## ****Network and Security Analysis Report Using Nmap and Wireshark****

### ****1. Introduction****

This report presents an analysis of a network using the Nmap and Wireshark tools to identify potential vulnerabilities and anomalies. The Nmap scan revealed open ports, services, and host details on the target system with IP address 192.168.42.75, while Wireshark was used to capture and analyze network traffic. The key objectives were to understand the network topology, identify vulnerabilities, and analyze anomalies like ARP spoofing and ICMP flooding, which pose significant security risks. Based on the findings, appropriate recommendations are provided to mitigate these risks.

### ****2. Network Topology Analysis (Nmap)****

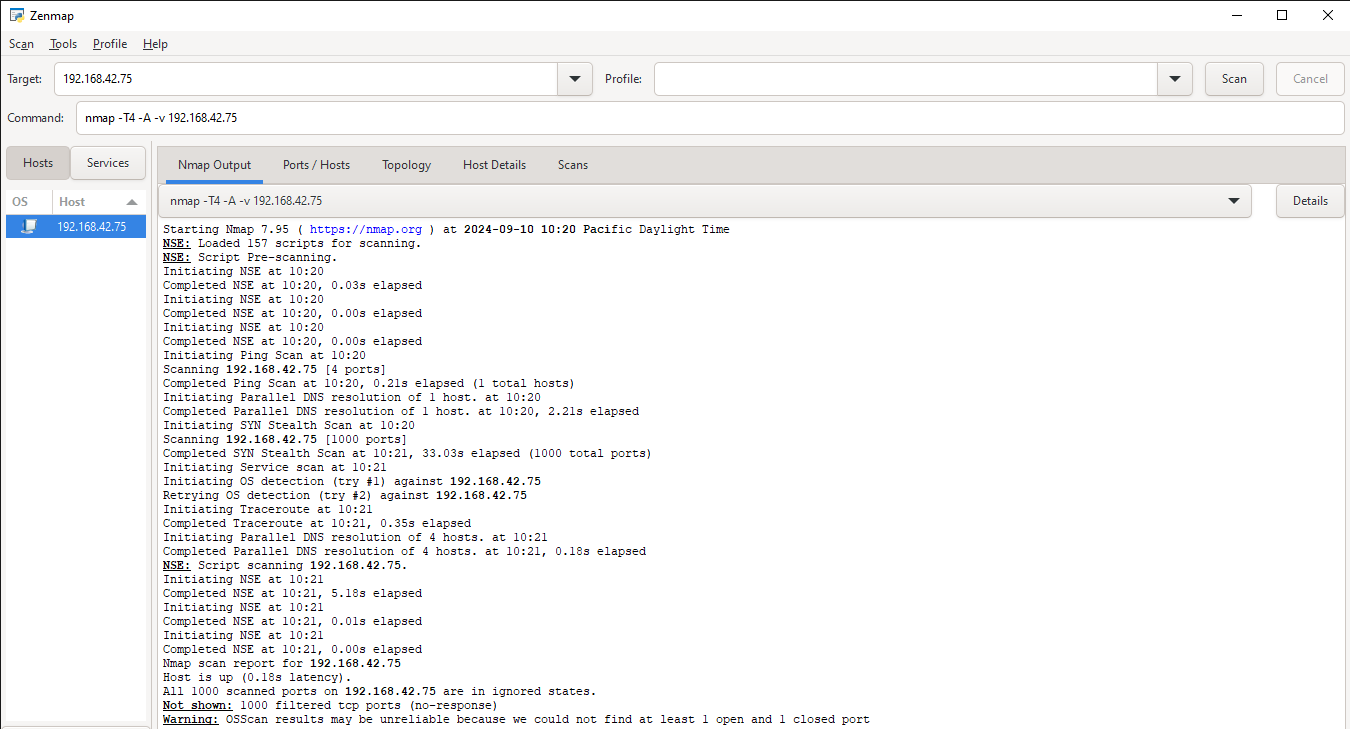
The Nmap scan performed on the target machine (IP: 192.168.42.75) revealed several open ports that expose the system to potential security threats. The scan was performed using the following command:

