WIRESHARK 101 – NETWORK TRAFFIC ANALYSIS REPORT

Platform: TryHackMe

Room: Wireshark 101 (Premium)

Role: Junior SOC Analyst / Network Security Analyst

Analysis Type: PCAP Traffic Analysis

Tools Used: Wireshark

Status: Room Completed (100%)

1. Introduction

This report documents the analysis and investigation of multiple network traffic captures (PCAP files) as part of the *Wireshark 101* room on the TryHackMe platform.

The objective of this report is to:

- Analyze real network traffic using Wireshark.
- Understand how common network protocols behave in normal conditions.
- Identify protocol-specific indicators that may point to suspicious or malicious activity.
- Demonstrate proper SOC-style documentation and investigation methodology.

The analyzed traffic includes ARP, ICMP, TCP, DNS, HTTP, HTTPS, and an exploit-based PCAP (Zerologon). These protocols are frequently reviewed during SOC investigations, DFIR cases, and threat hunting activities.

2. Analysis Summary

Task	Protocol	PCAP File	Purpose
Task 7	ARP	task7.pcap	Address resolution & MAC/IP mapping
Task 8	ICMP	task8.pcap	Network reachability analysis
Task 9	TCP	task9.pcap	Connection behavior analysis
Task 10	DNS	task10.pcap	Name resolution monitoring
Task 11	HTTP	task11.pcap	Clear-text web traffic analysis
Task 12	HTTPS	snakeoil2.pcap	Encrypted traffic & decryption
Task 13	Exploit	Zerologon PCAP	Attack chain identification

3. Detailed Traffic Analysis

3.1 ARP Traffic Analysis (task7.pcap)

Protocol: Address Resolution Protocol (ARP)

Investigation Steps:

- Applied display filter: `arp`
- Inspected Opcode field to distinguish Request vs Reply packets
- Identified source MAC addresses and corresponding IPs

Findings:

- Packet 6 Opcode was identified as **Request (1)**.
- Packet 19 source MAC address was **80:fb:06:f0:45:d7**.
- Reply packets were identified as packets **76, 400, 459, and 520** based on Opcode value **2**.
- The IP address associated with MAC **80:fb:06:f0:45:d7** was **10.251.23.1**.

Conclusion:

ARP traffic observed was normal and followed expected request–reply behavior. No ARP poisoning indicators were detected.

3.2 ICMP Traffic Analysis (task8.pcap)

Protocol: Internet Control Message Protocol (ICMP)

Investigation Steps:

- Applied filter: `icmp`
- Inspected ICMP Type and Code fields
- Reviewed timestamps and payload data

Findings:

- Packet 4 was identified as an **Echo Request (Type 8)**.
- Packet 5 was identified as an **Echo Reply (Type 0)**.
- Packet 12 timestamp resolved to **May 30, 2013**.
- Packet 18 contained a full hexadecimal data payload used for ICMP testing.

Conclusion:

ICMP traffic reflected normal ping activity with no malformed or suspicious packets.

3.3 TCP Traffic Analysis

Protocol: Transmission Control Protocol (TCP)

Investigation Steps:

- Reviewed TCP handshake behavior (SYN, SYN-ACK, ACK)
- Analyzed sequence and acknowledgment numbers
- Observed RST packets

Findings:

- TCP traffic demonstrated expected connection setup behavior.
- Presence of RST packets may indicate closed ports or scanning activity.

Conclusion:

TCP analysis highlighted the importance of reviewing packet sequences collectively rather than individually to understand session behavior.

3.4 DNS Traffic Analysis (task10.pcap)

Protocol: Domain Name System (DNS)

Investigation Steps:

- Applied filter: `dns`
- Reviewed query names and transaction IDs

Findings:

- Packet 1 queried **8.8.8.8.in-addr.arpa**.
- Packet 26 queried **www.wireshark.org**.
- Transaction ID for packet 26 was **0x2c58**.

Conclusion:

DNS traffic followed expected query-response behavior over UDP port 53. No DNS tunneling indicators were observed.

3.5 HTTP Traffic Analysis (task11.pcap)

Protocol: Hypertext Transfer Protocol (HTTP)

Investigation Steps:

- Applied filter: `http`
- Used Protocol Hierarchy, Endpoints, and Export Objects features
- Followed TCP streams to extract full URIs

Findings:

- DNS traffic accounted for **4.7%** of packets.
- Endpoint ending in `.237` was **145.254.160.237**.

- User-Agent in packet 4 indicated a Windows XP system.
- Full request URIs were successfully extracted from packets 18 and 38.

Conclusion:

HTTP traffic allowed full visibility into requested resources, highlighting why unencrypted traffic poses a security risk.

3.6 HTTPS Traffic Analysis (task12.pcap)

Protocol: HTTPS (TLS)

Investigation Steps:

- Imported RSA private key into Wireshark
- Decrypted TLS traffic
- Inspected decrypted HTTP streams

Findings:

- Packet 31 requested **/icons/apache_pb.png**.
- Packet 50 requested **/icons/back.gif**.
- User-Agent identified a Linux-based Firefox browser.

Conclusion:

Encrypted traffic can be analyzed when decryption keys are available, allowing SOC analysts to inspect otherwise hidden content.

3.7 Exploit PCAP Analysis – Zerologon

Attack Type: Zerologon (CVE-2020-1472)

Identified Entities:

- Attacker IP: **192.168.100.128**
- Domain Controller: **192.168.100.6**

Indicators Observed:

- Excessive DCERPC and EPM traffic
- SMB and DRSUAPI usage
- Behavior consistent with secretsdump

Conclusion:

The PCAP clearly demonstrated a successful Zerologon exploitation followed by credential dumping activity.

4. Investigation Process

The following SOC methodology was applied throughout the analysis:

- Reviewed PCAP metadata and protocol distribution
- Applied protocol-specific display filters
- Inspected packet headers and payloads
- Correlated traffic patterns across protocols
- Documented findings for reporting and escalation

5. Findings

- Multiple protocols were analyzed successfully using Wireshark.
- Normal vs suspicious traffic patterns were clearly distinguishable.
- Encrypted traffic analysis is possible with proper key material.
- Exploit PCAP analysis requires both protocol knowledge and threat intelligence awareness.

6. Conclusion

The *Wireshark 101* room provides practical, SOC-relevant experience in packet analysis and incident investigation. The hands-on analysis of both normal and malicious traffic reinforces essential skills required for SOC analysts, DFIR investigators, and network security professionals.

This investigation demonstrates the ability to analyze PCAPs, identify protocol behavior, and document findings in a professional SOC-style report.

Overall Assessment: True Positive learning outcomes with strong practical value.