

Análisis Forense y Hardering del Servidor de 4GeeksAcademy

Autor: Adrià Coll Ortega

Fecha: 16/07/2025

Curso: spain-cs-pt-6

Profesores: Raúl Moncada y Javier Álvarez

Repositorio [GITHUB](#)



INTRODUCCIÓN

Objetivo: Simulación de un análisis forense y hardening en un servidor Debian comprometido













El informe se basa en 3 fases:

- ❖ **Fase_1:** Reconocimiento y recolección de evidencias
- ❖ **Fase_2:** Detectar y corregir una vulnerabilidad distinta
- ❖ **Fase_3:** Plan de respuesta a incidentes y certificación

Máquinas usadas a lo largo del proyecto:

- ❖ **Máquina host:** Windows_11 Pro
- ❖ **Máquina Atacante:** VM Kali Linux
- ❖ **Máquina Víctima:** VM Servidor Debian

Para este punto, he empezado primeramente con un análisis usando el software de Autopsy

▼ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
 wtmp				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	21888	Allocated	Allocated	unknown
 speech-dispatcher				2022-11-25 14:04:48 CEST	2024-07-31 19:41:08 CEST	2024-07-31 19:29:45 CEST	2024-07-31 19:38:30 CEST	4096	Allocated	Allocated	unknown
 runit				2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST	2024-09-30 18:25:12 CEST	2024-09-30 18:25:13 CEST	4096	Allocated	Allocated	unknown
 private				2024-10-31 18:14:40 CEST	2024-07-31 18:14:40 CEST	2024-07-31 18:14:40 CEST	2024-07-31 18:14:40 CEST	4096	Allocated	Allocated	unknown
 lightdm				2024-10-08 23:28:53 CEST	2024-10-08 23:28:39 CEST	2024-07-31 21:57:12 CEST	2024-07-31 21:57:12 CEST	4096	Allocated	Allocated	unknown
 lastlog				2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	0	Allocated	Allocated	unknown
 journal				2024-07-31 21:56:39 CEST	2024-07-31 21:56:39 CEST	2024-09-30 18:46:01 CEST	2024-07-31 18:14:39 CEST	4096	Allocated	Allocated	unknown
 installer				2024-07-31 21:56:26 CEST	2024-07-31 21:56:26 CEST	2024-07-31 21:56:25 CEST	2024-07-31 21:56:24 CEST	4096	Allocated	Allocated	unknown
 fontconfig.log				2024-09-30 16:40:22 CEST	2024-09-30 16:40:22 CEST	2024-07-31 19:40:23 CEST	2024-07-31 19:40:23 CEST	5602	Allocated	Allocated	unknown
 faillog				2024-07-31 18:14:33 CEST	2024-07-31 18:14:33 CEST	2024-07-31 18:14:33 CEST	2024-07-31 18:14:33 CEST	0	Allocated	Allocated	unknown
 dupslog				2024-10-08 22:15:01 CEST	2024-10-08 22:15:01 CEST	2024-07-31 18:12:55 CEST	2024-07-31 18:12:55 CEST	765828	Allocated	Allocated	unknown
 cups				2024-07-31 21:57:14 CEST	2024-07-31 21:57:14 CEST	2024-09-30 18:48:37 CEST	2024-07-31 19:28:51 CEST	4096	Allocated	Allocated	unknown

