

# INFORME EJECUTIVO DE INCIDENTE DE SEGURIDAD – SERVIDOR DEBIAN

Simón A. Cervantes Martínez  
14 de abril de 2024



# Fase 1 – Corrección del Hackeo

- Identificación del incidente mediante análisis forense (Autopsy).
- Detección del vector de ataque: FTP anónimo, SSH inseguro.
- Bloqueo y documentación del exploit inicial.
- Capturas del uso de Hydra y Nmap.

```
(kali@kali)-[~]  
$ nmap -sS -sV -O -p- 10.0.2.22
```

```
(kali@kali)-[~]  
$ nmap -sS -sV -O -p- 10.0.2.22  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-04 14:13 EDT  
Nmap scan report for 10.0.2.22  
Host is up (0.0011s 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:A9:AF:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
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:linux_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 45.63 seconds
```

# Revisar logins sospechosos

`sudo grep 'Accepted\\|Failed' /var/log/auth.log`

```
debian@debian:/var/log$ ls  
alternatives.log  boot.log  cups      fontconfig.log  lightdm  speech-dispatcher  
alternatives.log.1 boot.log.1 dpkg.log  installer       private  wtmp  
apache2           btmp     dpkg.log.1 journal         README   Xorg.0.log  
apt              btmp.1   faillog   lastlog         runit    Xorg.0.log.old
```

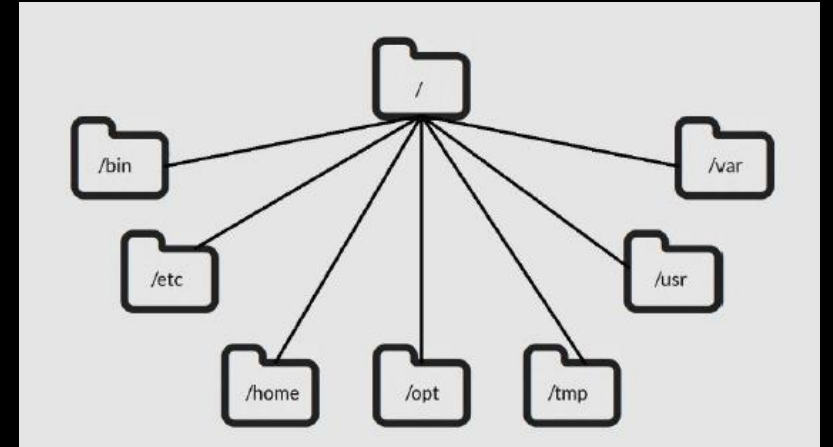
**Noto que los logs han sido borrados o alterados!**

Esto es **una señal clara de intrusión**. El atacante muy probablemente:

- Entró por **FTP o SSH**, y
- **Borró los registros** para ocultar su acceso.

# Fase 2 – Detección y Corrección de Vulnerabilidades

- Contraseñas débiles en MySQL.
- Permisos inseguros (FTP, SSH, wp-config.php).
- Servicios innecesarios con puertos abiertos.
- Listado de directorios web expuestos.
- Capturas de configuraciones corregidas.



```
(kali㉿kali)-[/usr/share/wordlists]
$ hydra -l debian -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.22 -t 4 -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-13 10:31:08
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~35
86100 tries per task
[DATA] attacking ssh://10.0.2.22:22/
[ATTEMPT] target 10.0.2.22 - login "debian" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 10.0.2.22 - login "debian" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 10.0.2.22 - login "debian" - pass "123456789" - 3 of 14344399 [child 2] (0/
0)
[ATTEMPT] target 10.0.2.22 - login "debian" - pass "password" - 4 of 14344399 [child 3] (0/0
)
[22][ssh] host: 10.0.2.22 login: debian password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-13 10:31:12
```



# Fase 3 – Respuesta y Certificación

- Aplicación de SGSI basado en ISO 27001.
- Firewall UFW, fail2ban y hardening SSH.
- Backups cifrados y monitoreo con Wazuh.
- Checklist de recuperación y pruebas.

