PROYECTO FINAL - INSTRUCCIONES DE USO EN MACBOOK PRO (macOS)

==========

1. INSTALAR HERRAMIENTAS BÁSICAS

Instalar Homebrew (si no lo tienes):

/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

Instalar Python 3, Nmap y Wireshark:

brew install python nmap wireshark

2. CREAR Y ACTIVAR UN ENTORNO VIRTUAL (opcional pero recomendado)

python3 -m venv auditoria-env

source auditoria-env/bin/activate

3. INSTALAR LIBRERÍAS DE PYTHON

pip install python-nmap pyshark scapy psutil

4. PERMISOS EN MACOS

Ejecuta con 'sudo' los scripts que capturan paquetes o envían tráfico:

sudo python3 scripts/captura_paquetes_pyshark.py

sudo python3 scripts/prueba_vulnerabilidad_scapy.py

Ve a Preferencias del Sistema > Seguridad y privacidad > Privacidad y da permisos a Terminal o tu IDE.

5. EJECUCIÓN DE LOS SCRIPTS

Escanear red y puertos con Nmap:

python3 scripts/auditoria_nmap.py

Captura de paquetes con Pyshark:

sudo python3 scripts/captura_paquetes_pyshark.py

Envío de paquetes SYN con Scapy:

sudo python3 scripts/prueba_vulnerabilidad_scapy.py

Monitorear tráfico de red:

python3 scripts/analisis_ancho_banda_psutil.py

Comunicación cliente-servidor:

Servidor

python3 scripts/server.py

Cliente

python3 scripts/client.py

RECOMENDACIONES FINALES

- Usa siempre una red de pruebas.
- Documenta los resultados.
- Ejecuta Wireshark una vez para aceptar permisos de red.
- Si tienes un chip M1/M2, ejecuta dependencias con 'arch -x86_64' si es necesario.