▼	name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
▼	stmp				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	21880	Allocated	Allocated	unknown
▼	speed-dispatcher				2022-11-25 14:04:48 CEST	2024-07-31 19:41:08 CEST	2024-07-31 19:29:45 CEST	2024-07-31 19:38:30 CEST	4096	Allocated	Allocated	unknown
▼	nunit				2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST	4096	Allocated	Allocated	unknown
▼	private				2024-07-31 18:14:40 CEST	2024-07-31 18:14:40 CEST	2024-07-31 18:14:40 CEST	2024-07-31 18:14:40 CEST	4096	Allocated	Allocated	unknown
▼	lightdm				2024-10-08 23:28:39 CEST	2024-10-08 23:28:39 CEST	2024-07-31 21:57:12 CEST	2024-07-31 21:57:12 CEST	4096	Allocated	Allocated	unknown
▼	lastlog				2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	2024-07-31 18:13:56 CEST	0	Allocated	Allocated	unknown
▼	journal				2024-07-31 21:56:39 CEST	2024-07-31 21:56:39 CEST	2024-09-30 16:40:01 CEST	2024-07-31 21:56:39 CEST	4096	Allocated	Allocated	unknown
▼	installer				2024-07-31 21:56:26 CEST	2024-07-31 21:56:26 CEST	2024-07-31 21:56:25 CEST	2024-07-31 21:56:26 CEST	4096	Allocated	Allocated	unknown
▼	fontconfig.log				2024-09-30 16:40:22 CEST	2024-09-30 16:40:22 CEST	2024-07-31 19:40:23 CEST	2024-07-31 19:40:23 CEST	5652	Allocated	Allocated	unknown
▼	faillog				2024-07-31 18:14:33 CEST	2024-07-31 18:14:33 CEST	2024-07-31 18:14:33 CEST	2024-07-31 18:14:33 CEST	0	Allocated	Allocated	unknown
▼	dpkg.log				2024-10-08 22:51:01 CEST	2024-10-08 22:51:01 CEST	2024-07-31 18:15:55 CEST	2024-07-31 18:15:55 CEST	765626	Allocated	Allocated	unknown
▼	cups				2024-07-31 21:57:14 CEST	2024-07-31 21:57:14 CEST	2024-09-30 15:48:37 CEST	2024-07-31 19:28:31 CEST	4096	Allocated	Allocated	unknown

[Hex](#)
[Text](#)
[Application](#)
[File Metadata](#)
[OS Account](#)
[Data Artifacts](#)
[Analysis Results](#)
[Context](#)
[Annotations](#)
[Other Occurrences](#)

[Strings](#)
[Extracted Text](#)
[Translation](#)

Page: 1 of 2
 [Page](#)

[Go to Page:](#)

Script: Latin - Basic

FASE_1: RECONOCIMIENTO Y EVIDENCIAS

Nos salimos de Autopsy y pasamos al ataque con la VM Kali Linux para obtener más información

```
(adri@kali)-[~]
$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:84:38:da brd ff:ff:ff:ff:ff:ff
    inet 10.171.158.203/24 brd 10.171.158.255 scope global dynamic noprefixroute eth0
        valid_lft 3550sec preferred_lft 3550sec
    inet6 fe80::20c:29ff:fe84:38da/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
(adri@kali)-[~]
$ nmap 10.171.158.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 01:39 CEST
Nmap scan report for 10.171.158.204
Host is up (0.00084s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:C8:E9:E6 (VMware)

Nmap scan report for 10.171.158.205
Host is up (0.00058s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

PRIVATE

```
Nmap scan report for 10.171.158.203
Host is up (0.00028s latency).
All 1000 scanned ports on 10.171.158.203 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
Nmap done: 256 IP addresses (4 hosts up) scanned in 35.55 seconds
```

```
(adri@kali)-[~]
$ nmap -sS -sV -O -p- 10.171.158.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 01:48 CEST
Nmap scan report for 10.171.158.204
Host is up (0.00070s 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))
MAC Address: 00:0C:29:C8:E9:E6 (VMware)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linu
x_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 35.20 seconds
```

Resumen de Escaneo Nmap

IP Escaneada: 10.171.158.204

MAC Address: 00:0C:29:C8:E9:E6 (VMware)

Puerto	Estado	Servicio	Versión	Vulnerabilidades Conocidas
21/tcp	Open	FTP	vsftpd 3.0.3	CVE-2021-42785 (DoS), CVE-2020-15719 (directory traversal)
22/tcp	Open	SSH	OpenSSH 9.2p1 Debian 2+deb12u3	CVE-2023-48795 (Terrapin attack)
80/tcp	Open	HTTP	Apache httpd 2.4.62 (Debian)	CVE-2023-25690 (HTTP Request Smuggling)

FASE_1: RECONOCIMIENTO Y EVIDENCIAS

Una vez confirmamos que tenemos acceso al servidor Debian, lo primero que hacemos es un **`sudo aptl update && sudo apt upgrade -y`**, que ha durado un buen rato.

