Task-3:Incident Response Report

Executive Summary

Preliminary analysis of network traffic capture reveals potentially suspicious communication from host 192.168.29.249. Key findings: Unusual TCP traffic to 103.162.246.81:1514, significant TLS traffic, and a TCP reset. Root cause undetermined due to limited data. Mitigation focuses on further investigation & monitoring. Recommendations: enhanced monitoring, logging, security best practices.

Incident Description

- Unusual TCP Traffic (Port 1514): 192.168.29.249 ⇔ 103.162.246.81 (Port 1514). Non-standard port, potential custom app/malware. Data exchange observed.

- TLS (HTTPS) Traffic (Port 443): Significant TLSv1.2 traffic involving 192.168.29.249 & multiple external IPs (54.220.192.176, 204.79.197.203, 20.207.73.85, IPv6 addresses). Could be HTTPS, encrypted C2, data exfiltration, or benign traffic.

- TCP Reset (RST):From 52.26.51.69:443 to 192.168.29.249:53330. Potential connection rejection, scanning, or network issue.

- Normal Traffic:IGMPv3, ICMPv6 (network management).

Root Cause Analysis

Potential Incident Scenarios: Suspicious Port 1514 Traffic: Malware Command & Control (C2) on non-standard port.
Legitimate non-standard application (less likely suspicious).
Ambiguous TLS Traffic: Encrypted C2 or Data Exfiltration (if linked to other suspicious activity).
Normal HTTPS web browsing (possibility). TCP Reset (52.26.51.69:443): Connection Rejection (server-side). Port Scanning/Probing. Benign Network Event.

Key Suspicion: Unusual TCP port 1514 traffic to 103.162.246.81 is the primary concern and needs further investigation.

Mitigation Steps

1. Analyze Port 1514 Traffic (Deeper): Examine full packet capture (if available) for TCP stream data. Research port 1514 for known uses.

2. Investigate IP 103.162.246.81: OSINT (VirusTotal, abuseIPDB, etc.) for reputation & location. WHOIS lookup for owner details.

3. Monitor Traffic to/from 103.162.246.81: Implement network monitoring for traffic involving 103.162.246.81 (especially port 1514).

4. Check Endpoint Logs (192.168.29.249): System, application, endpoint security logs around capture timestamp. Look for processes connecting to 103.162.246.81:1514, unusual activity, security alerts. Do NOT block 103.162.246.81 traffic yet - investigate first.

Recommendations for Prevention

1. Enhance Monitoring & Logging: Comprehensive network monitoring. Robust logging (firewall, network devices, servers, endpoints). Centralized SIEM (Splunk) for analysis.

