SOC ANALYST TRANING REPORT

ON

MALWARE ANALYSIS USING WIRESHARK

ANALYSED AND REPORTED

BY

ALI CHINASA JULIET

INSTRUCTOR: MR OLA OLAITAN

DATE: AUGUST 2024

Executive Summary

This report provides a detailed analysis of a network traffic capture (PCAP file) using Wireshark to identify potential malware activities. The investigation focused on identifying suspicious network behaviors, anomalies, and Indicators of Compromise (IOCs) by examining various network protocols, IP addresses, and traffic patterns. The analysis revealed that there was a transfer of potentially malicious files, including a password.txt file sent via an email service, indicating a possible data exfiltration attempt. Key security measures are recommended to mitigate identified threats.

Overview

The objective of this analysis was to investigate captured network traffic to detect any signs of malicious activity. Wireshark, a network protocol analyzer, was used to examine the PCAP file. The analysis focused on the following key areas:

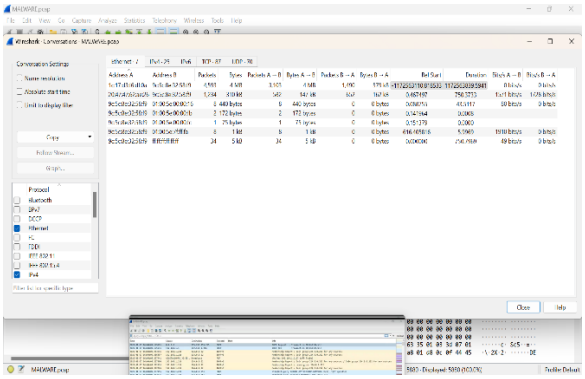
1. **Protocol Usage**: Identified the use of various protocols, including HTTP, TCP, UDP, and DHCP but we focused more on HTTP AND DHCP.
2. **Conversations and IP Analysis**: Analyzed conversations between source and destination IP addresses to understand the nature of communications.
3. **Indicators of Compromise (IOCs)**: Detected potential IOCs, such as unusual IP addresses and suspicious file transfers.
4. **Geolocation and Host Information**: Used geolocation data to identify the location of communications and hostname information to determine the device involved.

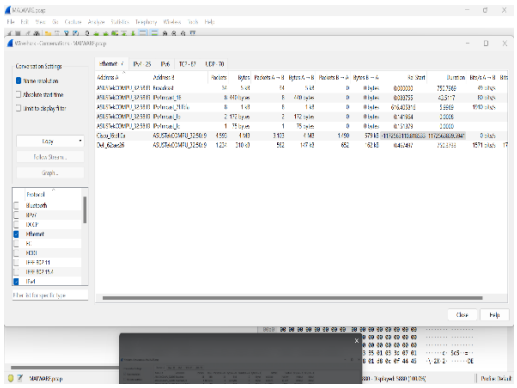
Analysis and Investigation

1. Protocol Analysis:

- **Protocol Statistics**: The Wireshark statistics tab was utilized to identify the protocols involved in the captured network traffic. The key protocols observed included IPv4, IPv6, TCP, UDP, and HTTP. These protocols are commonly used for network communication, but their usage in this capture indicated possible malicious activities.

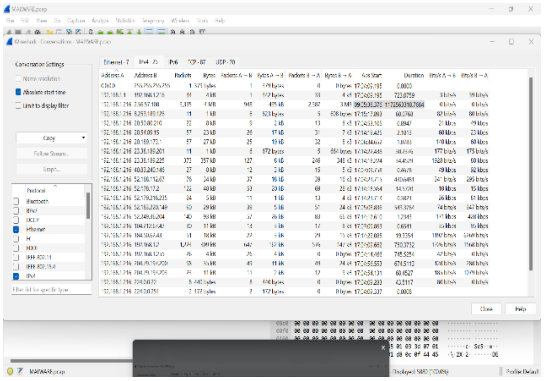
- **Conversation Analysis**: Through the conversation tab, we could identify communications between various devices. Notably, a device with the MAC address ASUS was communicating with devices identified as CISCO_F6:DF:0A and DELL_62:AE:26. The analysis of conversations helped reveal patterns of communication that were unusual and potentially indicative of malicious intent.