```
(adri@kali)-[~]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] contraseña para adri:

(adri@kali)-[~]
$ hydra -l debian -P /usr/share/wordlists/rockyou.txt ftp://10.171.158.204 -t 4 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-16 02:21:28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per
task
[DATA] attacking ftp://10.171.158.204:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.171.158.204 - login "debian" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 10.171.158.204 - login "debian" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 10.171.158.204 - login "debian" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 10.171.158.204 - login "debian" - pass "password" - 4 of 14344399 [child 3] (0/0)
[21][ftp] host: 10.171.158.204 login: debian password: 123456
[STATUS] attack finished for 10.171.158.204 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-16 02:21:34
```

FASE_1: RECONOCIMIENTO Y EVIDENCIAS

En este punto toca hacer el escáner de **rootkits** y **malware**, para saber si el/los atacantes han dejado algún fichero perjudicial en el servidor.

Resultados de **chkrootkit**

```
/usr/lib/libreoffice/share/.registry: WARNING
```

```
Output from ifpromisc: WARNING
```

```
WARNING: Output from ifpromisc:
```

```
lo: not promisc and no packet sniffer sockets
```

```
ens33: PACKET SNIFFER(/usr/sbin/NetworkManager[41231], /usr/sbin/NetworkManager[41231])
```

Resultados de **ClamAV**

```
----- SCAN SUMMARY -----
Known viruses: 8707603
Engine version: 1.0.7
Scanned directories: 36279
Scanned files: 176061
Infected files: 0
Total errors: 1038
Data scanned: 8853.20 MB
Data read: 7197.16 MB (ratio 1.23:1)
Time: 2613.228 sec (43 m 33 s)
Start Date: 2025:07:16 00:20:39
End Date: 2025:07:16 01:04:12
```

Juntando los resultados de **chkrootkit** y el escáner completo del sistema del antivirus **ClamAV**, vemos que no hemos encontrado ningún tipo de malware en el servidor.

Resultado normal después de haber actualizado y renovado la gran mayoría de dependencias del sistema

FASE_1: RECONOCIMIENTO Y EVIDENCIAS

Ahora que ya sabemos los principales problemas/vulnerabilidades del servidor Debian, toca pasar a la acción para remediarlas.

Instalación y configuración de reglas del firewall ufw

Empezamos con la instalación del firewall **ufw** (usado anteriormente en el curso), y añadimos las siguientes reglas:

- ❖ `sudo ufw default deny incoming`
- ❖ `sudo ufw default allow outgoing`
- ❖ `sudo ufw allow from <IP_KALI_LINUX> to any port 22`
- ❖ `sudo ufw enable`

```
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 10.171.158.203 to any port 22
Rules updated
debian@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
debian@debian:~$
```

FTP: Empezamos directamente eliminando el servicio **vsftpd**, ya que no le encuentro un motivo fundamental para mantenerlo. Importante también cerrar el puerto en el firewall mediante el comando `sudo ufw deny 21/tcp` (si no tenemos ningún servicio expuesto, entonces es mejor cerrar el puerto).

SSH: En este caso sí voy a dejar activo el servicio SSH, porque al fin y al cabo se trata de un servidor Debian que, en algún momento, puede requerir de conexión remota para ser gestionado en el futuro.

Para ello, requiere de una modificación en la configuración del servicio **ssh**. Lo haremos a partir del fichero `/etc/ssh/ssh_config`. La configuración es la siguiente:

```
#1 Deshabilitar características inseguras
HostbasedAuthentication no
GSSAPIAuthentication no
PasswordAuthentication no
PermitEmptyPasswords no
ChallengeResponseAuthentication no
PermitRootLogin no

