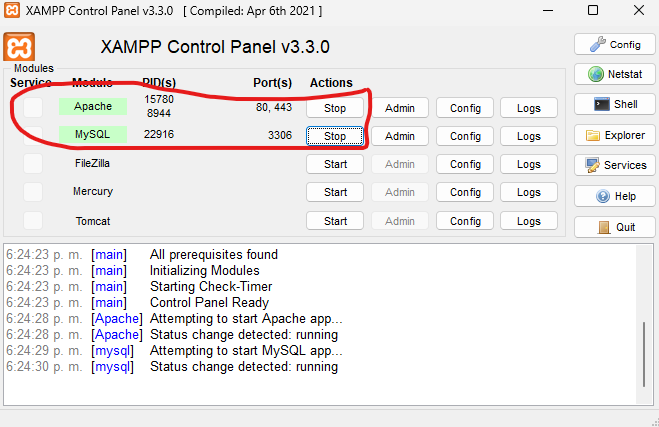
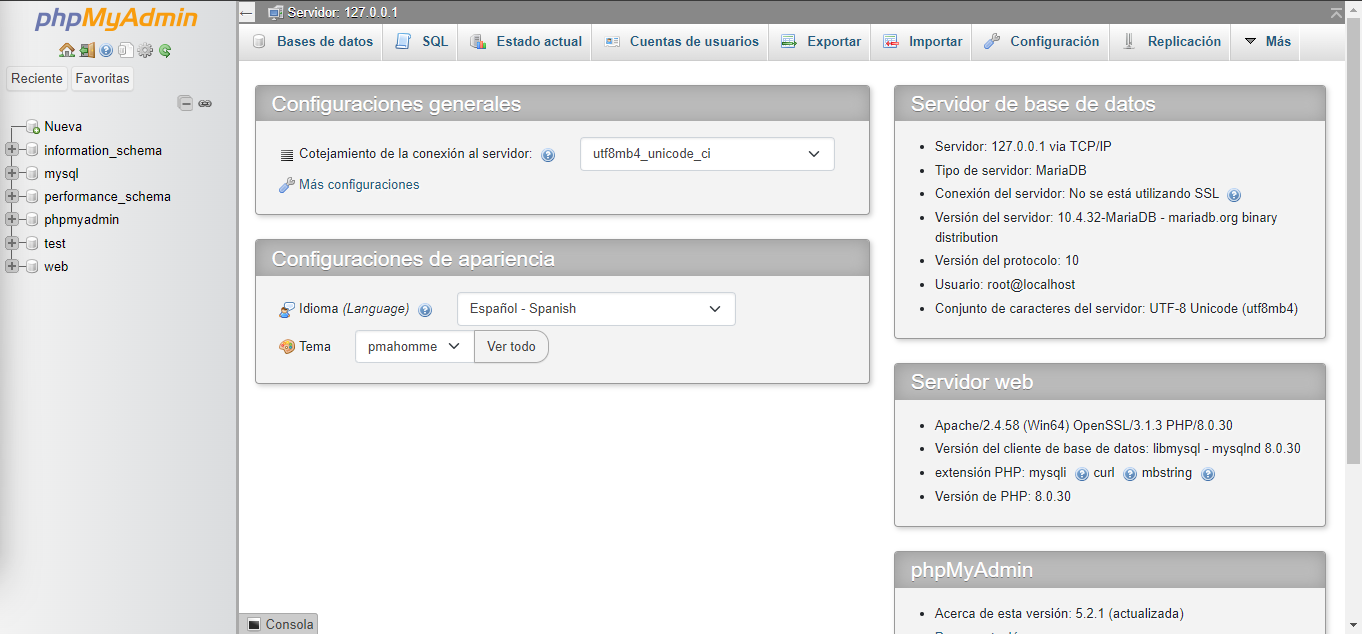
**file:///C:/xampp/htdocs/belleza/bellezaencasa/2024-02-13-ZAP-Report-.html**

