Foundational Network Defense & Traffic Analysis

Nicholas Massei

Cybersecurity Project/Lab

July 10, 2025

Introduction

In this task, I focused on understanding core network security principles and implementing essential defensive measures in a virtual lab environment. I began by researching the common network threats, including viruses, worms, trojans, and phishing attacks. Then, I wanted to transition into setting up and securing a basic network using VirtualBox – with 2 VMs – and my home router. I planned for these exercises to give me hands-on experience with both network defense in theory, and real-world application.

Network Threats

- **Virus**: A virus is malicious code that can attach itself to a legitimate program or file that spreads when the infected item is run or shared. Simply put, viruses can damage files, corrupt systems, and slow down performance.
- **Worm**: A worm is a standalone program that can replicate and spread across networks without user action. Unlike a virus, it doesn't need to attach to a file. Also, worms can often consume bandwidth or overload systems.
- **Trojan Horse**: A trojan is another type of malicious program that relies on pretending to be harmless or useful software. Once a trojan is installed, it can open a back door for attackers, steal sensitive data, or act as a Remote Access Trojan (RAT) to give full remote access of the system to the attacker.
- **Phishing**: Phishing is a common technique that tricks users through emails, websites, or messages into giving away sensitive information such as user credentials or credit card numbers. Attackers often impersonate trusted entities to seem convincing as well. Phishing attacks can range from broad, generic campaigns, to highly targeted attacks that are carefully researched and personalized, such as spear phishing.

Security Concepts

- **Firewalls**: Block/allow traffic based on rules (Windows Defender Firewall).
- **Encryption**: Secures data in transit (such as HTTPS or WPA2/WPA3).
- **Secure Configs**: Changing default router/admin passwords, disabling unused ports, and others.

Reference

National Institute of Standards and Technology. *Computer Security Resource Center Glossary*. U.S. Department of Commerce. https://csrc.nist.gov/glossary

Set up a simple network enviornment

Set up using VirtualBox – 2 virtual machines (Windows 10 & Ubuntu)

Enabled and configured basic firewall on Windows machine using Windows Defender Firewall

Set up other basic security configurations and network encryption by accessing my router's configuration page by entering the default gateway IP address into my web browser (gateway located by utilizing "ipconfig" in powershell). From there, I navigated to the wireless security settings and confirmed that WPA2-PSK (AES) was enabled to ensure strong encryption for my network. Also replaced the default credentials in use with a strong password via password manager (Bitwarden).

Monitor Network Traffic

Internal network created successfully – Windows and Ubuntu machines are able to communicate.

Launched Wireshark on the Windows VM to sniff packets from the Ubuntu VM across the internal network.

Filtered captured traffic using:

- http – viewed unencrypted web traffic (few generated)

- dns – observed domain name lookups

Suspicious Packets Example (not observed)

- Repeated ping traffic from Ubuntu (this example was observed)
- Traffic destined for unfamiliar IPs
- Example of potential DNS misdirections
- Any other unusual traffic depending on context

Document Findings

Configured basic **Windows Defender Firewall** controls on the Windows VM I set up to enforce traffic control and reduce exposure to unauthorized access to the system.

Accessed the router's administrative interface via the default gateway IP (identified beforehand using ipconfig) to review and update wireless security settings. Confirmed **WPA2-PSK (AES)** was enabled, ensuring a strong encryption standard was in place.

Default Wi-Fi credentials were replaced with a strong, randomly generated password stored securely using **Bitwarden**, reinforcing both password security and future access control.

Created a **VirtualBox** Internal Network environment to connect an Ubunutu and Windows machine together to enable direct communication. Verified connectivy between the systems and initiated live traffic capture (simualting practical packet capture scenarios).

Used **Wireshark** for packet capture on the Windows VM to monitor traffic originating from the Ubuntu VM. Also applied filters to capture **HTTP** and **DNS** traffic specifically, observing key protocol behavior in real time. The visibility into just basic traffic patterns highlighted how much can be observed from packet-level inspection from both offensive (red-team) and defensive (blue-team) objectives.

These foundational security measures can significantly reduce the attack surface by limiting unauthorzied access to systems. Even in simple lab environment, practicing enforcing firewall rules,

securing wireless settings, and monitoring traffic tools (such as Wireshark) help simulate the layered defenses needed to detect and prevent threats – and is a great learning experience for anyone interested in information security.

