INFORME TÉCNICO DE SEGURIDAD INFORMÁTICA

Autor: *Tina Calleja*

Fecha: *27-02-2025*

Tabla de contenido

1. OBJETO.

Este informe detalla un análisis de seguridad informática mediante el uso de diversas herramientas.

- Nmap: Herramienta de escaneo de redes y detección de puertos abiertos.
- Zenmap: Es la versión gráfica de Nmap.
- Xampp: Para levantar los servicios de Mysql y phpMyAdmin.
- Advanced IP Scanner: Analiza vulnerabilidades en aplicaciones.
- Anydesk: Permite acceso remoto a sistemas.
- Zero Tier: Permite la creación de una red local (LAN).
- Wireshark (análisis de tráfico TCP).
- Docker (Creación de contenedores).
- Pandora FMS (monitoreo de sistemas y redes).
- Nessus (escaneo de vulnerabilidades).

2. ALCANCE.

- Se crea una red local (LAN) con Zero tier.
- Se levanta el servicio de bases de datos con Xampp.
- Se realiza un escaneo de red y de puertos abiertos en la IP 192.168.1.114, verificando el estado del puerto 3306. En caso de estar abierto, se procede con un ataque de fuerza bruta utilizando nmap/zenmap para intentar obtener credenciales de MySQL.
- Se realiza una monitorización de paquetes TCP. Para conseguir datos de un login.
- Se comprueba el puerto FTP de la IP 192.168.5.102.
- Se usa Docker para levantar Pandora FMS y Nessus.

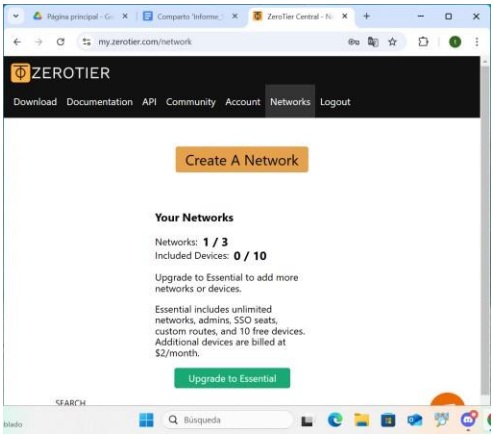
3. SITUACIÓN INICIAL.

La IP objetivo es 192.168.1.114. Se desconoce el estado de sus puertos y la posible exposición de MySQL en el puerto 3306, también se desconoce la vulnerabilidad del login de la landing page y el puerto FTP de la IP 192.168.5.102.

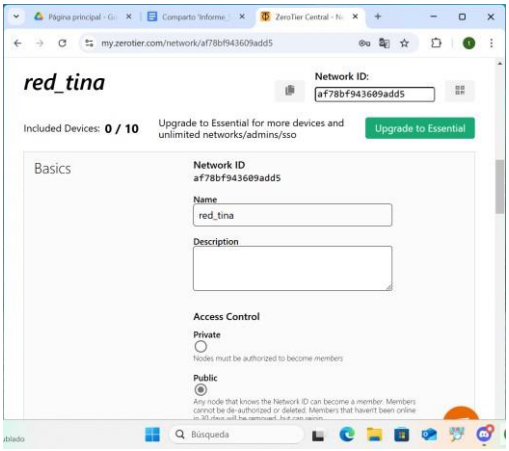
1. Se crea una red local con Zero Tier.
2. Se levantan los servicios con Xampp.
3. Se crea una landing page con un login.
4. Se realiza un escaneo de red inicial con Nmap/Zenmap para identificar los dispositivos activos.
5. Se escanea los puertos activos de la IP 192.168.1.114.
6. Se verifica el estado del puerto 3306 (MySQL).
7. En caso de estar abierto se utiliza Nmap/Zenmap MySQL brute para intentar obtener las credenciales.
8. Se listan las bases de datos y tablas disponibles con Nmap/Zenmap.
9. Se monitorea el tráfico de TCP del login con Wireshark.
10. Se comprueba el puerto FPT en la IP 192.168.5.102.
11. Se instala Docker para instalar diversas aplicaciones en varios contenedores.
12. Con Pandora FMS se supervisa la disponibilidad y el rendimiento de infraestructuras IT (tecnologías de la información).
13. Con Nessus se realiza una monitorización de la red.