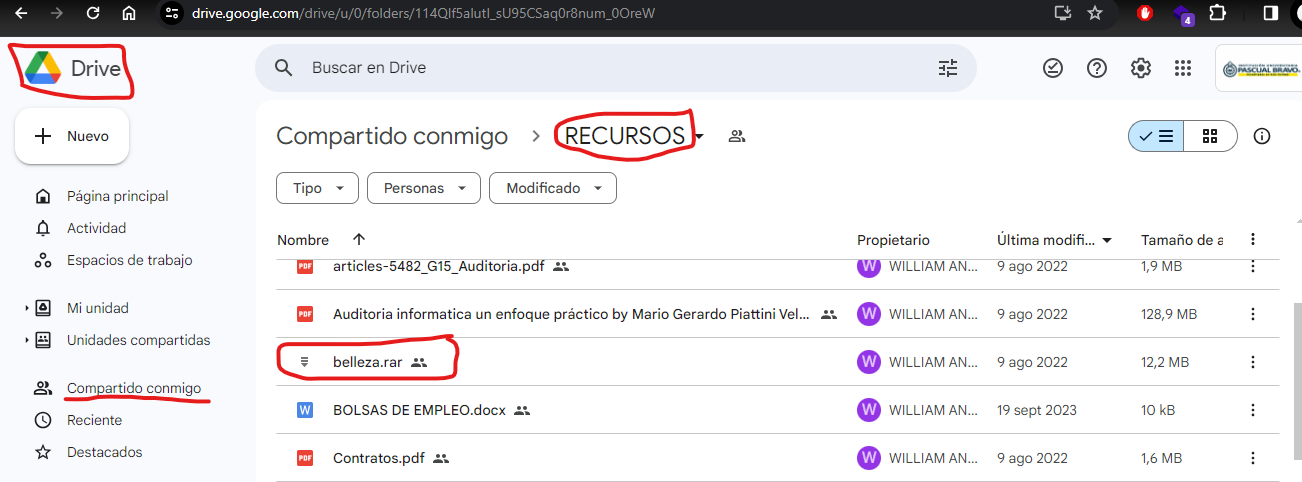
**AUDITORÍA O TALLER PRACTICO A UNA APP WEB Y RED DE SUS CASAS.**

1. **AUDITORÍA A UNA APLICACIÓN WEB LLAMADA BELLEZA EN CASA CON BASES DE DATOS EN phpMyAdmin-MYSQL: herramientas a utilizar.  
   \* XAMPP - MYSQL - APP WEB, OWASP ZAP. (http://127.0.0.1/belleza/bellezaencasa/)**

XAMPP… ****

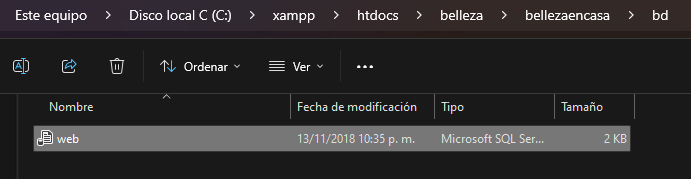
phpMyAdmin-MYSQL…

****

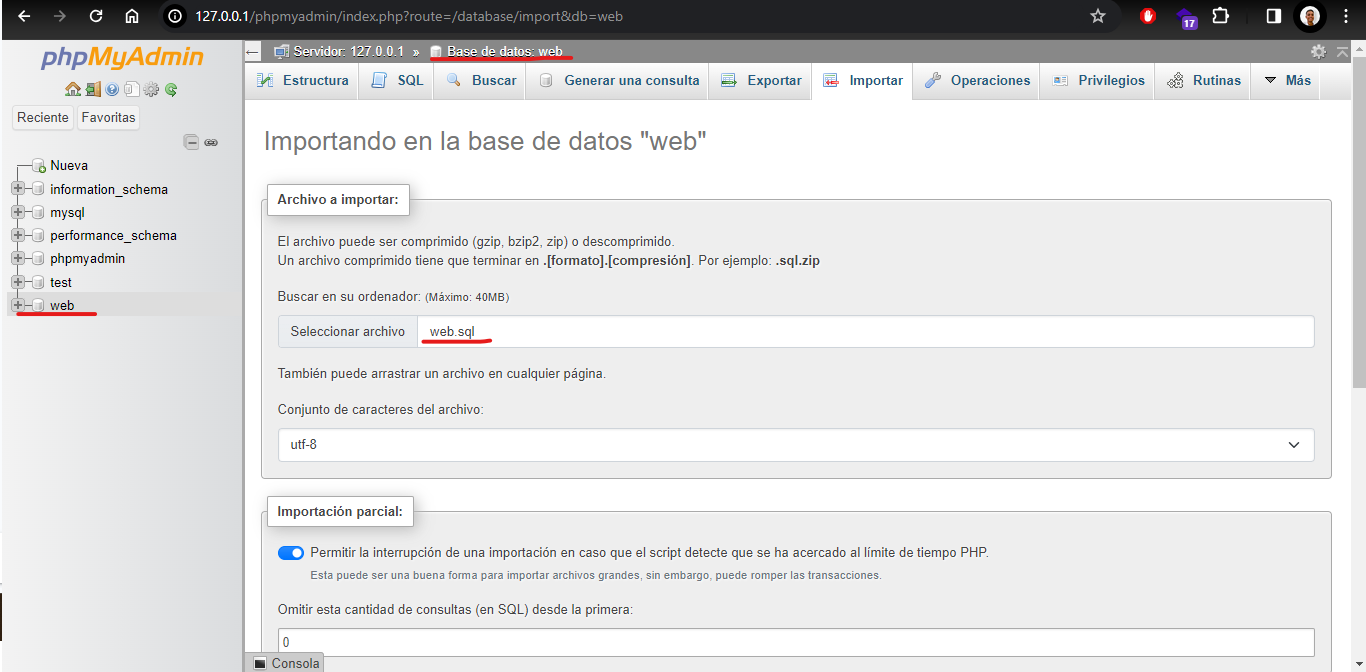
DESCARGAR LA APP WEB EN DRIVE, AUDITORIA DE SISTEMAS/RECURSOS/belleza.rar****

