Network Traffic Analysis Report

Objective

Analyze network traffic using tcpdump in a cybersecurity lab environment.

Environment

Online Linux Lab
Tool used: tcpdump

Methodology

Traffic was captured and analyzed using tcpdump to identify:
• DNS traffic
• External connections
• Internal communications

Findings

The following activities were observed:
• DNS requests to external servers
• Secure HTTPS connections
• Normal internal network traffic

No confirmed malicious activity detected.

Security Relevance

Network traffic analysis helps detect:
• Suspicious connections
• Data exfiltration
• Command and control traffic

Conclusion

This analysis demonstrates basic network monitoring skills required for SOC Analysts.