4. PROCESO.

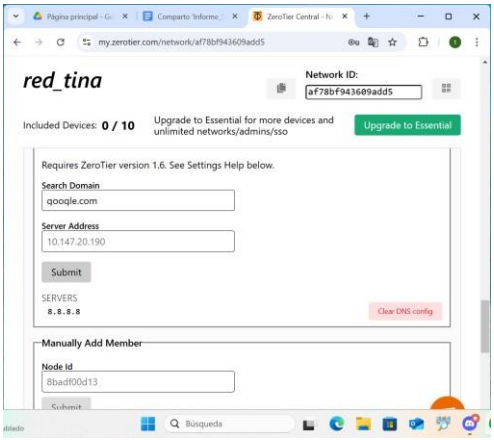
Creación de red local (LAN) con Zero Tier.



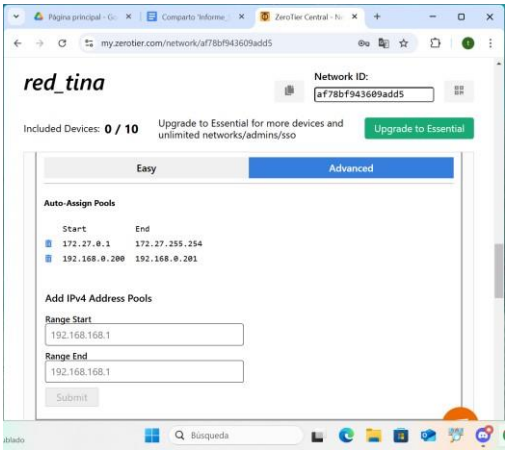
Creación de una red.



Selección del nombre de la red.



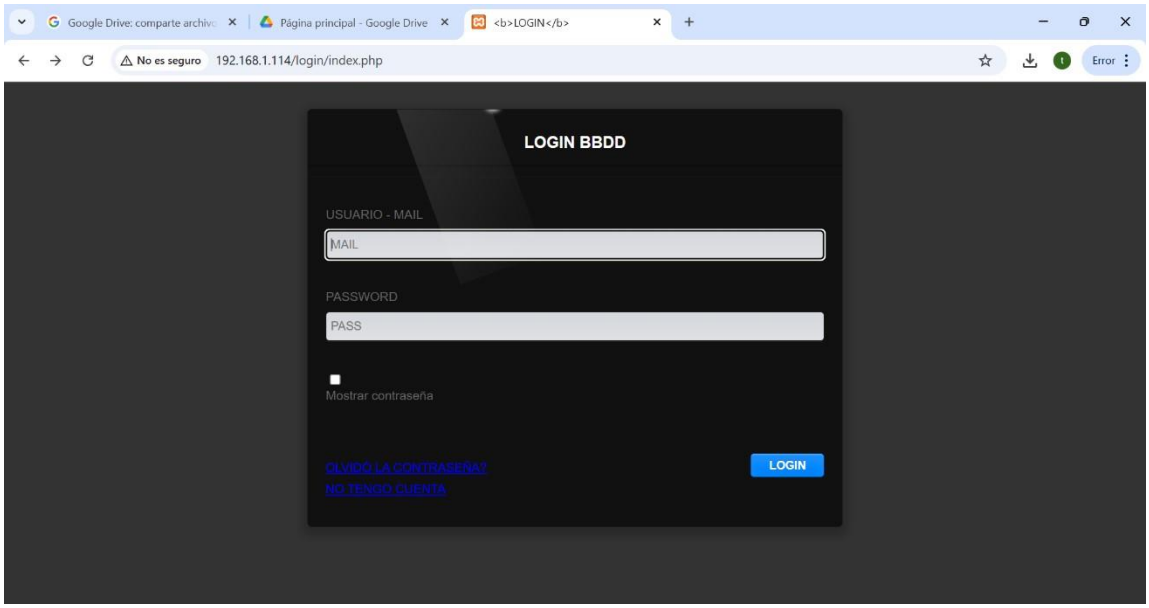
Configuración de DNS.



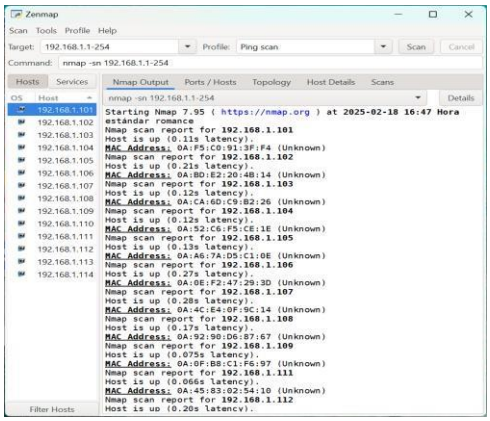
Creación de los rangos de direcciones IPs.