EJECUTAR LA APP WEB, (<http://127.0.0.1/belleza/bellezaencasa/>)****

1. **EVALUAR APP Y MONTAR BASE DE DATOS, RUTA.**

****

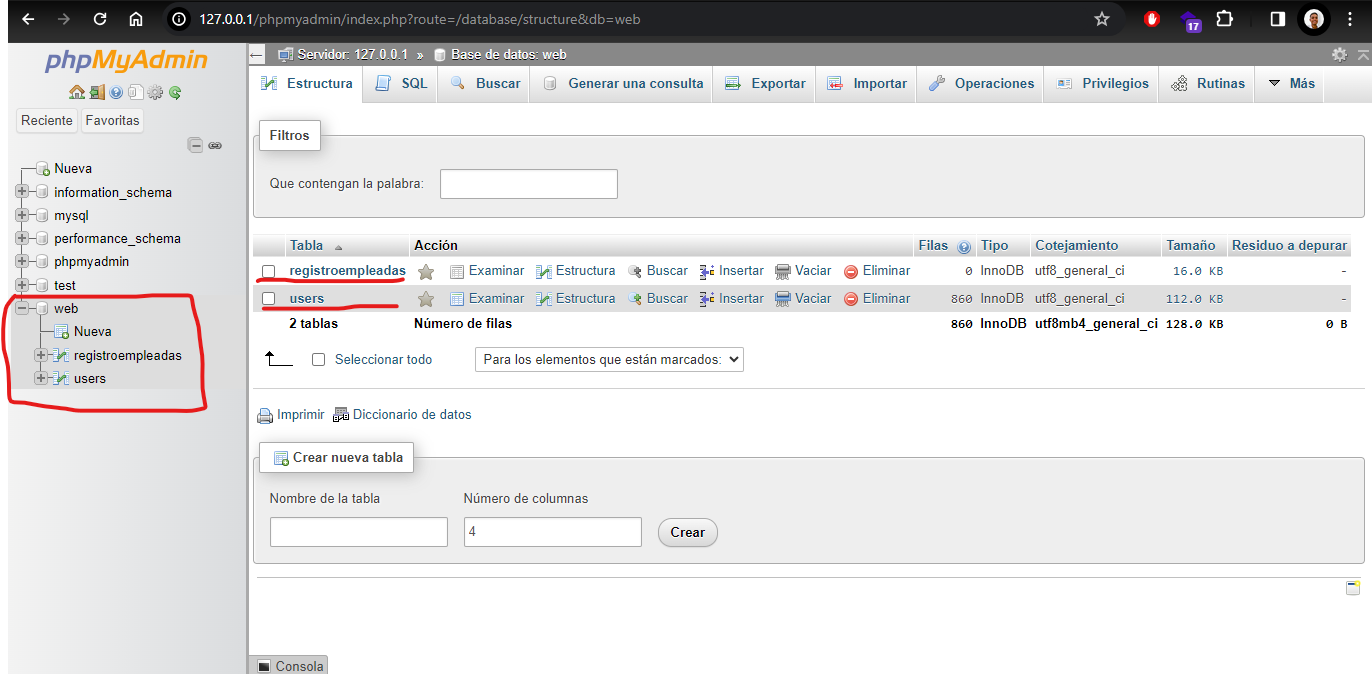
**SUBIR BASE DE DATOS A phpMyAdmin-MYSQL.**