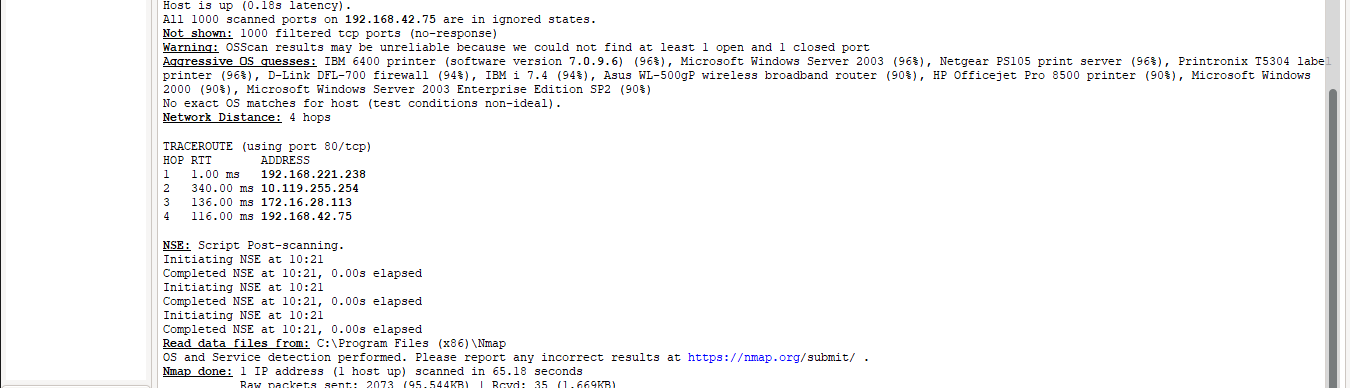
The scan revealed the following open ports:

* **135/tcp** (Microsoft RPC)
* **139/tcp** (NetBIOS)
* **445/tcp** (Microsoft-DS)
* **7070/tcp** (RealServer)

These services expose the host to remote execution attacks, particularly through RPC and SMB vulnerabilities, which are often targeted by malware such as WannaCry. The scan also provided additional host information, indicating that the system is running **Windows 10 (1809 - 21H2)**.

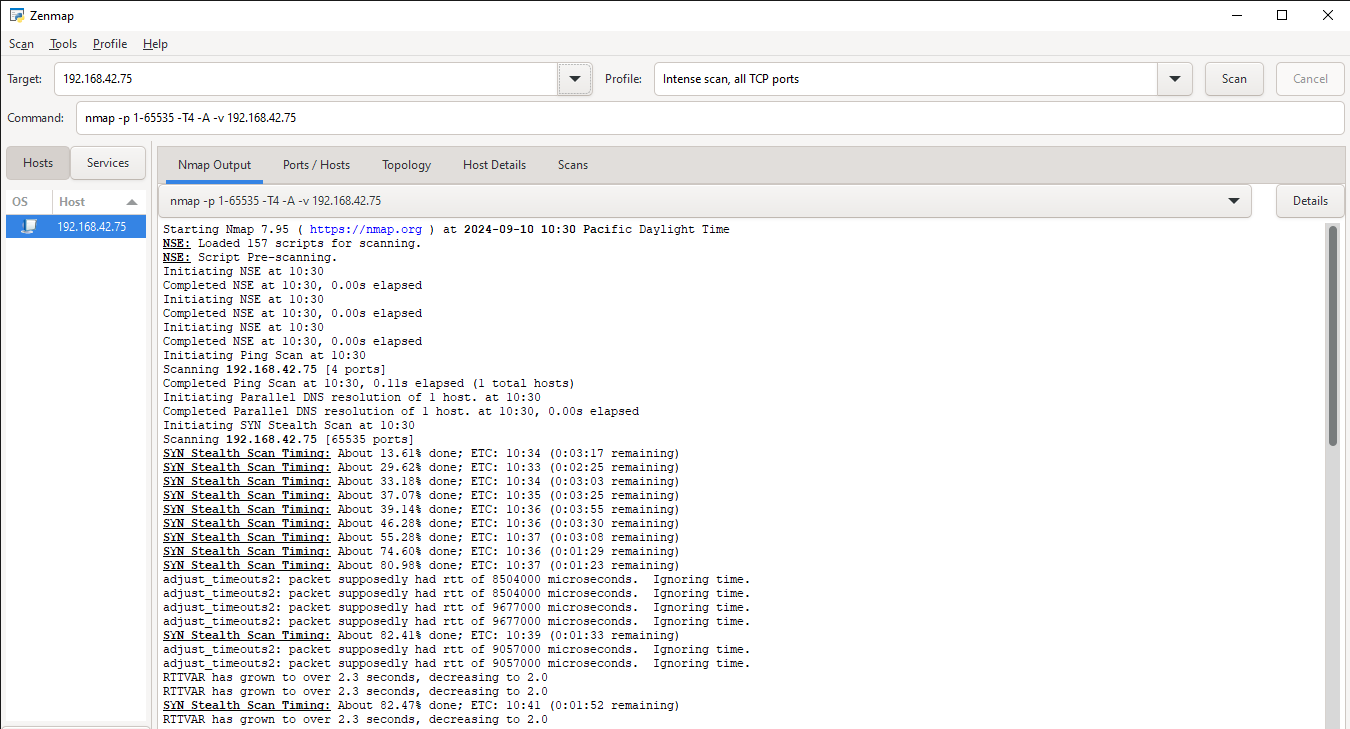
**Screenshot 1: Basic Nmap Scan Output**