Levantamiento de servicios.

Login.

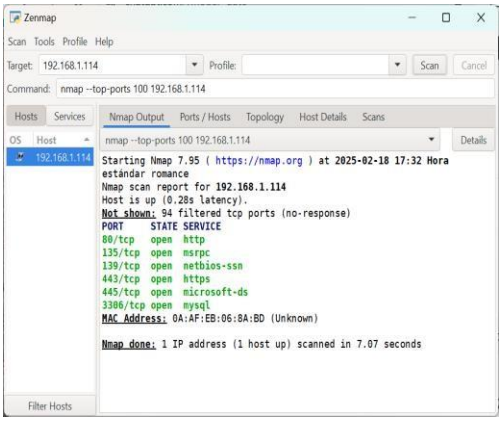


Escaneo de red inicial.



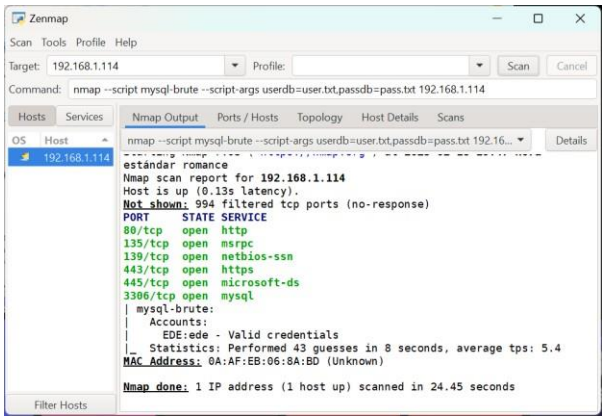
Con Zenmap y el comando: *nmap -sn 192.168.1.1-254* se comprueban los equipos conectados en la red.

Escaneo y verificación de puertos abiertos.



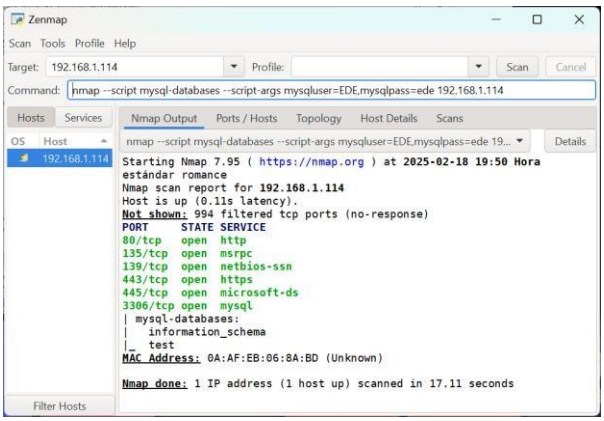
Con Zenmap y el comando: *nmap --top-ports 100 192.168.1.114* se escanea los 100 puertos más comunes de la IP 192.168.1.114.

Obtención de credenciales.



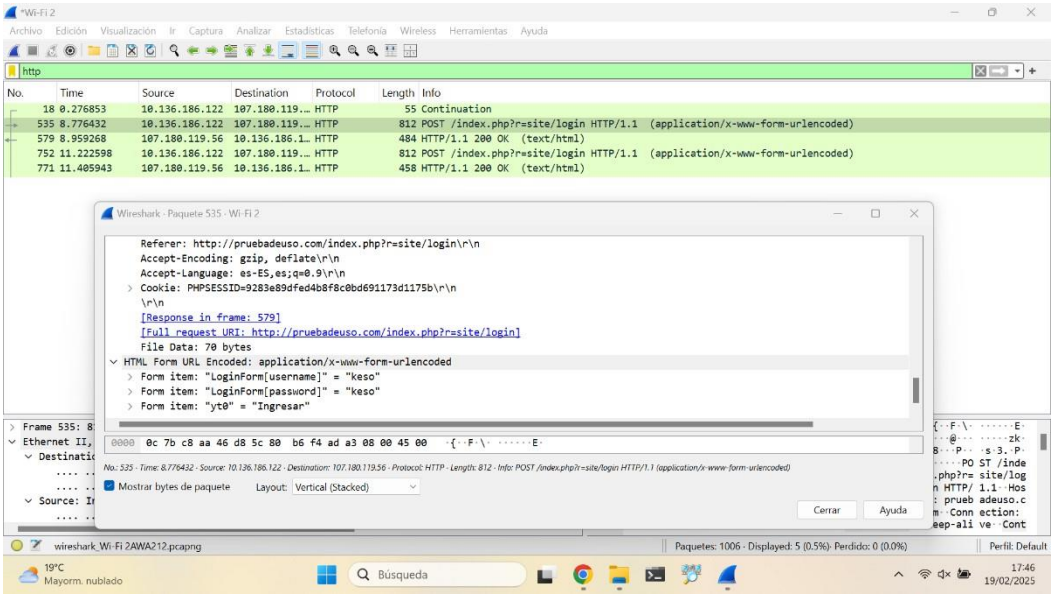
Con Zenmap y el comando: *nmap -T4 -A -v --script mysql-brute --script-args userdb=user.txt,passdb=pass.txt 192.168.1.114* donde los .txt son archivos de texto creados con datos probables de usuarios y contraseñas, se consigue las credenciales si coinciden, o no, si no coinciden.