****

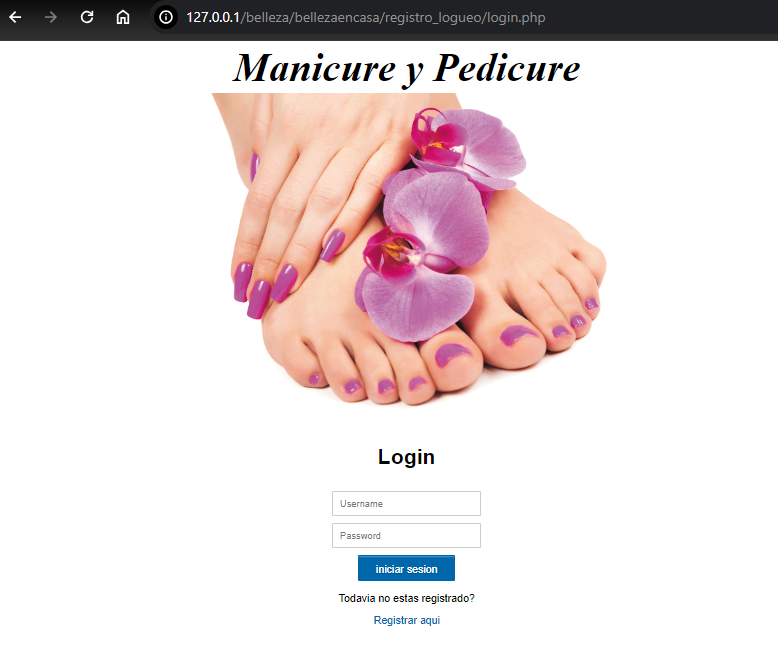
**finalizar con importar.**

****

**CREAR LAS PRIMERAS TABLAS.**

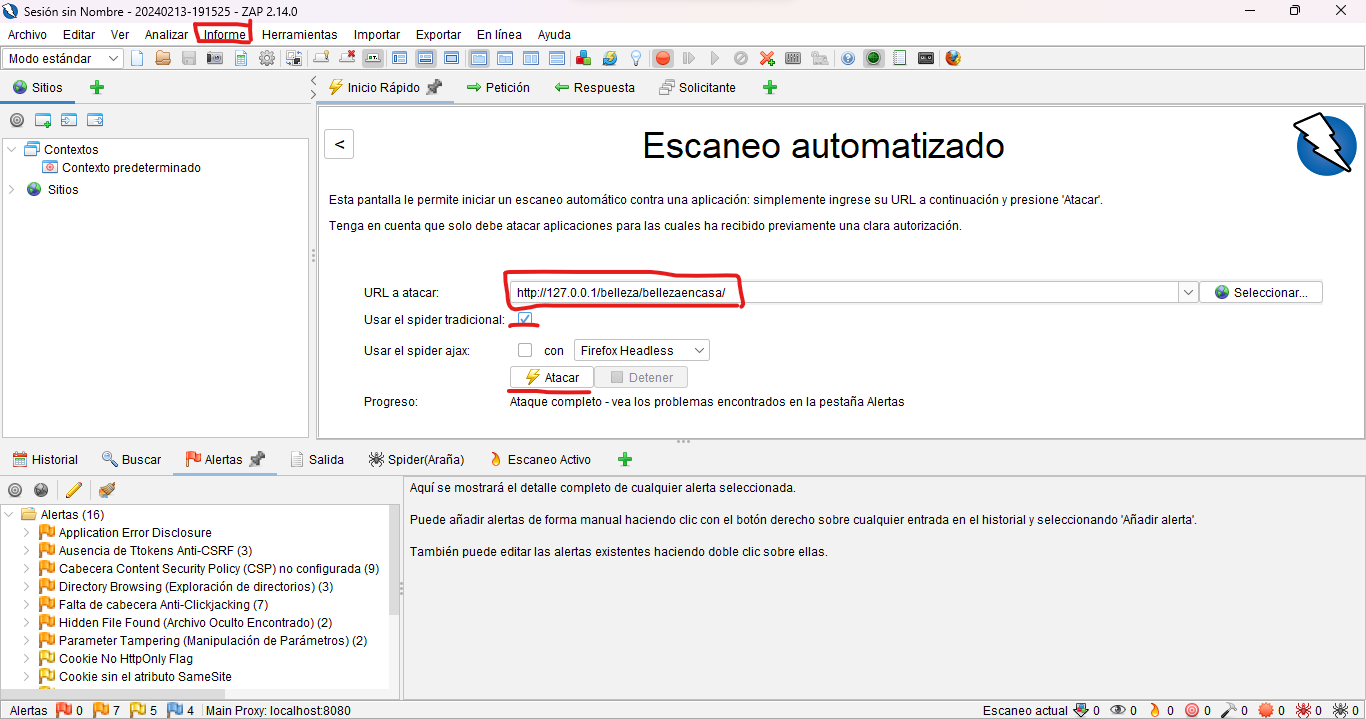
****

1. **REGISTRARSE O INGRESAR.**

****

**LA APP ESTA CORRIENDO DE FORMA ADECUADA…**

1. **TESTING: herramientas a utilizar OWASP ZAP, se genera informe.**

****

1. **VULNERABILIDADES:**

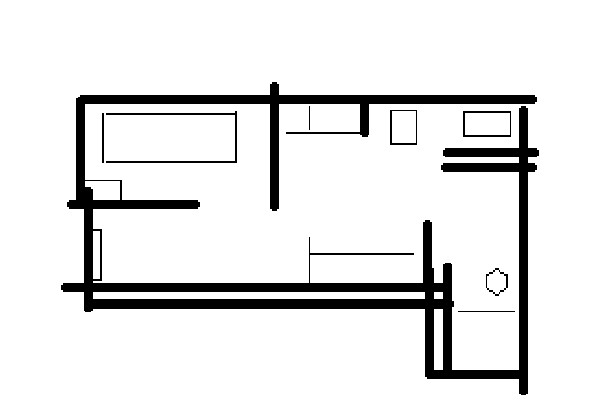
* Application Error Disclosure:  
  ¿Qué es?: Serefiere a la revelación de información detallada sobre errores internos de la aplicación a los usuarios finales o atacantes.

¿Cómo se ataca? Mitigando la vulnerabilidad de “Application Error Disclosure” y evitar que se muestren detalles sensibles de errores a los usuarios finales o atacantes. ¿como?

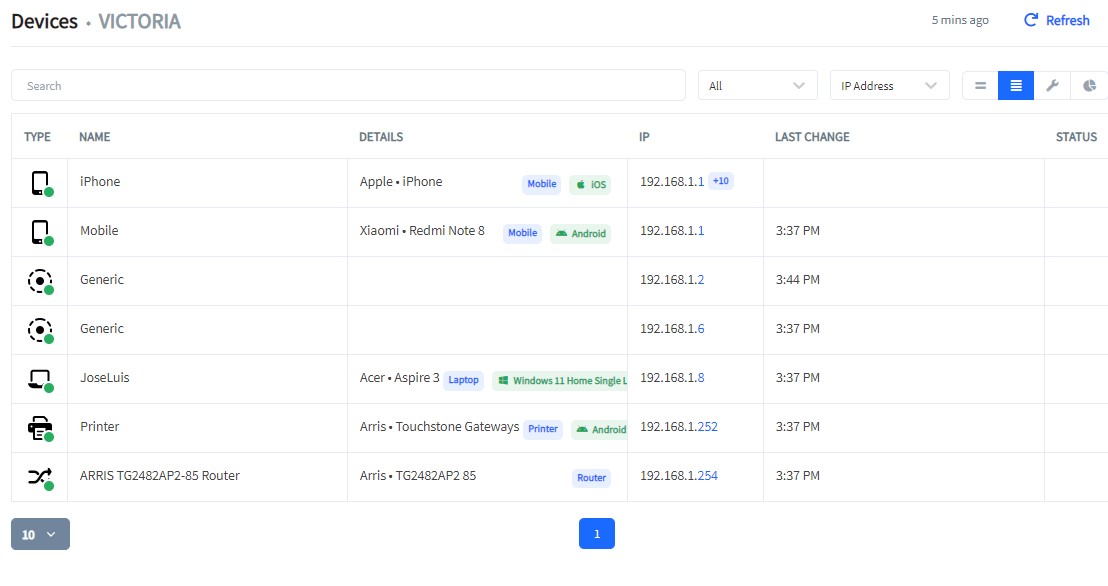
* Personalizando las páginas de Error.
* muestra mensajes genéricos y amigables para los usuarios en lugar de detalles técnicos.
* utilizando páginas de error personalizadas para distintos códigos de estado HTTP.
* Registros seguros de errores: configurando el sistema de registro de errores para almacenar información detallada en registros internos sin mostrarla a los usuarios finales.
* Manejo de excepciones: implementando un manejo adecuado de excepciones en tu código para capturar y manejar errores de manera controlada.
* Desactivar mostrar errores en producción: desactivando la opción de mostrar errores en la salida del navegador.
* ejemplo en php.   
  ini\_set('display\_errors', 'Off');
* Realizando escaneos automatizados.
* revisando el código.

