un escaneo completo del sistema objetivo y descubrir los puertos y servicios abiertos, incluyendo configuraciones potencialmente vulnerables.



```
root@kali2800:~#  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 8 bytes 480 (480.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 8 bytes 480 (480.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisi  
ons 0  
  
root@kali2800:~#  
root@kali2800:~# sudo nmap -sV -O -p- 192.168.0.13  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 19:4  
4 EST  
Nmap scan report for 192.168.0.13  
Host is up (0.00050s latency).  
Not shown: 65529 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
6850/tcp  open  iccrushmore?  
7680/tcp  open  pando-pub?  
9012/tcp  open  ssl/websocket WebSocket++ 0.8.2  
9013/tcp  open  websocket    WebSocket++ 0.8.2  
12177/tcp open  unknown  
27036/tcp open  ssl/steam    Valve Steam In-Home Streaming service (TLSv1.2 PSK)  
MAC Address: AB:41:F4:63:A5:E4 (Unknown)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%), FreeBSD 6.X (88%)  
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10  
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (87%), Microsoft Windows Server 2022 (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
  
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 469.26 seconds  
  
root@kali2800:~#  
root@kali2800:~# sudo nmap -sV --script=vuln 192.168.0.13  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 20:0  
5 EST  
Pre-scan script results:  
| broadcast-avahi-dos:  
| Discovered hosts:  
| 724.0.0.251  
| After NULL UDP avahi packet DoS (CVE-2011-1002).  
| Hosts are all up (not vulnerable).  
Nmap scan report for 192.168.0.13  
Host is up (0.0011s latency).  
All 1000 scanned ports on 192.168.0.13 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: AB:41:F4:63:A5:E4 (Unknown)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 57.81 seconds
```

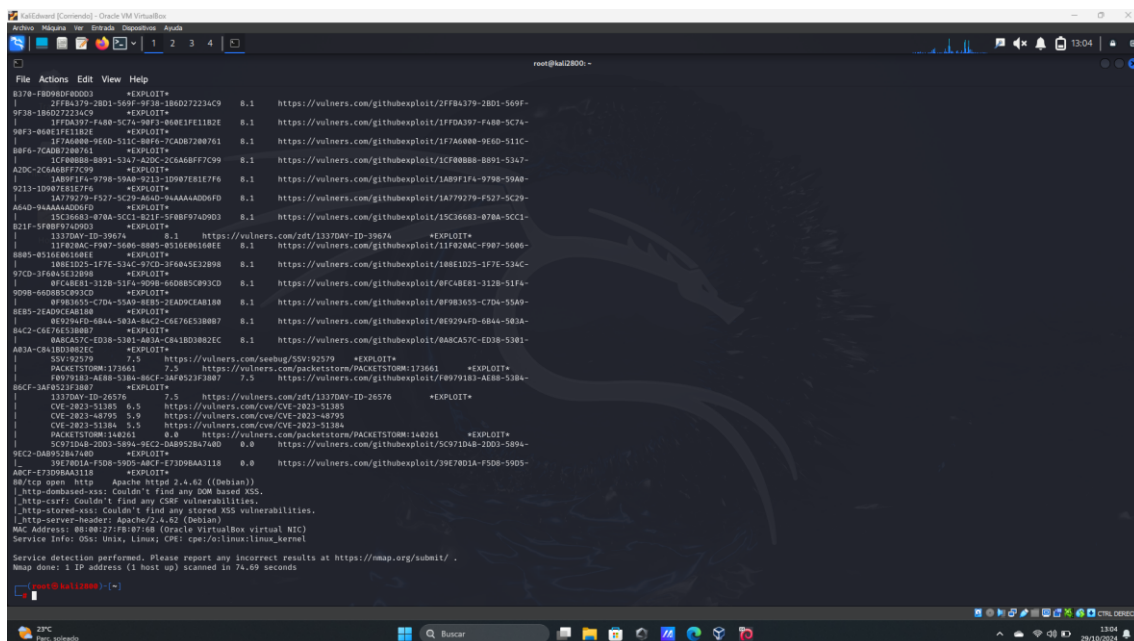
En este caso detectamos la vulnerabilidad en avahi-coresocket.c en Avahi que detalla: avahi-core/socket.c en avahi-daemon en Avahi antes de v0.6.29 permite a atacantes remotos provocar una denegación de servicio (bucle infinito) a través de un paquete UDP (1) IPv4 o (2) IPv6 vacíos al puerto 5353. NOTA: esta vulnerabilidad existe debido a una corrección incorrecta del CVE-2010-2244.