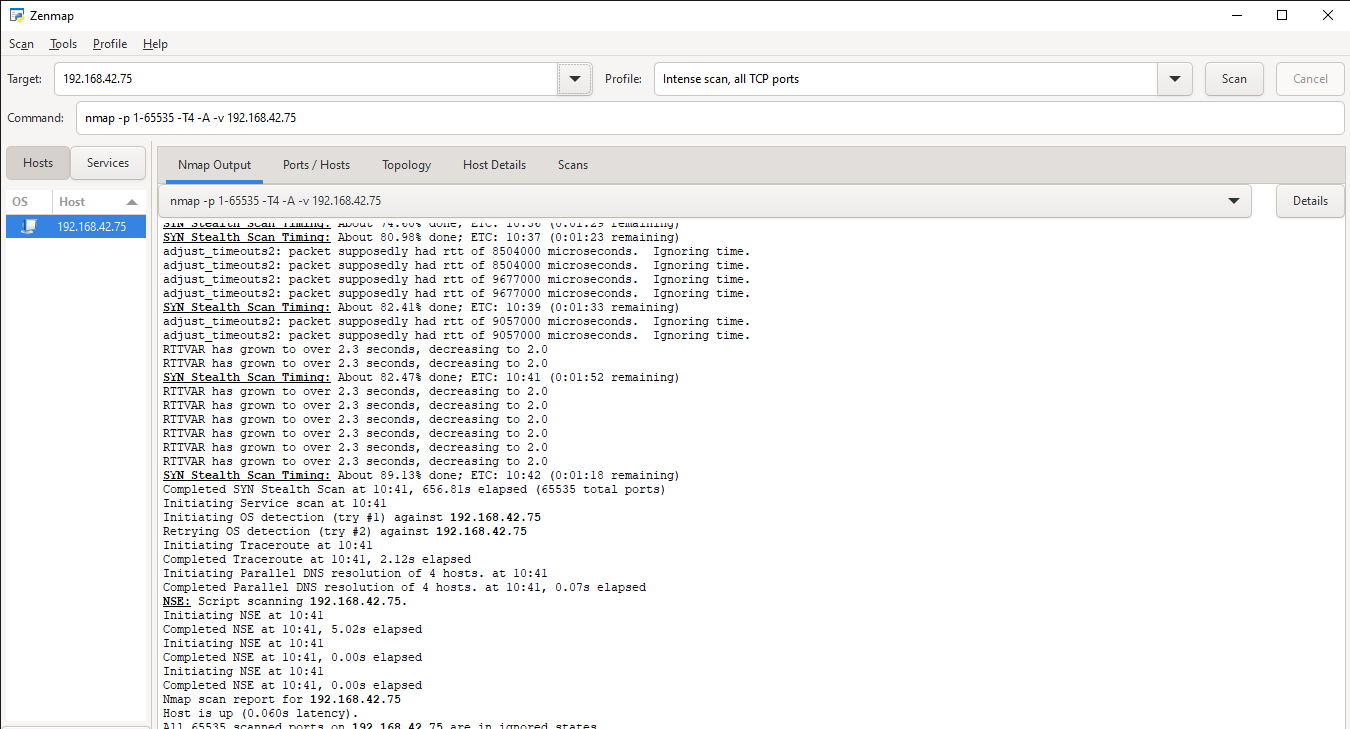


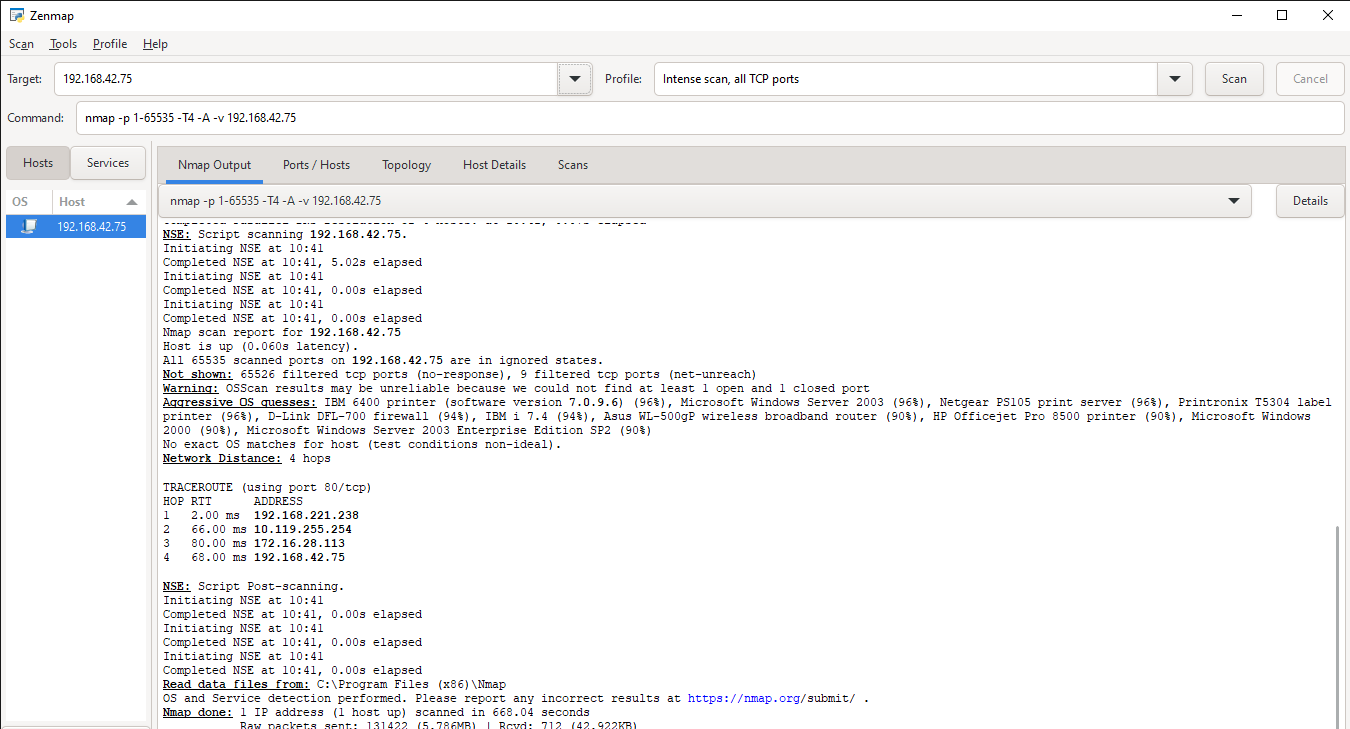


The Nmap output in Figure 1 shows the details of the open ports and services running on the target machine.

In addition, a full port scan was conducted to examine whether additional services were exposed. The scan of all 65,535 TCP ports was conducted using the following command:



