

Reporte de incidente

16/07/2025

ESCANEO DE PUERTOS

- Se realizo un escaneo de puertos con nmap, estos son los resultados.

```
(kali㉿kali)-[~]
└─$ nmap -v 192.168.100.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 11:05 EDT
Initiating ARP Ping Scan at 11:05
Scanning 192.168.100.7 [1 port]
Completed ARP Ping Scan at 11:05, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:05
Completed Parallel DNS resolution of 1 host. at 11:05, 0.09s elapsed
Initiating SYN Stealth Scan at 11:05
Scanning 192.168.100.7 [1000 ports]
Discovered open port 22/tcp on 192.168.100.7
Discovered open port 80/tcp on 192.168.100.7
Discovered open port 21/tcp on 192.168.100.7
Completed SYN Stealth Scan at 11:05, 0.03s elapsed (1000 total ports)
Nmap scan report for 192.168.100.7
Host is up (0.00058s 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: 08:00:27:9E:CC:AE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
  Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.040KB)
```



ACCESO ROOT REMOTO EN MARIADB

- Configuración que permite conexiones administrativas desde cualquier red externa, facilitando el control completo de las bases de datos por atacantes.

```
Performing system configuration file checks
  Checking for an SSH configuration file          [ Found ]
  Checking if SSH root access is allowed          [ Warning ]
  Checking if SSH protocol v1 is allowed          [ Not set ]
  Checking for other suspicious configuration settings [ None found ]
  Checking for a running system logging daemon    [ Found ]
  Checking for a system logging configuration file [ Found ]
```

ACCESO ROOT REMOTO EN MARIADB

- Se encontró un acceso de un usuario no identificado mediante root.

```
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:28:38 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot f0a7292a18684f839b6d504398582d88 --
```

FTP CON ACCESO ANÓNIMO HABILITADO

FTP con acceso anónimo habilitado

- **Servicio de transferencia de archivos que no requiere credenciales, permitiendo la descarga/upload de archivos sin restricciones.**

```
debian@debian:~$ sudo systemctl list-units --type=service | grep -i ftp
vsftpd.service                      loaded active running vsftpd FTP server
debian@debian:~$ sudo grep -i "anonymous_enable" /etc/vsftpd.conf
anonymous_enable=YES
debian@debian:~$
```

CONTRASEÑAS DÉBILES

- Configuración que permite conexiones administrativas desde cualquier red externa, facilitando el control completo de las bases de datos por atacantes.

```
MariaDB [(none)]> SHOW GRANTS FOR 'user'@'localhost';
+-----+
| Grants for user@localhost
  |
+-----+
| GRANT ALL PRIVILEGES ON *.* TO `user`@`localhost` IDENTIFIED BY PASSWORD '*2470C0C06DEE42FD1618BB99005ADCA
2EC9D1E19' WITH GRANT OPTION |
+-----+
1 row in set (0.001 sec)
```

PERMISOS GLOBALES (777) EN WP-CONFIG.PHP

- Archivo crítico de WordPress con permisos de escritura/lectura para todos los usuarios del sistema, permitiendo su modificación por procesos maliciosos.

```
debian@debian:/var/www/html$ ls -l wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 2024 wp-config.php
```

L I S T A D O D E D I R E C T O R I O S W E B A C T I V A D O

- Configuración del servidor web que muestra el contenido de carpetas cuando no hay archivo índice, exponiendo estructura de directorios y archivos sensibles.

```
debian@debian:/$ curl -I http://localhost/wp-content/  
HTTP/1.1 200 OK  
Date: Tue, 15 Jul 2025 18:19:51 GMT  
Server: Apache/2.4.62 (Debian)  
Content-Type: text/html; charset=UTF-8
```

RESUMEN

SE ENCONTRARON LOS SIGUIENTES PROBLEMAS

Configuraciones Peligrosas

Incluyen permisos excesivos, servicios innecesarios habilitados y falta de cifrado. Son vulnerabilidades "de baja dificultad" frecuentemente explotadas por scripts automatizados.

Falta de Monitoreo

La ausencia de registros detallados y alertas tempranas permite que ataques pasen desapercibidos durante meses (promedio: 287 días según IBM).

Debilidades en Autenticación

Mecanismos de verificación de identidad insuficientes, principal vector en el 80% de brechas relacionadas con hacking (Verizon DBIR 2023).

Exposición de Datos

Configuraciones que revelan información sensible directa o indirectamente, violando principios de "need-to-know".

Vulnerabilidad	Tipo de Impacto	Nivel de Riesgo	Pérdida Potencial (USD)	Impacto Operacional
Acceso root remoto en MySQL	Robo de datos/Pérdida de integridad	Crítico	\$250,000 - \$5M+	Paralización de sistemas críticos, multas regulatorias
FTP anónimo habilitado	Exfiltración de información	Alto	\$150,000 - \$1M	Pérdida de propiedad intelectual, daño reputacional
Autenticación SSH por contraseña	Acceso no autorizado/Ransomware	Alto	\$100,000 - \$3M	Cifrado de sistemas, tiempo de inactividad prolongado
wp-config.php con permisos 777	Defacement/Inyección de malware	Medio	\$50,000 - \$500K	Blacklisting por Google, pérdida de clientes
Listado de directorios web	Exposición de información sensible	Medio	\$20,000 - \$300K	Robo de credenciales, escalada de privilegios
Servicios obsoletos con puertos abiertos	Explotación de vulnerabilidades conocidas	Crítico	\$180,000 - \$2.5M	Compromiso de red interna, pivoting a sistemas críticos

MEDIDAS DE CONTENCION

- Se cambiaron las contraseñas débiles
- Se activo el firewall
- Se cambio la configuracion de los servicios ftp y ssh
- Implementar softwares de monitoreo (wazuh)
- Realizar un analisis forense de l sistema operativo con Autopsy

SISTEMA DE GESTION DE SEGURIDAD

**Marco de
Implementación**

**Controles Clave
Explicados**

**Modelo de
Gobernanza**



GRACIAS