Se descubrió que avahi, una implementación del protocolo zeroconf, puede bloquearse de forma remota con un solo paquete UDP, lo que puede provocar una denegación de servicio. Para la distribución estable antigua (lenny), este problema se ha solucionado en la versión 0.6.23-3lenny3.

Para la distribución estable (squeeze), este problema se ha solucionado en la versión 0.6.27-2+squeeze1.

Para la distribución de prueba (wheezy) e inestable (sid), este problema se ha solucionado en la versión 0.6.28-4.

Le recomendamos que actualice sus paquetes de avahi.



Vulnerabilidad en Open SSH (CVE-2023-38408)

La característica PKCS#11 en ssh-agent en OpenSSH anterior a 9.3p2 tiene una ruta de búsqueda insuficientemente confiable, lo que lleva a la ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante. (El código en /usr/lib no es necesariamente seguro para cargar en ssh-agent). NOTA: este problema existe debido a una solución incompleta para CVE-2016 10009. Esta vulnerabilidad se encuentra en el puerto 22/tcp con el servicio SSH.

2. Detección de vulnerabilidades no relacionada con el hackeo anterior, como una mala configuración en Apache, puertos abiertos innecesarios, o un servicio expuesto y explota esta vulnerabilidad detectada.

```
(root@kali2800)-[~]
# searchsploit avahi

Exploit Title | Path
-----|-----
Avahi < 0.6.24 - mDNS Daemon Remote Denia | multiple/dos/7520.c

Shellcodes: No Results

(root@kali2800)-[~]
#
```

```
(root@kali2800)-[~]
# searchsploit OpenSSH

Exploit Title | Path
-----|-----
Debian OpenSSH - (Authenticated) Remote S | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_C | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Ex | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9 | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrit | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45210.py
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Of | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Toke | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer O | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer O | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege | linux/local/41173.c
OpenSSH 7.2 - Denial of Service | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Com | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execut | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation D | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary File | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote U | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discov | linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration | linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Ti | multiple/remote/3303.sh

Shellcodes: No Results

(root@kali2800)-[~]
#
```

Consultamos en la base de datos de vulnerabilidades (CVE Details o Exploit-DB) si la versión del servicio Apache tiene vulnerabilidades conocidas. Buscamos vulnerabilidades con: **searchsploit (nombre de la vulnerabilidad)**.

Verificación de Configuración Débil.

Resultado

El servidor respondió con una página predeterminada de Apache que indica que el servidor web está instalado y funcionando correctamente en la dirección 192.168.0.14. Esta página es conocida como la "Apache Debian Default Page", con el mensaje "It works!" (¡Funciona!).

Explicación del Contenido

1. **Encabezado HTML:** El documento comienza con una declaración DOCTYPE, seguida de etiquetas <html>, <head>, y <title>. Esto indica que la página es una respuesta HTML básica, configurada en el servidor web Apache.
2. **CSS Incorporado:** El servidor también entrega algunos estilos CSS internos, que definen la apariencia de esta página por defecto. Se especifican colores de fondo, alineación de texto, fuentes, y márgenes para la estructura de la página.
3. **Mensaje de Éxito:** Esta página predeterminada es una indicación de que Apache está funcionando correctamente, pero no hay un contenido personalizado configurado en la ruta principal. Esto suele ocurrir cuando el servidor web está instalado, pero no se ha configurado una página de inicio personalizada o una aplicación web.

En efecto, el servidor web Apache en 192.168.0.14 está mostrando una página por defecto, lo que podría indicar que el directorio público principal (/var/www/html/) es accesible sin restricciones. Esto podría ser un riesgo de seguridad si el servidor expone directorios o archivos sensibles que no deberían ser accesibles desde el exterior.

3. Escalación de privilegios.

El mismo se realiza para obtener permisos adicionales en un sistema, que permitan ejecutar acciones que normalmente estarían restringidas para el usuario actual.

```
Reading package lists... Done
root@debian:~# 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
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:systemd 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/s
bin/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
rtkit:x:109:119:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,:/var/lib/colord:/usr/sbi
n/nologin
debian:x:1000:1000:4geeks,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,:/srv/ftp:/usr/sbin/nologin
root@debian:~#
```

En primera instancia pudimos tener acceso como root de Debian en nuestra maquina Kali, a continuación, estaremos haciendo paso a paso del escalamiento de privilegios. Primero enumeramos usuarios con el comando (**cat /etc/passwd**), tal como lo muestra la imagen de arriba. Esto mostrará una lista de usuarios en el sistema.