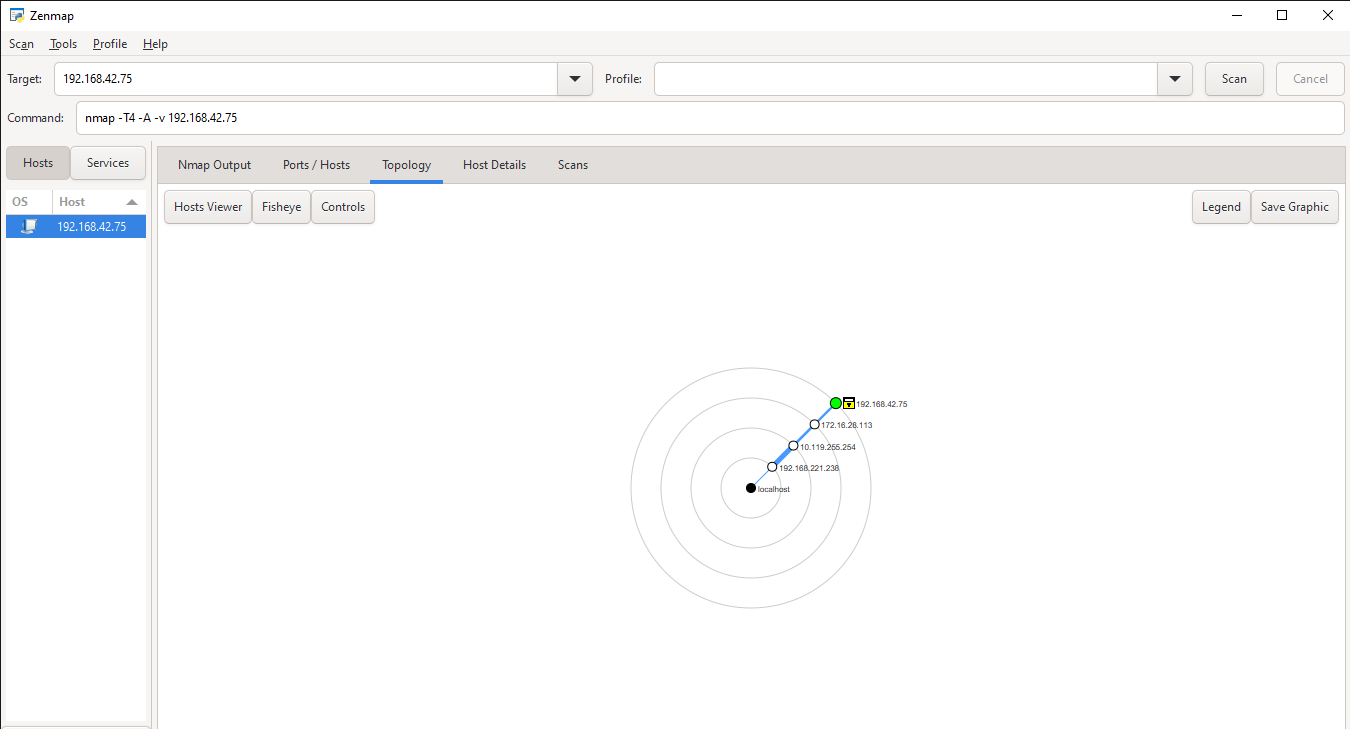




reveal any additional critical services running on the machine. However, it emphasizes the importance of securing the open ports detected in the basic scan.

### ****3. Network Topology Visualization****

The topology generated by Nmap visually represents the connections of the target machine within the network. As seen in the visualization, the target machine (192.168.42.75) has direct connections to the scanning machine and is marked with a yellow circle, indicating 3 to 6 open ports. This visualization highlights the network’s configuration and helps in identifying potential security gaps that could be exploited.



### ****4. Vulnerabilities and Their Implications****

Based on the open ports detected during the Nmap scan, the following vulnerabilities were identified:

* **Port 135 (Microsoft RPC)**: This port is often targeted by remote execution attacks, allowing attackers to execute commands on the system without authorization.
* **Ports 139 and 445 (NetBIOS and SMB)**: These ports are associated with Windows file-sharing services and are commonly exploited in attacks like WannaCry ransomware. They pose a significant risk for network-wide malware propagation.
* **Port 7070 (RealServer)**: This port is used for streaming media services and, if misconfigured, could allow unauthorized access to the server.