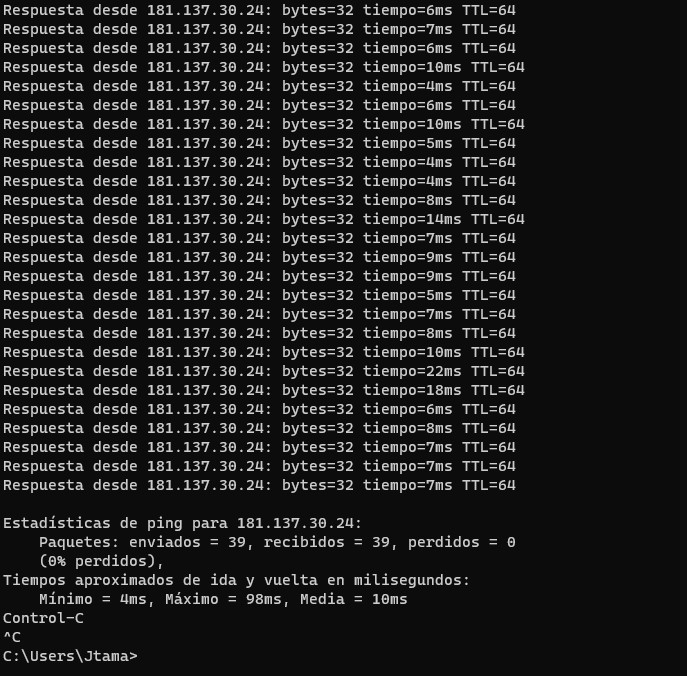
¿Cómo me defiendo?:

* Validando los datos de entrada: se implementa una validación robusta de los datos de entrada para prevenir errores relacionados con datos incorrectos.
* Pruebas de penetración: realizando de forma regular auditorías de seguridad para identificar posibles problemas de error disclosure.
* Actualizaciones y parches.
* Seguridad en las capas: Utiliza enfoques de seguridad en capas para proteger tu aplicación desde diferentes frentes, incluida la red, la capa de aplicación y la base de datos.
* Configuración de servidores: Configura adecuadamente los servidores web y aplicativos para limitar la exposición de información sensible en los mensajes de error

1. PING EN CMD DESDE MI CASA…[](https://drive.google.com/drive/folders/1wr7MEm16MtrBPV4TjqX1Ixs61twLnyPF?usp=drive_link)

PING DESDE LA CUADRA.





1. COMANDOS DE RED DE DOS, CON 10 EJEMPLOS:

* ipconfig: Muestra la configuración de red, incluyendo la dirección IP, la máscara de subred y la puerta de enlace   
  Ej: ipconfig / all
* ping: envía un paquete de datos a una dirección IP o nombre de host y muestra la respuesta, util para verificar la conectividad de red.   
  Ej: ping [www.google.com](http://www.google.com)
* tracert: rastrea la ruta que toma un paquete para llegar a su destino, mostrando cada salto en la red.   
  Ej: tracert www.example.com
* netstat: muestra estadísticas de red y conexiones activas, tanto entrantes como salientes.  
  Ej: netstat -an
* nslookup: proporciona información sobre la resolución de nombres de dominio y las direcciones IP asociadas.   
  Ej: nslookup www.example.com
* arp: Muestra y modifica la tabla de resolución de direcciones de protocolo (ARP), que asocia direcciones IP con direcciones físicas (MAC).
* route: Muestra y modifica la tabla de enrutamiento del sistema, que determina como se dirigen los paquetes hacia su destino.   
  Ej: route print
* nbtstat: muestra estadísticas y conexiones NetBios sobre TCP/IP, útil en redes locales.  
  Ej: nbtstat -A 192.168.1.1
* Telnet: permite establecer una conexión con un servidor remoto utilizando el protocolo Telnet.   
  Ej: telnet [www.example.com](http://www.example.com) 80
* net: proporciona varias funciones relacionadas con la administración de recursos compartidos, usuarios y grupos en una red.   
  Ej: net view.

1. TEST DE VELOCIDAD…

