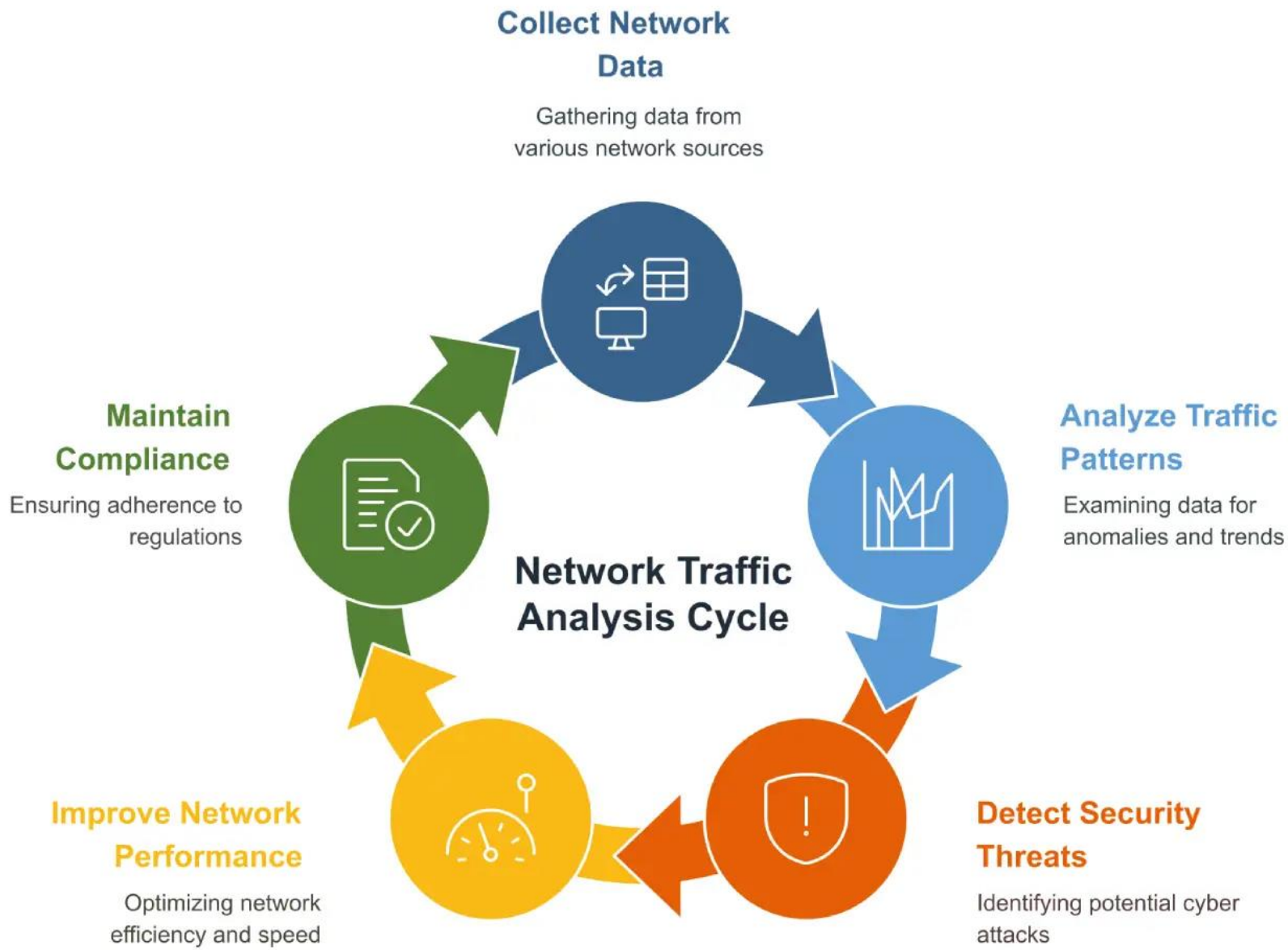
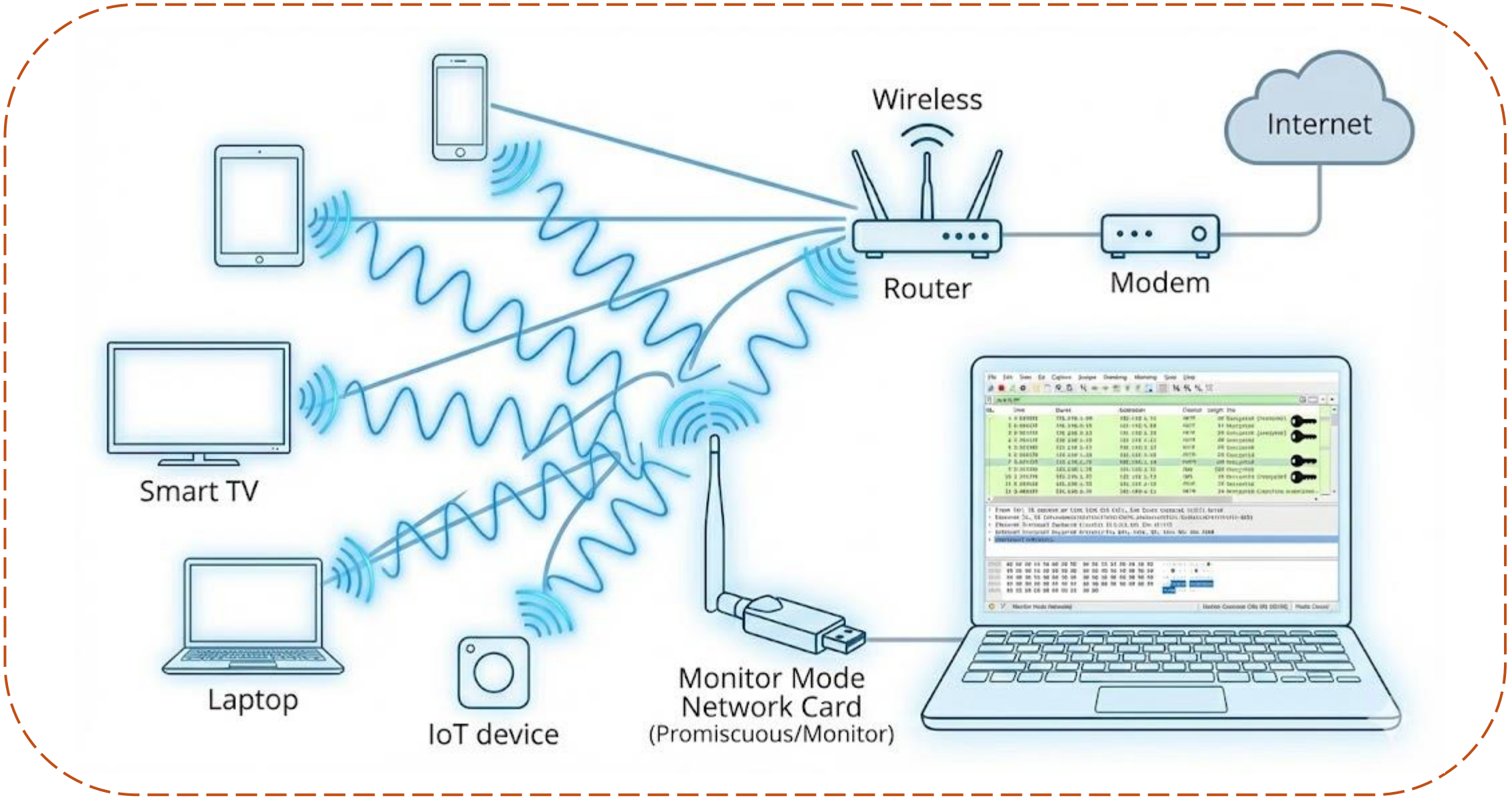
Análisis de tráfico para detección de vulnerabilidades