- **Firewall y controles de acceso de red:** Implementa reglas de firewall (iptables/ufw o firewalld) para permitir solo el tráfico necesario. Por ejemplo, limita SSH a IPs de confianza o puertos no estándar, cierra puertos no utilizados, etc. Esto contiene movimientos del atacante en caso de futuras brechas.

```
sudo apt install ufw -y
```

```
sudo ufw default deny incoming
```

```
sudo ufw allow from <IP_KALI> to any port 22
```

```
sudo ufw allow 80,443/tcp
```

```
sudo ufw enable
```

```
debian@debian:/$ sudo apt install ufw -y
^Ziting for cache lock: Could not get lock /var/lib/dpkg/lock-frontent. It is held by process 186692 (apt)... 9s
[2]+  Stopped                  sudo apt install ufw -y
debian@debian:/$
```

## 2. METODOLOGÍA DE ANÁLISIS

- **Enfoque Normativo y Marco de Trabajo**
  - Proyecto es estructurado bajo en enfoque estructurado basado en estándares
  - NIST SP 800-61
  - ISO/IEC 27001:2022
  - ISO/IEC 27035
  - Ciclo forense tradicional forense tetages
- **Fases Técnicas del Ciclo Forense Aplicado**
  - Identificación sistemática forense estages:
    - Identificación
    - Adquisición
    - Preservación
    - Análisis
    - Erradicación
    - Docuperación

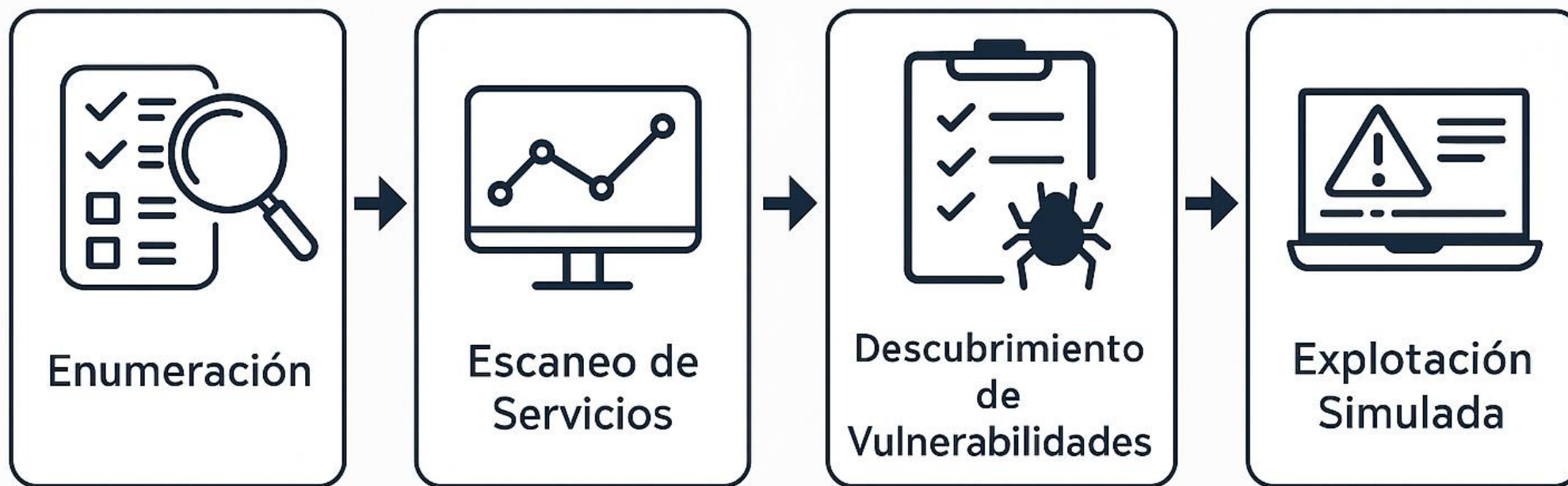
### Integración con el Ciclo de Respuesta (NIST SP 800-61)

- Aplicado al NIST SP 800-61 aplicand connuma:



- Integración con el Ciclo de Respuesta (NIST SP 800-61)