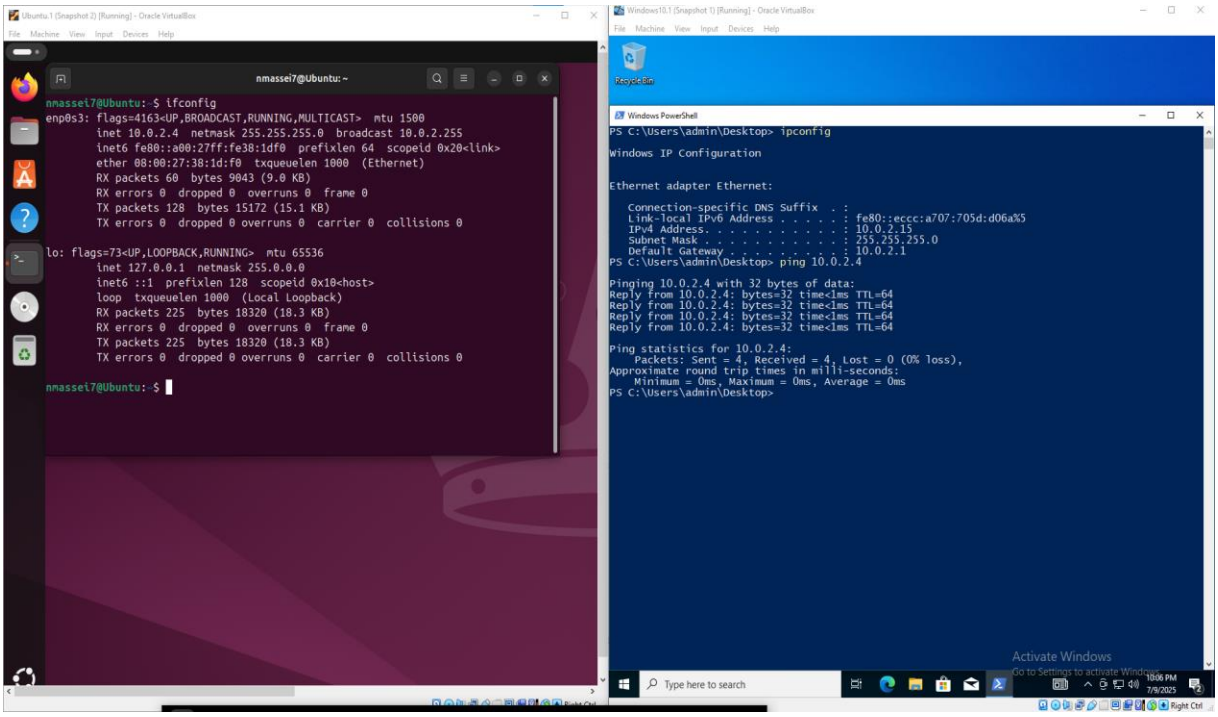
Challenges Faced

While setting up two virtual machines (Windows 10 and Ubuntu), I encountered configuration issues related to internal networking and firewall rule conflicts. Wireshark also initially failed to capture traffic until the correct adapter settings were applied. Troubleshooting these issues deepened my understanding of how VMs are configured.