Listar las bases de datos.



Con Zenmap y el comando: *nmap --script mysql-databases --script-args mysqluser=EDE,mysqlpass=ede 192.168.1.114* donde EDE y ede son las credenciales obtenidas en el paso anterior, se consigue ver las bases de datos.

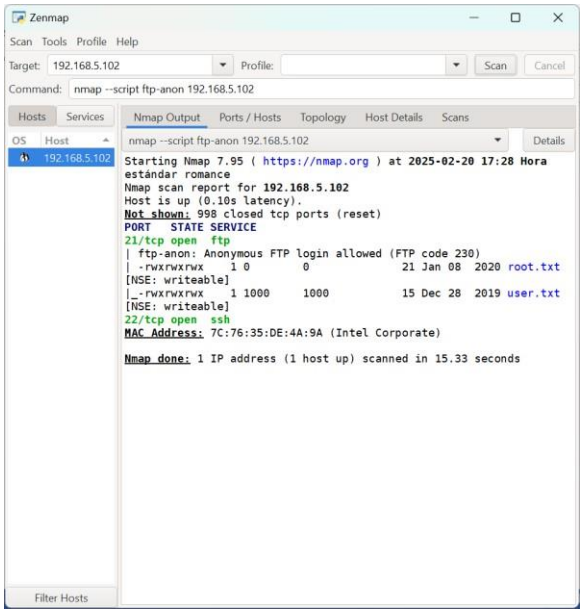
Monitoreo el tráfico de TCP.



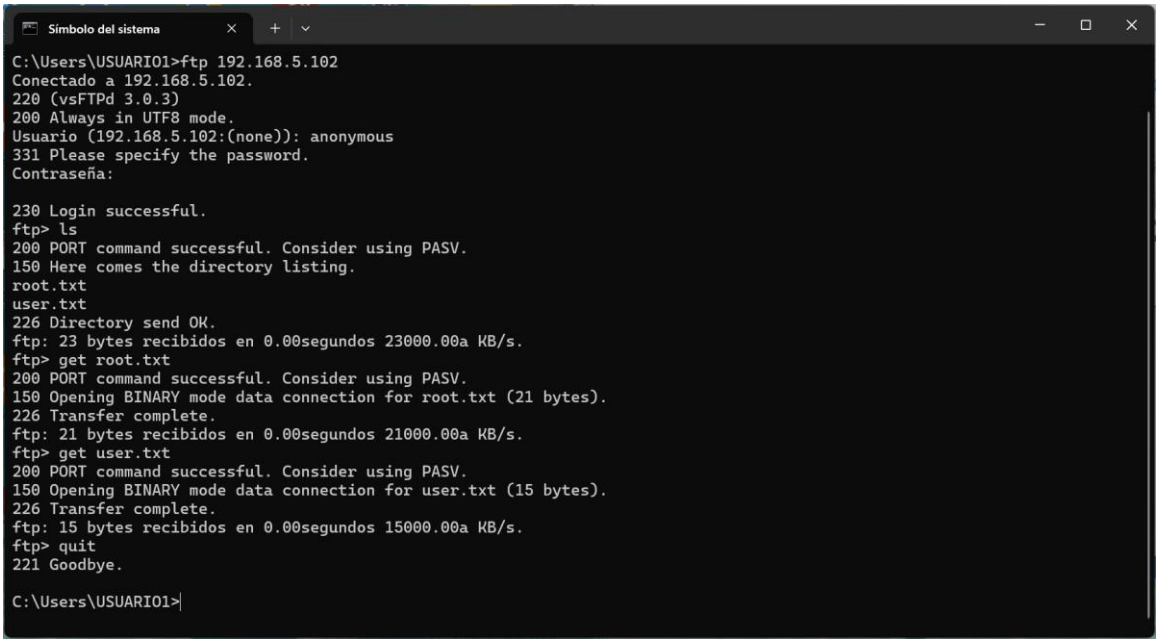
Con Wireshark se monitoriza el tráfico de la IP y filtramos por HTTP.