El Sniffing es la acción de interceptar, capturar y registrar el tráfico de datos que viaja a través de una red. El análisis de patrones dentro de este, nos permite identificar protocolos vulnerables: sin cifrado, mala configuración o versiones obsoletas.


Collect Network Data
Gathering data from various network sources
Analyze Traffic Patterns
Examining data for anomalies and trends
Detect Security Threats
Identifying potential cyber attacks
Improve Network Performance
Optimizing network efficiency and speed
Maintain Compliance
Ensuring adherence to regulations
Network Traffic Analysis Cycle

Laboratorio & Herramientas


Wireless
Internet
Router
Modem
Smart TV
Laptop
IoT device
Monitor Mode
Network Card
(Promiscuous/Monitor)

Proceso de Intercepción de tráfico

El Resultado (Man-in-the-Middle):

1. La víctima cree que la computadora del atacante es el Router.
2. La víctima envía sus datos (Facebook, banco, Google) al atacante.
3. El atacante recibe los datos, los **"Sniffea"** (los lee/guarda).
4. El atacante reenvía los datos al Router real para que la víctima no pierda conexión y no sospeche nada.

Comandos

```
sudo apt update
sudo apt install -y ettercap-common
ettercap-text-only arp-scan tcpdump nmap
tshark net-tools

# Opcional:
sudo apt install -y wireshark sslstrip
```