# Flujo de Pentesting



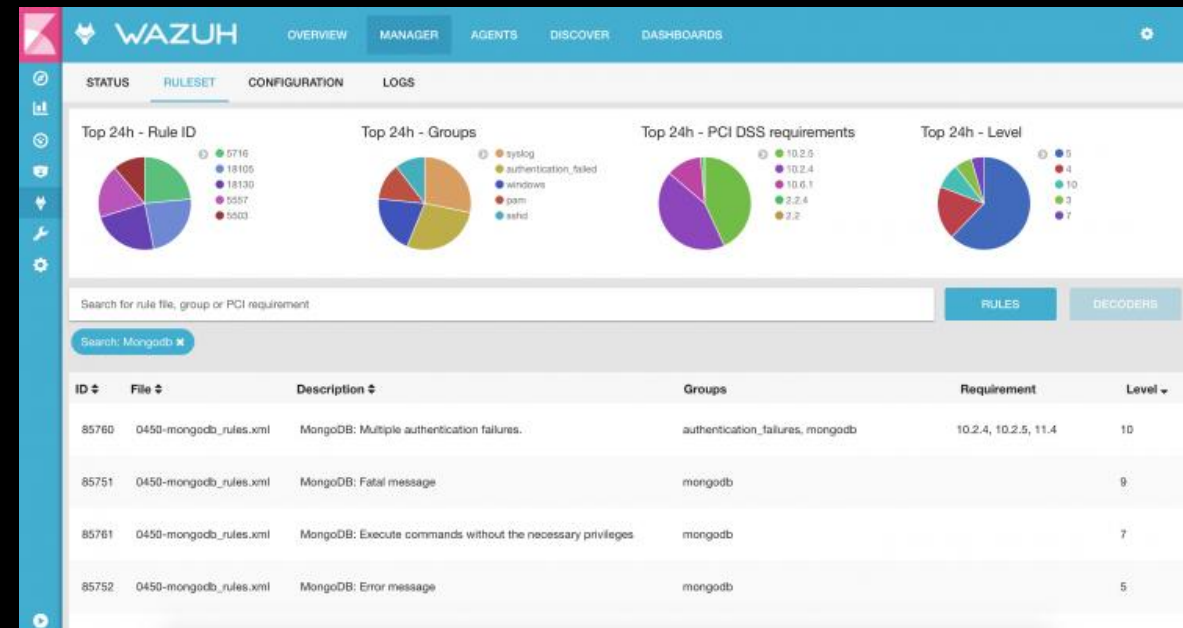


# Acciones Correctivas y Preventivas

- ✓ Corrección del FTP vulnerable.
- ✓ Reforzamiento de políticas SSH y acceso administrativo.
- ✓ Instalación de firewall, fail2ban, y control de puertos.
- ✓ Procedimientos documentados para respuesta futura.



```
debian@debian:~$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
debian@debian:~$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
debian@debian:~$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
debian@debian:~$ sudo ufw allow from 10.0.2.8 to any port 22 proto tcp
Rules updated
debian@debian:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
debian@debian:~$
```