Se consigue el usuario = keso y la contraseña = keso del login de la landing page.

Comprobación del puerto FTP.

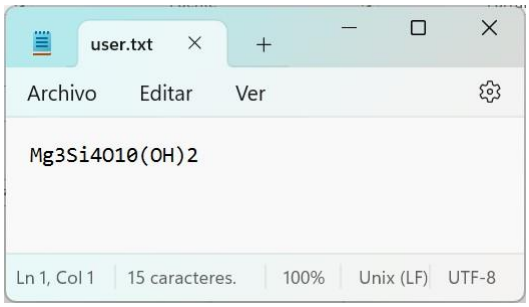


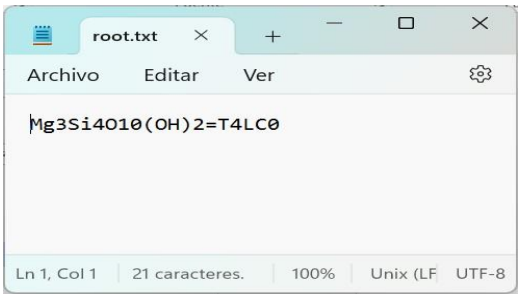
Con Zenmap y el comando: *nmap –script ftp anon 192.168.5.102* se obtienen los nombres de los archivos: root.txt, user.txt, las credenciales: Anonymous y "vacío" y también los permisos de lectura(r), escritura(w), y ejecución(x).



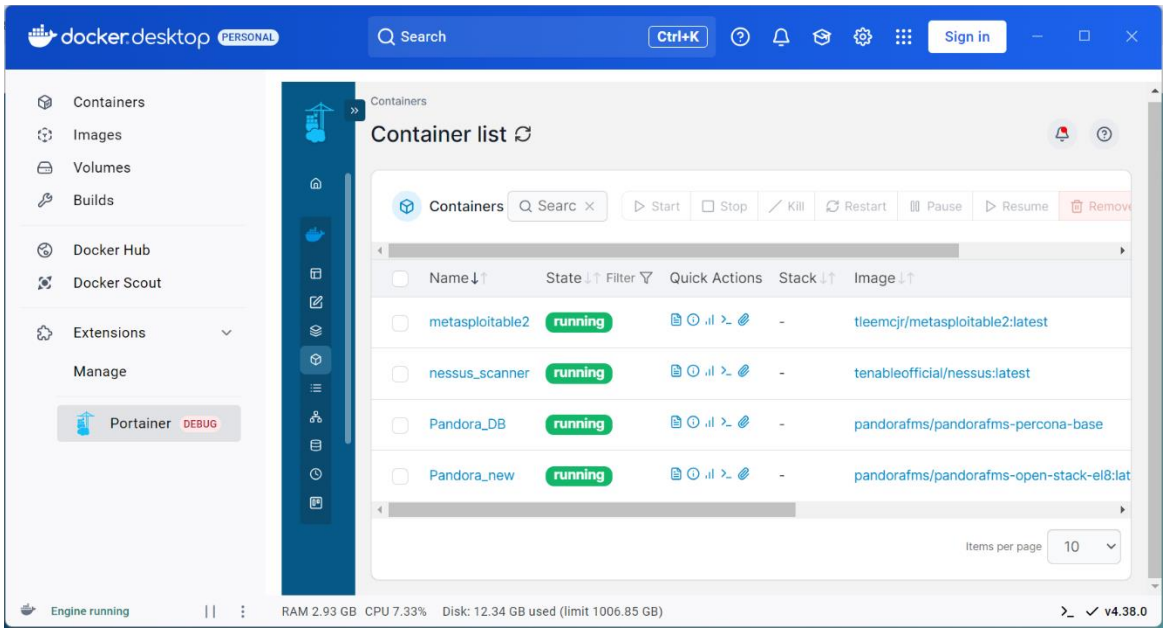
Con la consola de windows(CMD):

1. Se entra en el Puerto FTP con el commando *ftp 192.168.5.102*
2. Se comprueba el acceso con credenciales por defecto (user = anonymous, contraseña = “empty” y se consige acceder.
3. Con el commando *ls* se lista todos los archivos.
4. Con el commando *get* se descargan los archivos.