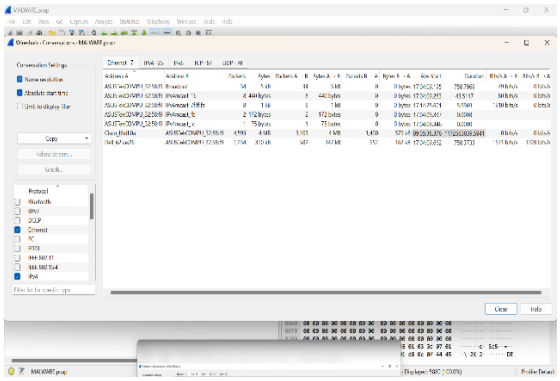




2. Name Resolution and Anomalies Detection:

- **Name Resolution**: By enabling name resolution, we identified the domain and host names involved in specific conversations. For example, a device with the hostname DESKTOP-GXMYNO2.SPOONWATCH.NET was identified as a client in several communications.
- **Expert Information Analysis**: The expert information feature in Wireshark was used to spot anomalies, such as unexpected communication patterns and potential protocol misuse, which could indicate malicious activities or network intrusions.

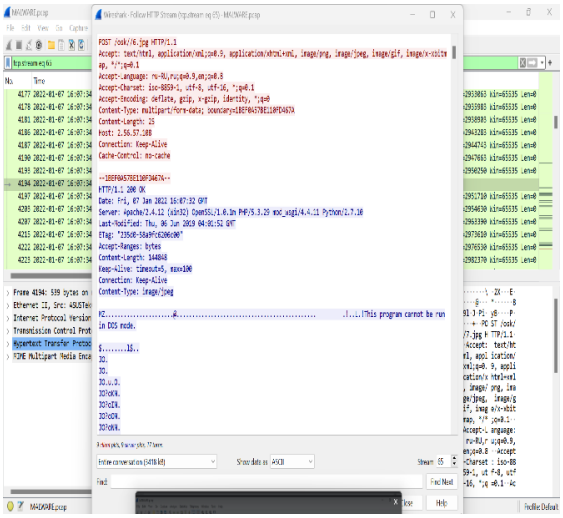


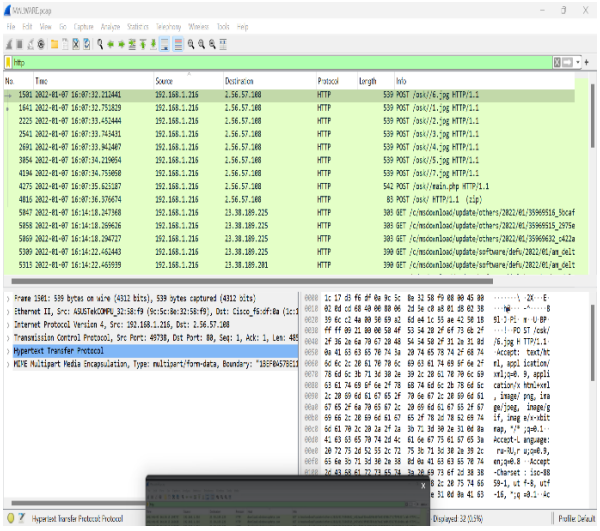


3. HTTP Traffic and File Transfer:

- **HTTP Traffic Analysis**: By filtering for HTTP traffic, the investigation uncovered communications between the source IP address 192.168.1.216 and the destination IP 2.56.57.108. The traffic captured between these IPs indicated a short-lived but significant exchange that occurred from 2022/01/07 16:07:32 to 2022/01/07 16:07:32.376674.

- **Malicious File Detection**: A specific HTTP stream revealed a password.txt file transmitted from a client to a server using a POST request. This file appeared to contain login credentials, indicating a possible data exfiltration attempt via an email service (Outlook). The detection of this file is a significant IOC and suggests malicious intent to harvest credentials or perform unauthorized access.