# Cadena de Custodia & Anti-Foreense

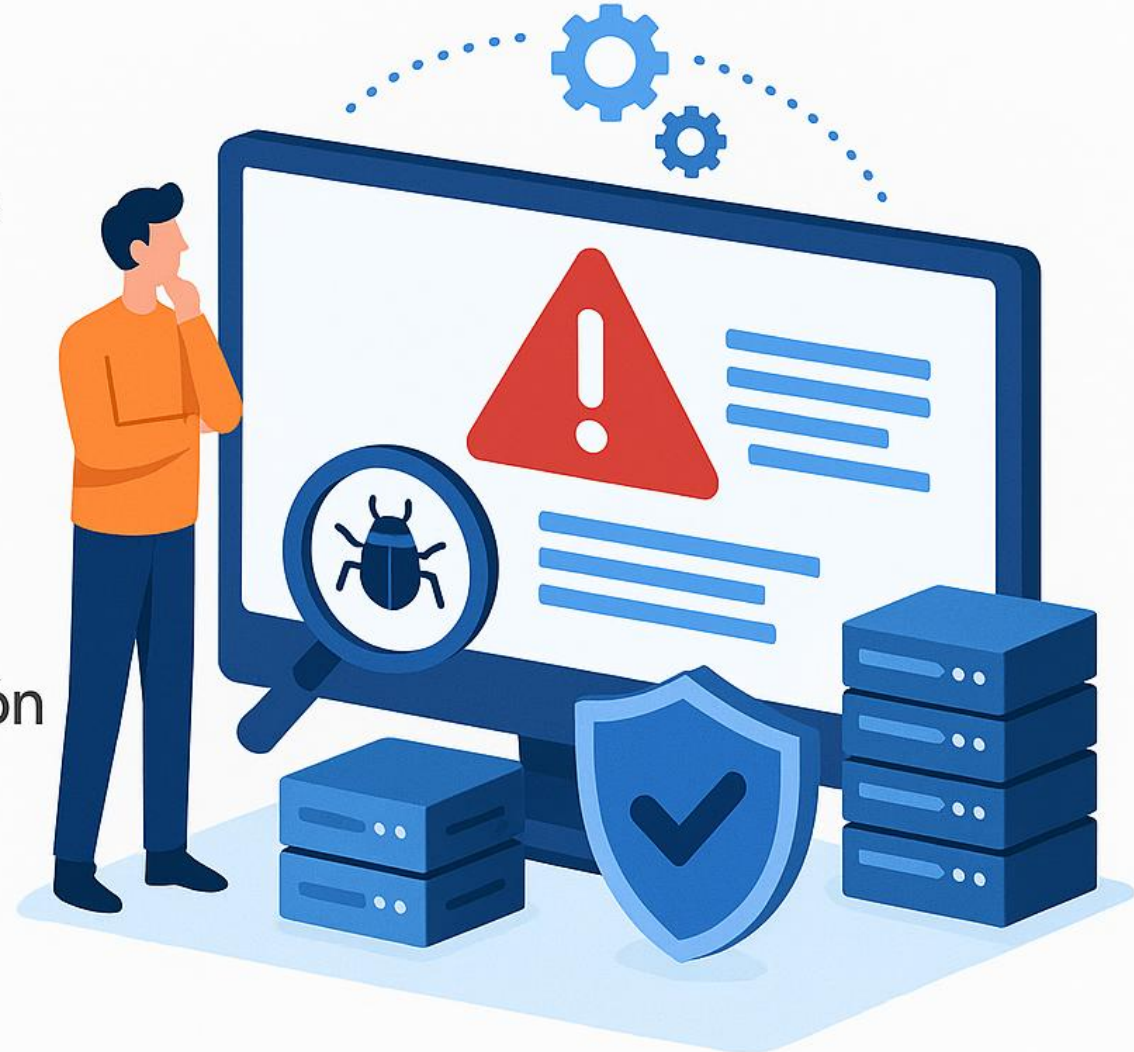
- Análisis de la cadena de custodia para garantizar la integridad de la evidencia
- Detección de técnicas anti-forense: borrado de huellas, modificación de metadatos, ofuscación, etc.





# RESPUESTA A INCIDENTES

- Identificación y clasificación de incidentes
- Contención para limitar daños
- Eliminación de amenazas detectadas
- Recuperación y restauración de sistemas