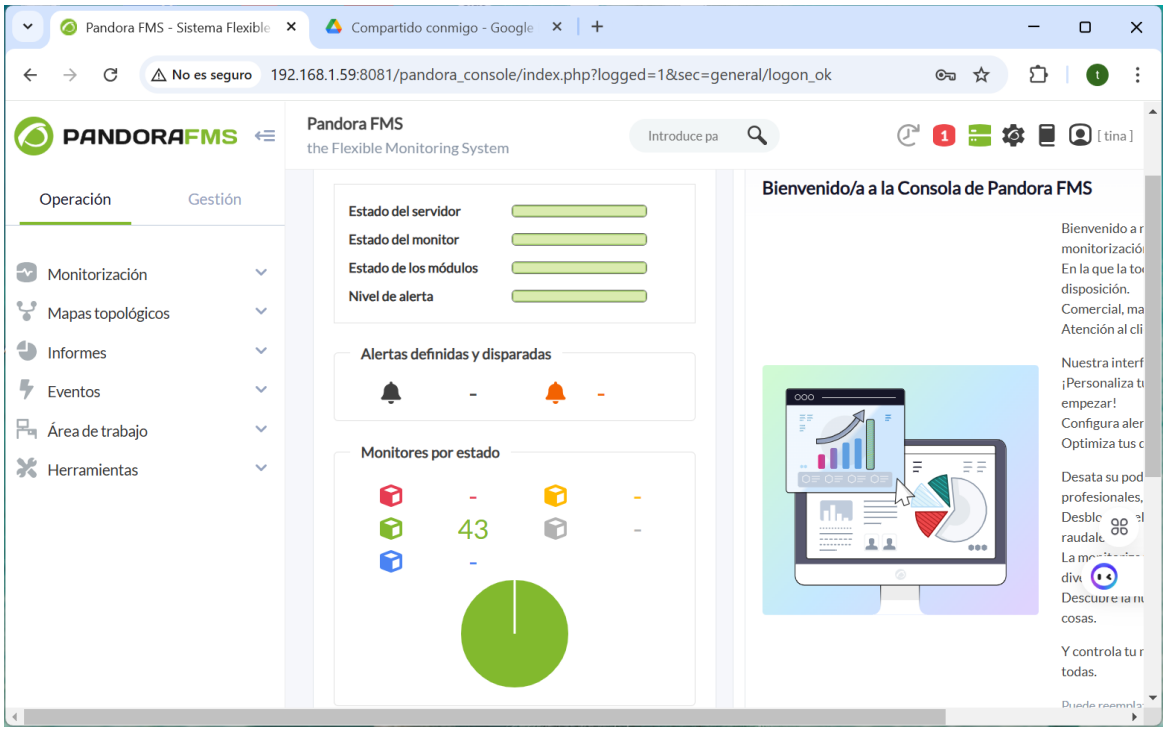


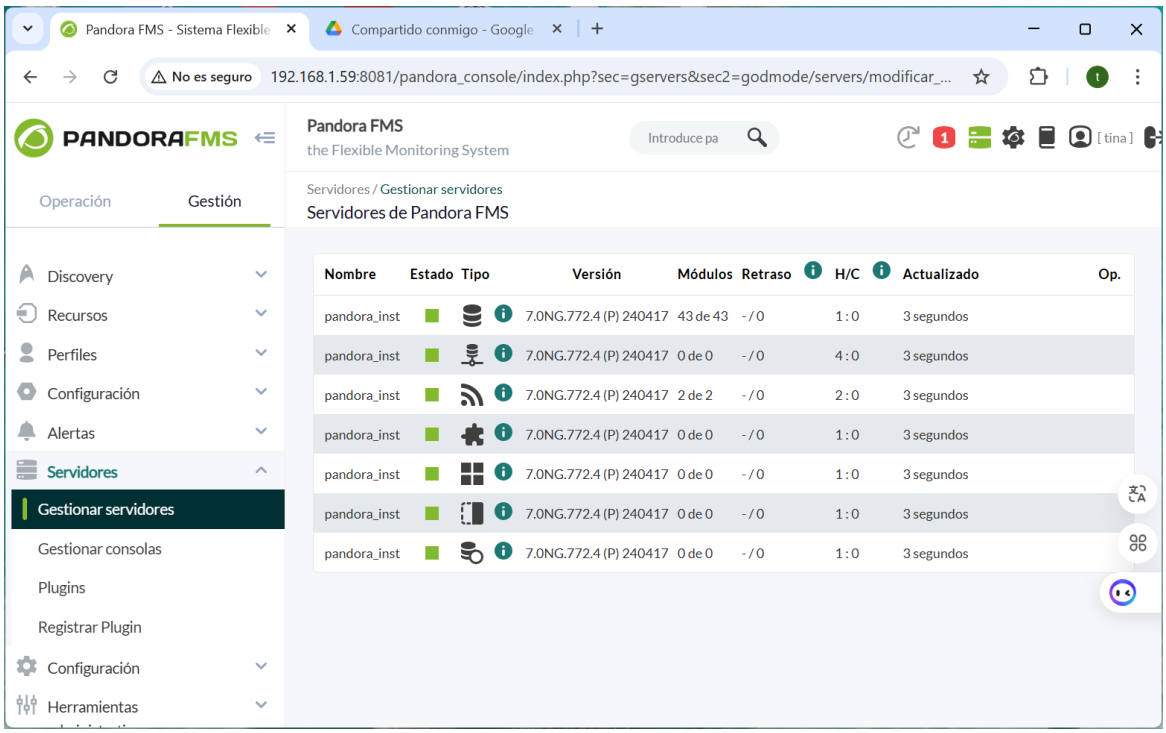
Instalación de Docker.



Con los comandos: *docker run --name Pandora_DB -p 3308:3308 -e MYSQL_ROOT_PASSWORD=pandora -e MYSQL_DATABASE=pandora -e MYSQL_USER=pandora -e MYSQL_PASSWORD=pandora-d pandorafms/pandorafms-percona-base* y docker run --name Pandora_new --rm -p 8081:80 -p 41125:41121 -e DBHOST=172.17.0.2 -e DBNAME=pandora -e DBUSER=pandora -e DBPASS=pandora -e DBPORT=3308 -eINSTANCE_NAME=pandora_inst -ti pandorafms/pandorafms-open-stack-el8:latest se instala Percona y Pandora FMS para el monitoreo de servidores y dispositivos. Con el comando: docker run -d --name nessus_scanner -p 8834:8834 -e