**Home VM Lab & Network Traffic Analysis**

**Overview**

Designed and implemented a virtualized network environment using VirtualBox to simulate real-world networking scenarios. Installed and configured Wireshark to capture and analyze network traffic for security and performance insights. This project involved setting up virtual machines, configuring a network adapter (Bridged modes), and applying packet filters to identify specific protocols such as HTTP, DNS, and TCP. Through this hands-on experience, I developed skills in network troubleshooting, system administration, and cybersecurity analysis, demonstrating the ability to monitor and secure network environments in virtualized settings.

**Lab Setup**

* Virtualization Tool: Oracle VirtualBox
* Tools Used: Wireshark, Windows
* Network Configuration: NAT & Bridged Adapter

**Objectives**

* Capture and analyze real network traffic from virtual machines
* Identify protocols like HTTP, TCP, UDP, and DNS
* Detect and flag potentially suspicious or abnormal activity
* Build foundational skills for SOC analyst and GRC roles

**Skills Demonstrated**

* VM setup and basic networking (NAT, Bridged)
* Use of Wireshark for traffic analysis
* Packet filtering and protocol analysis
* Detection of insecure or unusual traffic behavior
* Documentation of technical findings

**Deliverables**

* Report: Home\_VM\_Lab\_Network\_Traffic\_Analysis\_Edward\_Gaines.doc
* Wireshark screenshots
* Summary of key findings and security takeaways

**Lessons Learned**

* How common protocols behave on a live network
* Importance of monitoring internal traffic
* The power of tools like Wireshark for entry-level cybersecurity analysis
* Reinforced concepts from Security+ and CompTIA Network+

**Author**

Edward Gaines

Cybersecurity Student | GRC & SOC Enthusiast

May 2025