Home Network Security & Traffic Analysis

Author: Abeiku Quayson
Email: abeikuqsn@gmail.com

Introduction

This project focuses on strengthening the security of a small home network and analyzing traffic to better understand common protocols and potential threats. I configured my **home router** with secure settings, hardened my system with firewall rules, and used Wireshark to capture and analyze traffic. The goal was to practice real-world defensive measures and build a strong foundation in network security basics.

Objective

- To understand common network threats and their mitigations.
- To configure a home router with secure settings (WPA2, firewall, SSID management, etc.).
- To use Wireshark for live traffic monitoring and protocol analysis.
- To document findings and lessons learned.

Tools & Methods Used

- **Router Admin Interface** (for secure configuration)
- **Windows Defender Firewall** (host-based security)
- **Wireshark** (traffic monitoring & protocol analysis)
- **Documentation tools** (Notepad, browser research, screenshots)

Steps Taken

1. Research Phase

- Reviewed common threats: viruses, worms, trojans, phishing.
- Studied best practices: WPA2/WPA3 encryption, firewall rules, disabling WPS.

2. Network Setup & Hardening

- Accessed my home router's web interface.
- Changed the **default admin password**.
- Enabled **WPA2 encryption**.
- Disabled **WPS** (no PIN/PBC).
- Configured a **custom SSID** for the 5GHz Wi-Fi band.
- Adjusted firewall and guest network access settings.
- Configured **Windows Defender Firewall** to block unauthorized connections.

3. Traffic Monitoring with Wireshark

- Installed Wireshark and selected the correct network interface.
- Captured live traffic during browsing activities.
- Applied filters to focus on **DNS, HTTP, HTTPS, and ARP packets**.
- Learned to recognize normal vs. suspicious traffic patterns.

4. Documentation

- Captured screenshots of:
    - Router security settings (encryption, SSID, WPS disabled).
    - Windows Defender Firewall configuration.
    - Wireshark traffic analysis.

- Summarized findings and steps for reproducibility.

Challenges & Solutions

- **Choosing the setup**: Unsure whether to use a virtual or physical network → opted for my **home router** to keep it realistic.
- **Wireshark confusion**: At first, traffic seemed overwhelming → solved by applying protocol filters.
- **Correct interface**: Initially selected the wrong network interface → fixed by identifying traffic spikes in the right one.

Results & Outcomes

- Successfully **secured my home router** with strong encryption, disabled WPS, and improved firewall rules.
- Gained confidence in using **Wireshark** for packet analysis.
- Improved understanding of how everyday protocols like DNS, HTTP/HTTPS, and ARP behave in real-time.
- Strengthened my ability to secure and monitor small networks.

Conclusion

This project was an important step in applying cybersecurity knowledge in a practical setting. By configuring my **home router** and analyzing its traffic, I learned hands-on techniques for protecting small networks and detecting potential issues. These skills form a strong foundation for more advanced network and web application security work.