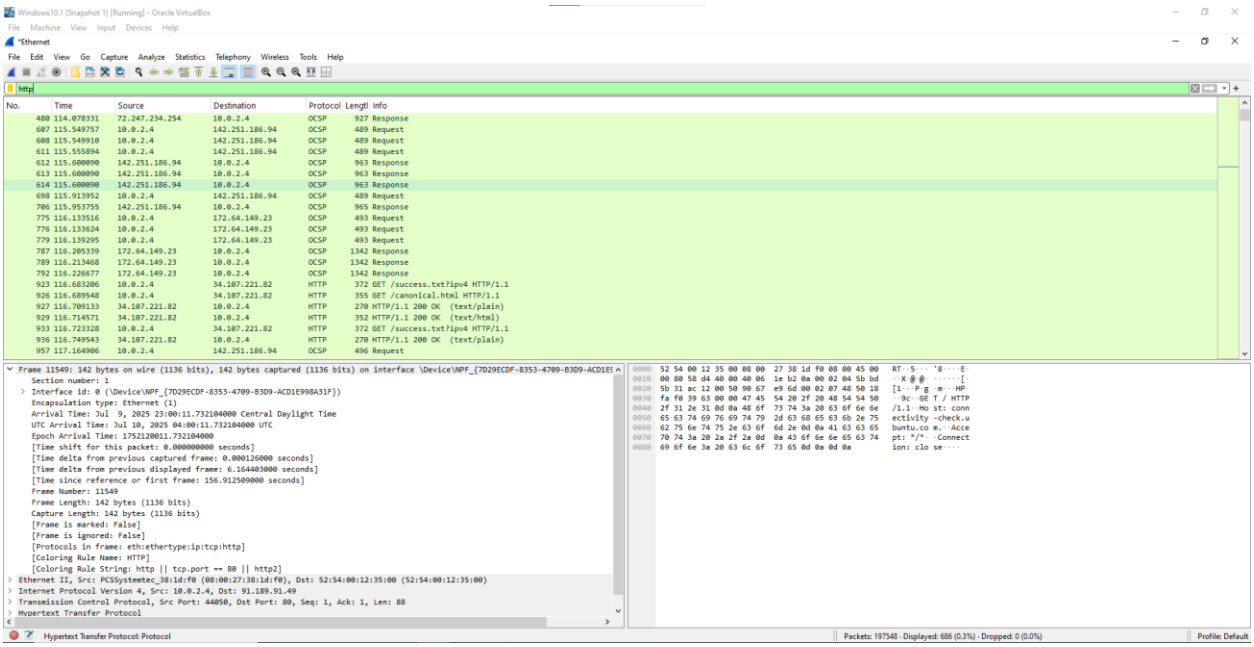
Reflect on Security Best Practices

Even in larger or more complex environments, the importance of basic security measures really stands out. These small steps I went through like enabling a firewall, using strong passwords, and securing the wireless network create a solid foundation that everything else builds on. While they might seem simple at first, I've come to see how they play a huge role in reducing risk and keeping systems protected. Larger networks obviously need more advanced solutions like intrusion detection systems (IDS), endpoint protection, and network segmentation with VLANs, but the basics still matter just as much.

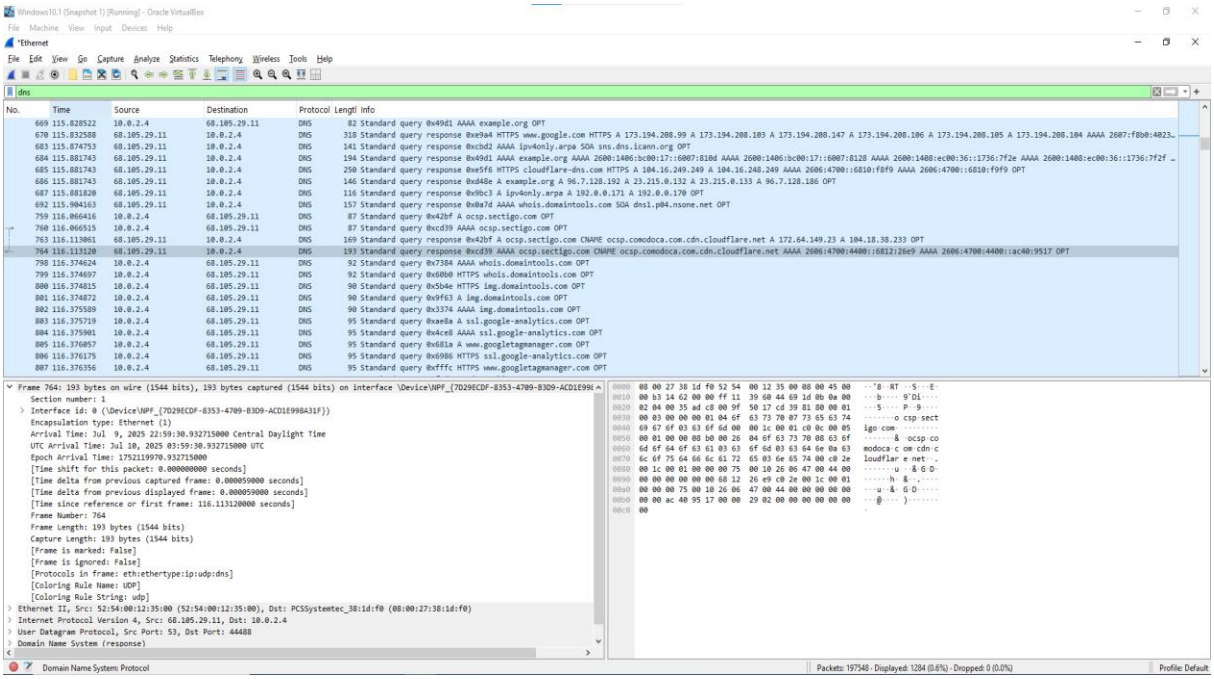
I also think user awareness is key to network security and this really showed in changing default credentials. Things like regular software updates, multi-factor authentication, and avoiding phishing attempts can make a big difference and would be the first things to cover in educating people on the importance of network security. I would also show real-world examples of attacks that happened simply because the basics were ignored as people tend to learn best when they see the actual consequences of oversights like these. Even simple habits, when practiced consistently, can go a long way in strengthening the overall security posture and lowering the attack surface for threat actors.



Successful Ping to connected machines



http packets captured including multiple “GET” requests and OCSP packets sent over http



Captured and observed DNS traffic displaying the records requested during browsing activity.