Ahora buscamos archivos de configuración con el comando **find / -name "*.conf" -o -name "*.ini"**



```
KaliEdward [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

File  Actions  Edit  View  Help

sshd:x:112:65534::/run/ssh:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
root@debian:~# groups
root
root@debian:~# find / -name "*.conf" -o -name "*.ini"
/usr/lib/binfmt.d/python3.11.conf
/usr/lib/firefox-esr/browser/crashreporter-override.ini
/usr/lib/firefox-esr/crashreporter.ini
/usr/lib/firefox-esr/application.ini
/usr/lib/firefox-esr/platform.ini
/usr/lib/sysctl.d/50-bubblewrap.conf
/usr/lib/sysctl.d/50-pid-max.conf
/usr/lib/sysctl.d/99-protect-links.conf
/usr/lib/sysusers.d/polkitd.conf
/usr/lib/sysusers.d/systemd-network.conf
/usr/lib/sysusers.d/basic.conf
/usr/lib/sysusers.d/systemd-timesync.conf
/usr/lib/sysusers.d/dbus.conf
/usr/lib/sysusers.d/systemd-journal.conf
/usr/lib/kernel/install.conf
/usr/lib/environment.d/99-environment.conf
/usr/lib/tmpfiles.d/polkitd.conf
/usr/lib/tmpfiles.d/home.conf
/usr/lib/tmpfiles.d/gvfsd-fuse-tmpfiles.conf
/usr/lib/tmpfiles.d/systemd-network.conf
/usr/lib/tmpfiles.d/tmp.conf
/usr/lib/tmpfiles.d/journal-nocow.conf
/usr/lib/tmpfiles.d/passwd.conf
/usr/lib/tmpfiles.d/systemd-nologin.conf
/usr/lib/tmpfiles.d/systemd.conf
/usr/lib/tmpfiles.d/dbus.conf
/usr/lib/tmpfiles.d/systemd-pstore.conf
/usr/lib/tmpfiles.d/systemd-tmp.conf
/usr/lib/tmpfiles.d/man-db.conf
/usr/lib/tmpfiles.d/legacy.conf
/usr/lib/tmpfiles.d/x11.conf
/usr/lib/tmpfiles.d/sudo.conf
/usr/lib/tmpfiles.d/vsftpd.conf
/usr/lib/tmpfiles.d/debian.conf
/usr/lib/tmpfiles.d/var.conf
/usr/lib/tmpfiles.d/static-nodes-permissions.conf
/usr/lib/tmpfiles.d/speech-dispatcher.conf
/usr/lib/tmpfiles.d/colord.conf
/usr/lib/tmpfiles.d/provision.conf
/usr/lib/x86_64-linux-gnu/gconv/gconv-modules.d/gconv-modules-extra.conf
/usr/lib/modprobe.d/fbdev-blacklist.conf
/usr/lib/modprobe.d/systemd.conf
/usr/lib/modprobe.d/aliases.conf
/usr/lib/systemd/system/systemd-locale.service.d/locale-gen.conf
/usr/lib/systemd/system/rc-local.service.d/debian.conf
/usr/lib/systemd/system/mariadb@bootstrap.service.d/use_galera_new_cluster.conf
/usr/lib/systemd/system/user-.slice.d/10-defaults.conf
/usr/lib/systemd/system/user@.service.d/10-login-barrier.conf
```

Este comando nos ayuda a buscar archivos de configuración comunes que podrían contener información útil.

Fase 3: Plan de respuesta de incidentes y certificación.

Objetivo: Diseña un plan de respuesta a incidentes basado en las mejores prácticas y desarrolla un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001.

1. Plan de Respuesta a Incidentes (PRI).

El PRI debe cubrir las cuatro fases claves según el NIST SP 800-61, que son **Preparación, Detección y Análisis, Contención, Erradicación y Recuperación**

1.1 Preparación

- **Políticas y procedimientos:** Documentar políticas de respuesta a incidentes para estandarizar y agilizar las reacciones ante cualquier incidente de seguridad.
- **Entrenamiento:** Capacitar al equipo de TI y ciberseguridad en el protocolo de respuesta y en sus responsabilidades individuales.
- **Implementación de herramientas de monitoreo:** Configurar herramientas de detección de intrusiones (IDS), sistemas de gestión de eventos e información de seguridad (SIEM) y análisis de tráfico de red.
- **Comunicaciones:** Definir los canales y medios de comunicación internos y externos para manejar los incidentes y notificar a partes afectadas.