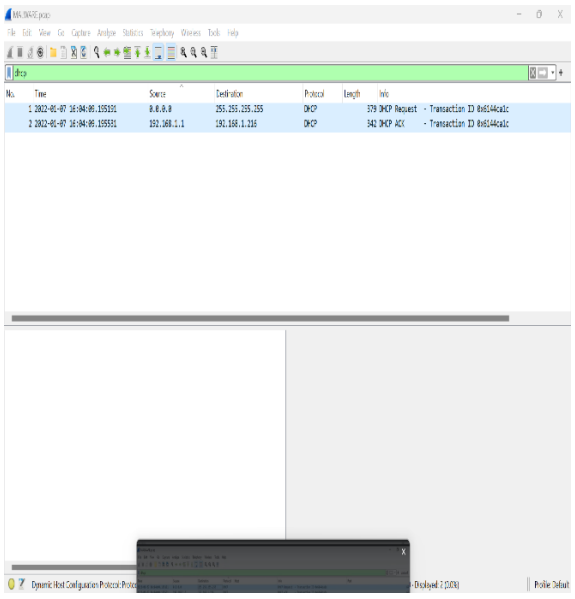


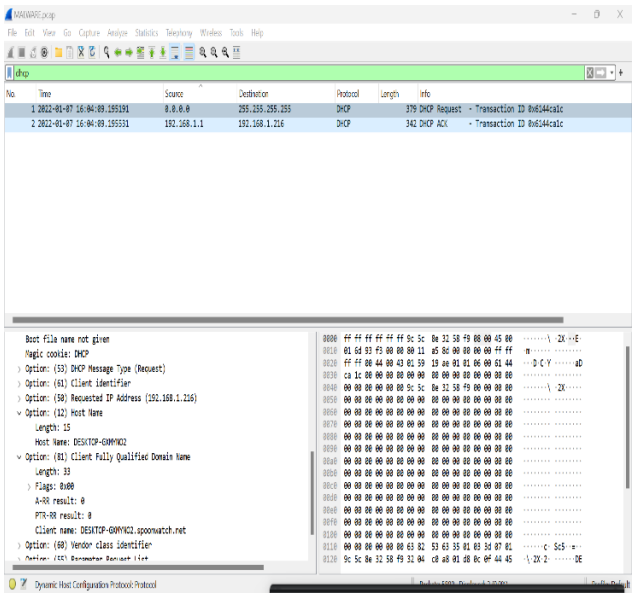
4. DHCP Analysis and Host Identification:

- **DHCP Filtering**: Filtering for DHCP traffic allowed the identification of the host involved in the communication. The source IP 192.168.1.1 (likely a router or gateway) communicated with the destination IP 192.168.1.216, which had the client name DESKTOP-GXMYNO2. The DHCP analysis provided further insight into the devices involved and their potential roles in the network.

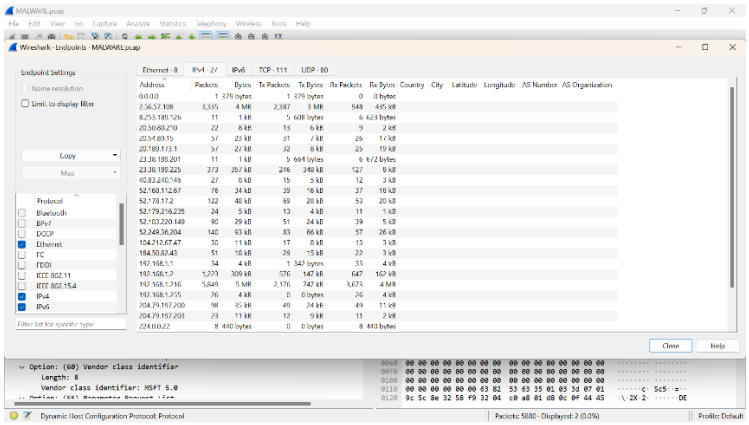
5. Geolocation and Endpoint Analysis:

- **Geolocation Data**: Enabling geolocation features in Wireshark allowed the analysis of the physical locations associated with IP addresses involved in the traffic. The communication between devices was traced to specific geographic locations, which can help correlate physical presence with digital activities.





- **Endpoint Analysis**: The endpoint tab in Wireshark provided a comprehensive view of the IPv4 and IPv6 addresses, including additional details like country, city, latitude, AS number, and AS organization. This information was crucial in understanding the broader network context and identifying external entities involved in the communication.



In summary

Using Wireshark to analyze the network traffic recorded in the PCAP file, multiple signs of possible malware activity and attempts at data theft were found. There are worries regarding unauthorized access and credential theft after it was discovered that a password.txt file containing login credentials

was sent via HTTP. Furthermore, anomalous patterns of communication between particular MAC addresses and IP addresses imply deliberate malicious behavior.

Recommendations

Based on the findings of this analysis, the following security measures are recommended:

1. **Quarantine the Identified Malicious Document**: Immediately quarantine the password.txt file detected in the network traffic to prevent further access or distribution.
2. **Mandatory Password Reset**: Implement a mandatory password reset policy for all users whose credentials may have been compromised, particularly for accounts identified in the malicious file transfer.
3. **Network Segmentation and Monitoring**: Enhance network segmentation to isolate critical systems from general network traffic. Deploy advanced network monitoring tools to detect and alert on unusual communication patterns.
4. **Update and Patch Systems**: Ensure all devices, including routers and endpoints, are updated with the latest security patches to prevent exploitation of known vulnerabilities.
5. **Employee Training and Awareness**: Conduct regular training sessions for employees on recognizing phishing attempts and the importance of safeguarding credentials.
6. **Continuous Threat Intelligence Monitoring**: Integrate threat intelligence feeds into security monitoring tools to stay updated on new IOCs and potential threats.