#2 Configuración de Privacidad
StrictHostKeyChecking yes
HashKnownHosts yes
AddressFamily inet
ConnectTimeout 30
TCPKeepAlive no
```

PermitRootLogin no: Niega el inicio de sesión como root.

PermitEmptyPasswords no: Bloquea cuentas con contraseña vacía

FASE_1: RECONOCIMIENTO Y EVIDENCIAS

```
root@debian:/run/user/1000# passwd debian
New password:
Retype new password:
passwd: password updated successfully
root@debian:/run/user/1000# exit
exit
```

Nueva contraseña: **XqbmKfpt.45!**

```
(adri@kali)-[~]
$ ssh debian@10.171.158.204
debian@10.171.158.204's password:
Linux debian 6.1.0-37-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.140-1 (2025-05-22) 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 new mail.
Last login: Tue Jul 15 23:12:04 2025 from 10.171.158.203
debian@debian:~$ exit
logout
Connection to 10.171.158.204 closed.

(adri@kali)-[~]
$
```

```
Hardening index : 63 [#####]
Tests performed : 262
Plugins enabled : 1

Comments :
- Firewall [V]
- Malware scanner [V]
```

Resultados de un escaneo básico de auditoria con la herramienta [Lynis](#)

Fase_2: Detectar y corregir una vulnerabilidad distinta

```
Warnings (1):
! Couldn't find 2 responsive nameservers [NETW-2705]
https://cisofy.com/lynis/controls/NETW-2705/

Suggestions (55):

* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
https://cisofy.com/lynis/controls/DEB-0280/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
https://cisofy.com/lynis/controls/DEB-0810/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are
old versions of libraries and need restarting. [DEB-0831]
https://cisofy.com/lynis/controls/DEB-0831/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-512]
https://cisofy.com/lynis/controls/BOOT-512/

* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
https://cisofy.com/lynis/controls/BOOT-5264/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
https://cisofy.com/lynis/controls/KRNL-5820/

* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
https://cisofy.com/lynis/controls/AUTH-9262/

* When possible set expire dates for all password protected accounts [AUTH-9282]
https://cisofy.com/lynis/controls/AUTH-9282/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
```

```
Hardening index : 11 [#####]
Tests performed : 382
Plugins enabled : 1
```

```
Components :
- Firewall [V]
- Malware scanner [V]
```





Fase_3: Plan de respuesta de incidentes

1.Preparación

- ❖ Creación de un equipo CSIRT con roles de Líder de Respuesta, Analista Forense, Administrador de Sistemas y Responsable de comunicación.

2.Detección y análisis

- ❖ Priorizar análisis de logs, servicios vulnerables a ejecución remota, contención de **backdoors**, etc.

3.Contención

- ❖ Corto plazo: Aislamiento del servidor de la red y cambio de contraseñas
- ❖ Largo plazo: Actualización de los servicios vulnerables (`sudo apt upgrade <Dependencia> -y`) y cierre de puertos innecesarios.

4.Erradicación

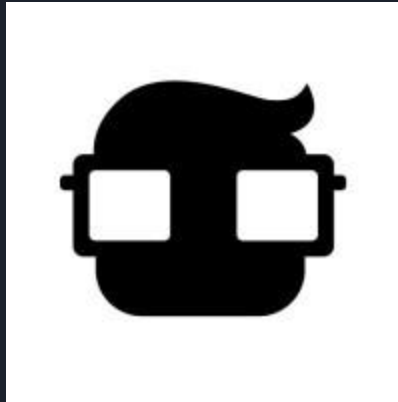
- ❖ Eliminación de archivos maliciosos. NOTA: En nuestro análisis, este paso no ha sido necesario.

5.Recuperación

- ❖ Validación de los servicios restaurados (`systemctl status <servicio>`)
- ❖ Implantación del antivirus ClamAV

6.Lecciones Aprendidas

- ❖ Hardening de la máquina (SSH en nuestro caso)
- ❖ Parches automáticos
- ❖ Análisis post-incidentes



MUCHAS GRACIAS POR LA ATENCIÓN