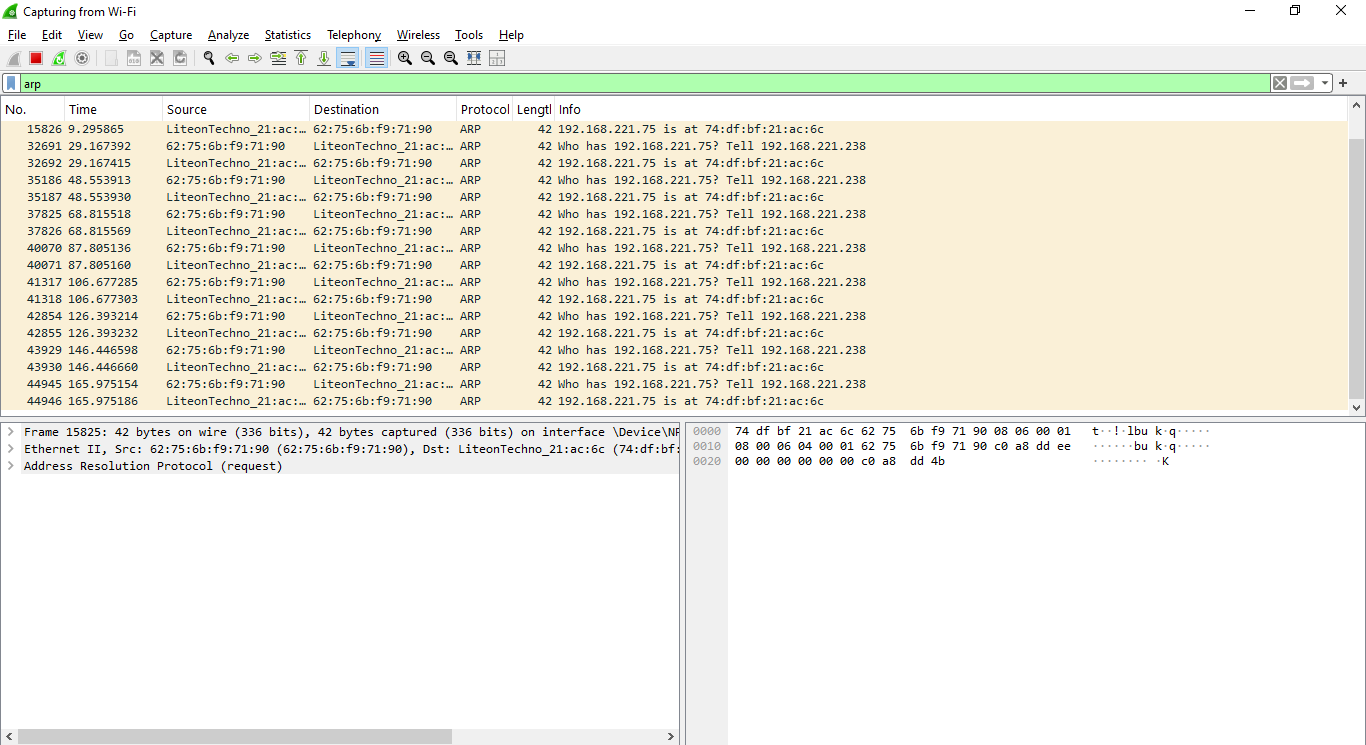
Failure to secure these ports could lead to data breaches, malware infections, and denial-of-service (DoS) attacks (Asriza et al., 2023).

### ****5. Wireshark Anomalies Analysis****

Wireshark was used to capture and analyze network traffic on the target machine. Two major anomalies were identified: **ARP spoofing** and **ICMP flooding**.