NESSUS_USERNAME=ede -e NESSUS_PASSWORD=ede tenableofficial/nessus:latest se instala Nessus, con el que también escaneamos los dispositivos conectados a la red.

Pandora FMS.

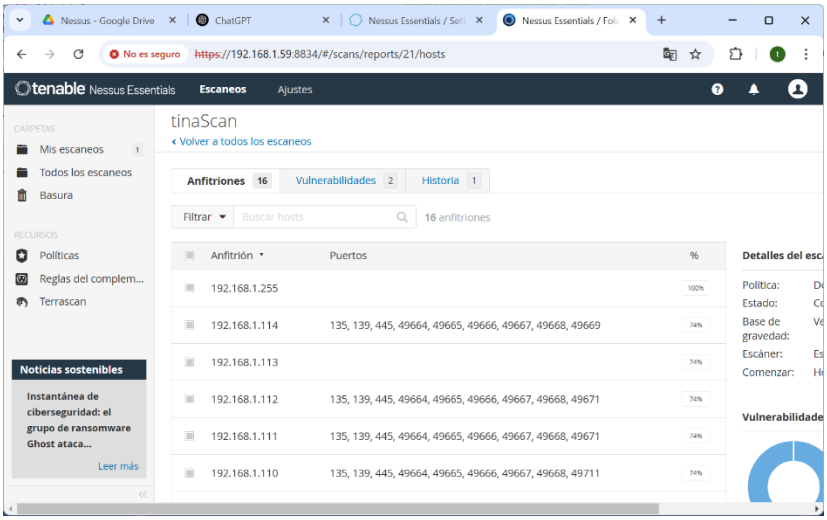

Pandora FMS - Sistema Flexible
Compartido conmigo - Google
No es seguro
192.168.1.59:8081/pandora_console/index.php?logged=1&sec=general/logon_ok
PANDORAFMS
Pandora FMS
the Flexible Monitoring System
Introduce pa
[tina]
Operación
Gestión
Monitorización
Mapas topológicos
Informes
Eventos
Área de trabajo
Herramientas
Estado del servidor
Estado del monitor
Estado de los módulos
Nivel de alerta
Alertas definidas y disparadas
Monitores por estado
43
Bienvenido/a a la Consola de Pandora FMS