# ANÁLISIS FORENSE DIGITAL

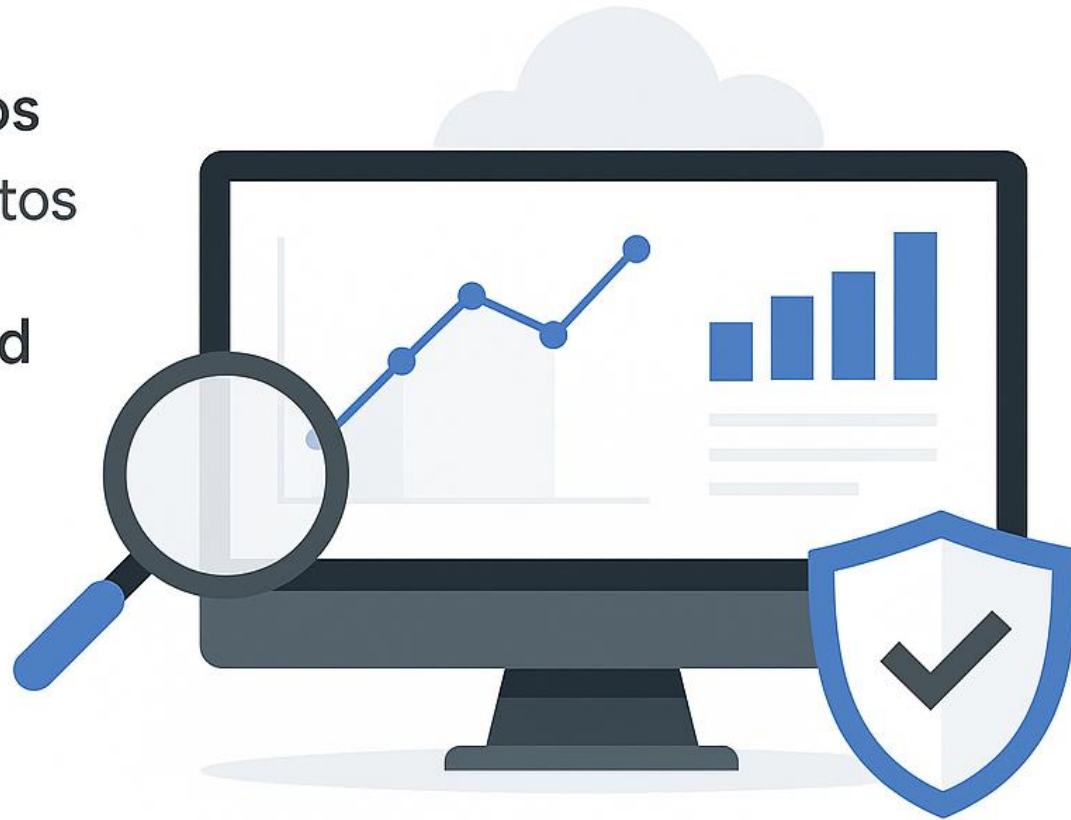
- Colección y examinación de pruebas digitales
- Utilización de herramientas especializadas
- Generación de informes forenses detallados



# Monitoreo de Seguridad (Instrumentación)

---

- **Recopilación de registros**  
Reunión de datos de eventos
- **Análisis del tráfico de red**  
Evaluación de paquetes y conexiones
- **Alertas y notificaciones**  
Detección de actividades sospechosas





# Desarrollo de Contramedidas

- Implementación de parches y actualizaciones de seguridad
- Mejora en las políticas de configuración y acceso
- Fortalecimiento de la capacitación en seguridad



# Plan de Recuperación ante Incidentes

- Establecimiento de backups automáticos y cifrados.
- Manual de contingencia y respuesta rápida.
- Checklist post-incidente y validación de restauración segura.
- Pruebas regulares de recuperación de servicios críticos.



## 5 fases de un plan de respuesta a incidentes



### 1. Preparación

- Identificación de riesgos y vulnerabilidades potenciales
- Desarrollar contramedidas para hacerles frente



### 2. Detección y análisis

- Implantar métodos y herramientas de detección de amenazas
- Identificar el tipo de amenaza y el nivel de gravedad



### 3. Contención y erradicación

- Aislar los sistemas afectados
- Eliminar la causa raíz de la amenaza
- Implantar los parches de seguridad necesarios



### 4. Recuperación

- Restaurar los sistemas afectados
- Aplique copias de seguridad de los datos para restaurar los archivos perdidos
- Asegúrese de que todas las acciones de recuperación se ajustan a los requisitos legales y reglamentarios



### 5. Mejora continua

- Realice un análisis posterior al incidente
- Aborde las áreas susceptibles de mejora
- Revisar, probar y actualizar periódicamente el plan





# Resultados

- Reducción de superficie de ataque.
- Mejoras en detección y respuesta.
- Infraestructura reforzada.
- Contraseñas débiles detectadas
- Malas configuraciones corregidas
- Mejora en la seguridad en conectividad



# Conclusiones Finales

-  El incidente pudo haberse evitado mediante:
  - - Hardening inicial de servicios.
  - - Eliminación de software innecesario (ejm. WordPress mal configurado).
  - -Una política de contraseñas más seguras
  - -Evitar tener servicios desactualizados o abiertos innecesarios.
  - - Monitoreo activo de logs y accesos.
  - Capacitación continua en ciberseguridad
-  Lecciones aprendidas: importancia del SGSI, controles mínimos activos, y prácticas anti-forense del atacante.

# Recomendaciones Incibe





Gracias a 4Geeks Academy



Especial mención a los profesores:  
Raúl Moncada y Javier Álvarez