1.2 Detección y Análisis

- **Monitoreo de eventos:** Configurar alertas automáticas para identificar posibles incidentes. Esto incluye análisis de logs y alertas de comportamiento sospechoso.
- **Evaluación de impacto:** Clasificar el incidente según su impacto y riesgo, estableciendo el alcance del daño y qué sistemas fueron comprometidos.
- **Identificación y diagnóstico:** Determinar la naturaleza del ataque (por ejemplo, ransomware, exfiltración de datos, etc.).

1.3 Contención, Erradicación y Recuperación.

Contención	<ul style="list-style-type: none">• Contención inmediata: Aislar sistemas comprometidos para evitar la propagación.• Contención a largo plazo: Implementar soluciones temporales (p. ej., firewalls o parches) mientras se diseña una solución definitiva.
-------------------	---

Erradicación	<ul style="list-style-type: none"> • Eliminación de amenazas: Limpiar sistemas afectados, eliminar malware y aplicar parches de seguridad. • Fortalecimiento de seguridad: Actualizar credenciales comprometidas y realizar escaneos para asegurarse de que no quedan amenazas.
Recuperación	<ul style="list-style-type: none"> • Restauración de sistemas: Restaurar desde respaldos y realizar pruebas para verificar la funcionalidad. • Validación: Supervisar el sistema recuperado para asegurarse de que no hay actividad sospechosa y que las operaciones vuelven a la normalidad.

2. Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO 27001.

El SGSI debe cumplir con la norma ISO 27001, estableciendo un ciclo de mejora continua para gestionar riesgos de seguridad de la información. Las fases principales son **Análisis de Riesgos, Políticas de Seguridad, Implementación de Controles, y Auditoría y Revisión.**

2.1 Análisis de Riesgos

- **Identificación de activos:** Catalogar activos de información críticos (datos, sistemas, infraestructura).
- **Evaluación de riesgos:** Analizar amenazas y vulnerabilidades de cada activo para priorizar según el nivel de riesgo.
- **Plan de tratamiento de riesgos:** Definir acciones y controles necesarios para mitigar los riesgos identificados.

2.2 Definición de Políticas de Seguridad

- **Políticas y procedimientos de seguridad:** Establecer un marco que incluya políticas de acceso, uso de la información y gestión de incidentes.

- **Clasificación de la información:** Asignar niveles de confidencialidad y acceso según la sensibilidad de los datos.
- **Responsabilidades y roles:** Definir roles de seguridad y responsabilidades en todos los niveles de la organización.

2.3 Implementación de Controles

- **Controles de acceso:** Implementar controles de acceso basados en roles (RBAC) y autenticación multifactorial para limitar el acceso a información sensible.
- **Cifrado y protección de datos:** Cifrar datos en tránsito y en reposo, así como implementar controles de protección perimetral.
- **Respaldos periódicos:** Establecer respaldos automáticos de datos críticos en múltiples ubicaciones y realizar pruebas de restauración.
- **Concientización y capacitación:** Impartir programas de concientización sobre seguridad y entrenar al personal para reconocer y responder a amenazas.

2.4 Auditoría y Revisión

- **Monitoreo y auditoría:** Implementar un programa de auditoría continua para evaluar la efectividad del SGSI y el cumplimiento con la norma.
- **Revisión de desempeño:** Evaluar el rendimiento del SGSI periódicamente para identificar áreas de mejora.
- **Mejora continua:** Adaptar el sistema según los hallazgos de auditorías y cambios en el entorno de amenazas.

3. Implementación de Mecanismos de Protección de Datos.

- **Respaldos periódicos:** Programar respaldos automáticos y seguros de datos críticos, y establecer un sistema de recuperación ante desastres.
- **Cifrado de datos sensibles:** Cifrar información tanto en tránsito como en reposo, utilizando algoritmos seguros (AES-256, RSA).
- **Controles de acceso estrictos:** Implementar políticas de acceso mínimo (principio de privilegios mínimos) y autenticación multifactor para áreas de información crítica.
- **Segmentación de red:** Separar redes sensibles de otras áreas de la organización para reducir la superficie de ataque.

- **Monitoreo y análisis de actividad:** Configurar sistemas de monitoreo continuo (SIEM) para detectar y alertar sobre actividades anómalas en tiempo real.

Diagrama de red utilizando Packet Tracer.