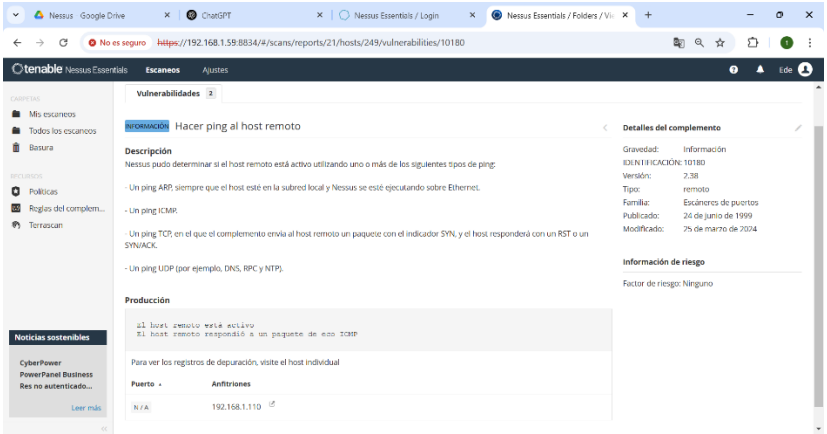

Pandora FMS - Sistema Flexible
Compartido conmigo - Google
No es seguro
192.168.1.59:8081/pandora_console/index.php?sec=gservers&sec2=godmode/servers/modificar_...
PANDORAFMS
Pandora FMS
the Flexible Monitoring System
Introduce pa
[tina]
Operación
Gestión
Servidores / Gestionar servidores
Servidores de Pandora FMS
Discovery
Recursos
Perfiles
Configuración
Alertas
Servidores
Gestionar servidores
Gestionar consolas
Plugins
Registrar Plugin
Configuración
Herramientas
Nombre Estado Tipo Versión Módulos Retraso H/C Actualizado Op.
pandora_inst 7.0NG.772.4 (P) 240417 43 de 43 -/0 1:0 3 segundos
pandora_inst 7.0NG.772.4 (P) 240417 0 de 0 -/0 4:0 3 segundos
pandora_inst 7.0NG.772.4 (P) 240417 2 de 2 -/0 2:0 3 segundos
pandora_inst 7.0NG.772.4 (P) 240417 0 de 0 -/0 1:0 3 segundos
pandora_inst 7.0NG.772.4 (P) 240417 0 de 0 -/0 1:0 3 segundos
pandora_inst 7.0NG.772.4 (P) 240417 0 de 0 -/0 1:0 3 segundos
pandora_inst 7.0NG.772.4 (P) 240417 0 de 0 -/0 1:0 3 segundos

	A	B
1		
2	Agentes totales	4
3	MÃ³dulos totales	45
4	Grupos totales	8
5	Total de registros de datos de mÃ³dulos	227
6	Registro total de acceso de agentes	88
7	Total de eventos	52
8	Traps totales	
9	Usuarios totales	11
10	Sesiones totales	88
11		
12		
13		

Archivo CSV descargado desde Pandora FMS.

Nessus.





5. SITUACIÓN FINAL.

- Tras el análisis, se determinaron los servicios expuestos.
- Se evaluó la seguridad del puerto 3306.
- Se obtuvieron las credenciales de acceso a la base de datos con nmap MySQL brute.
- Se consiguió listar las bases de datos del servicio con nmap MySQLdatabases.
- Con Wireshark se consiguió localizar el usuario y la contraseña del login.
- Con Zenmap y a través de comandos de consola se accede al Puerto FTP y se consigue descargar dos archivos de texto.
- Con Docker se levanta Pandora FMS y Nessus con los que se realiza un monitoreo de servidores físicos, virtuales, y otros dispositivos de red comprobando su estado.

6. CONCLUSIÓN.

El informe demuestra que la seguridad tanto del servicio MySQL como del login, en el equipo con IP 192.168.1.114, presenta deficiencias, especialmente en la gestión de credenciales. El equipo con IP 192.168.5.102 también presenta deficiencias en la gestión de credenciales.

Se recomienda incrementar medidas de seguridad como:

- Restricciones de acceso.
- Uso de contraseñas robustas.
- Monitoreo de intentos de conexión no autorizados para reducir riesgos de intrusión.