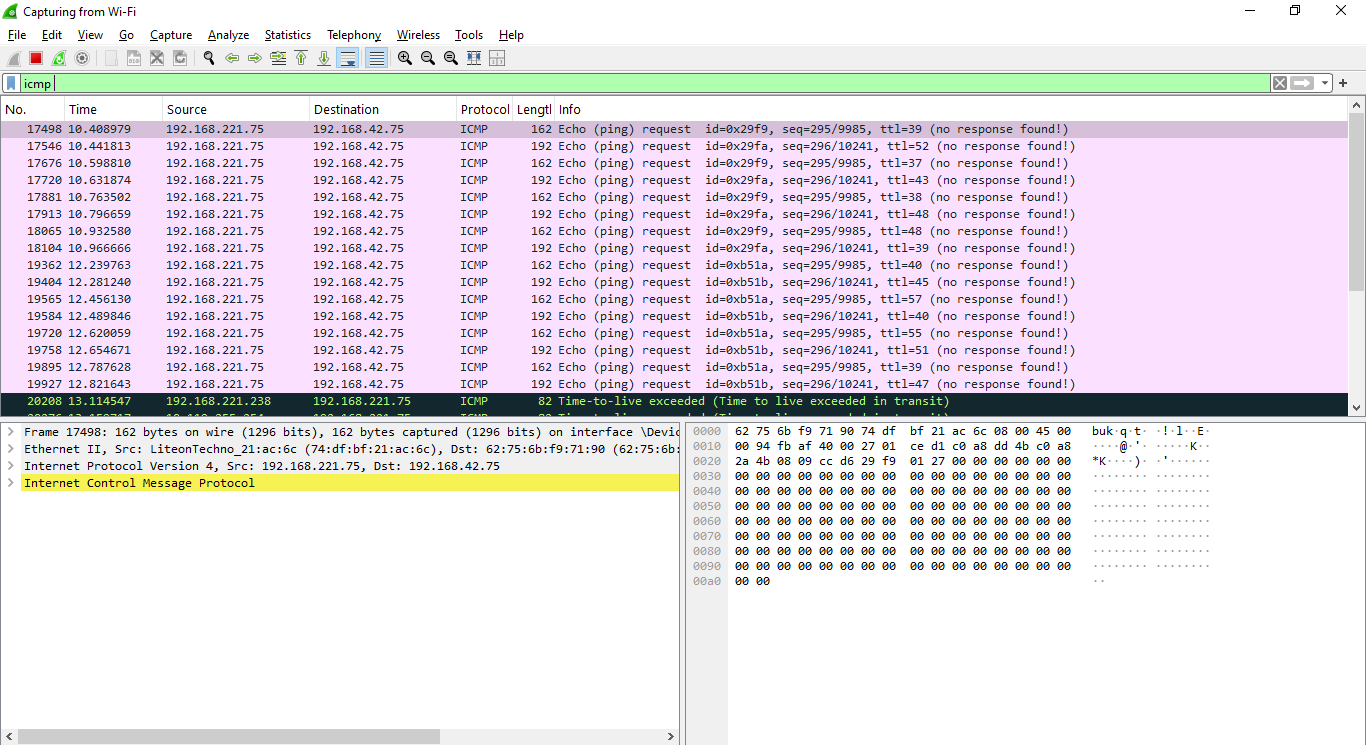
**ARP Requests Anomalies (ARP Spoofing)**

During the capture, Wireshark detected multiple ARP requests without corresponding replies. This is indicative of a possible ARP spoofing attack, where an attacker associates their MAC address with the IP address of another host, allowing them to intercept, modify, or block traffic.



**ICMP Traffic Anomalies (ICMP Flooding)**

In addition to ARP anomalies, a high volume of ICMP requests (ping requests) was detected. These ICMP requests could be used for reconnaissance by external attackers, attempting to map the network and identify live hosts. If left unchecked, this could escalate into a denial-of-service (DoS) attack, overwhelming the network.



### ****6. Recommendations****

To mitigate the identified vulnerabilities and anomalies, the following actions are recommended:

1. **Disable Unused Services**: Close ports 135, 139, 445, and 7070 if they are not required for legitimate operations. If these services must remain open, ensure they are fully updated and patched to prevent exploitation.
2. **Implement Firewall Rules**: Configure firewall rules to restrict access to services running on the open ports (135, 139, 445). Limit access to internal users only to reduce the attack surface.
3. **Intrusion Detection Systems (IDS)**: Deploy an IDS to detect anomalies like ARP spoofing and ICMP floods in real-time. IDS solutions can alert network administrators to suspicious activity and help mitigate threats before they escalate.
4. **Dynamic ARP Inspection (DAI)**: Implement DAI to prevent ARP spoofing by verifying ARP requests and responses. This ensures that attackers cannot manipulate the ARP cache to intercept network traffic.
5. **Regular Monitoring**: Continuously monitor the network using tools like Wireshark and Nmap to identify unusual traffic patterns and ensure that security patches are applied promptly.

### ****7. Conclusion****

The analysis of the network using Nmap and Wireshark revealed several critical vulnerabilities and anomalies that could compromise the security of the network. By addressing these issues—such as closing unused ports, implementing firewall rules, and deploying an IDS—the organization can significantly reduce the risk of attacks and maintain the integrity of its network. Continuous monitoring and proactive management of network traffic are essential to prevent future incidents.

**Reference**

Asriza Yolanda, & Cutifa Safitri. (2023). Analyzing Proxychains Traffic on the Pentest Scenario: Enhancements in Network Forensics through Wireshark. <https://doi.org/10.1109/icitcom60176.2023.10442589>