2. Deploy IDS/IPS: Network & host-based IDS/IPS. Alerts for unusual ports & suspicious IPs.

3. Strengthen Endpoint Security: Up-to-date Antivirus & EDR solutions.

4. Enforce Firewall Rules: Review & strengthen inbound/outbound rules. Egress filtering (limit outbound ports/services).

5. Security Awareness Training: User training on phishing, malware, cyber threats.

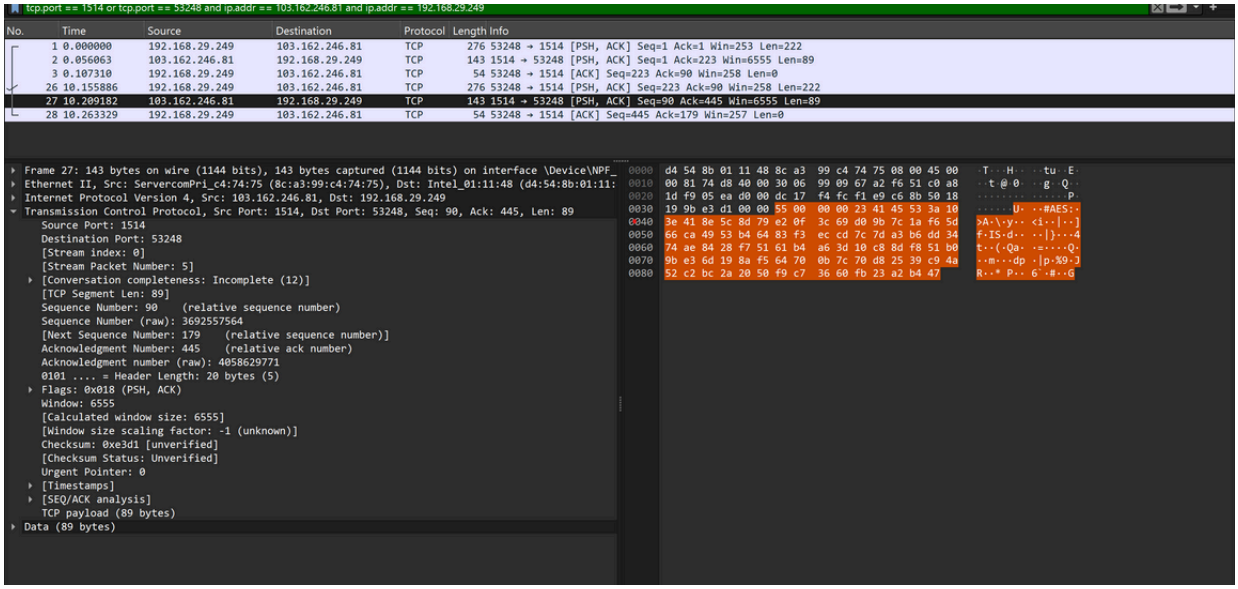
6. Incident Response Plan: Develop, maintain, test IR plan.

Conclusion:

Preliminary analysis points to potentially suspicious network activity, particularly TCP port 1514 traffic. Further investigation with more comprehensive data (full capture, logs) is crucial. Mitigation focuses on investigation & monitoring. Prevention recommendations aim to enhance security posture and incident response readiness. This is a preliminary report - further investigation is essential.

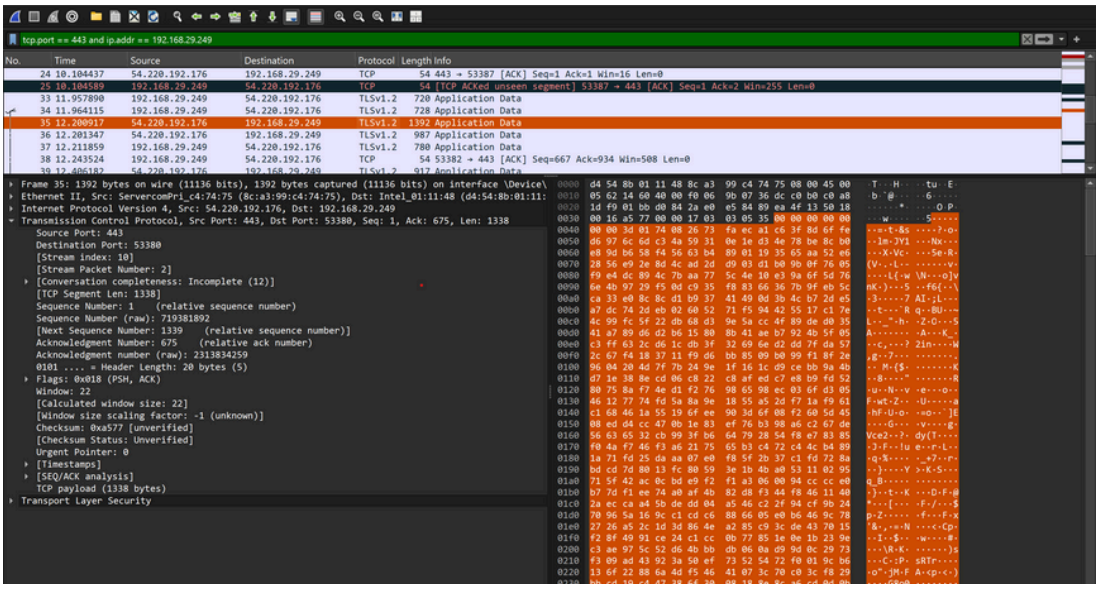
Screenshots:

Screenshot Highlighting Suspicious Port 1514 Traffic:



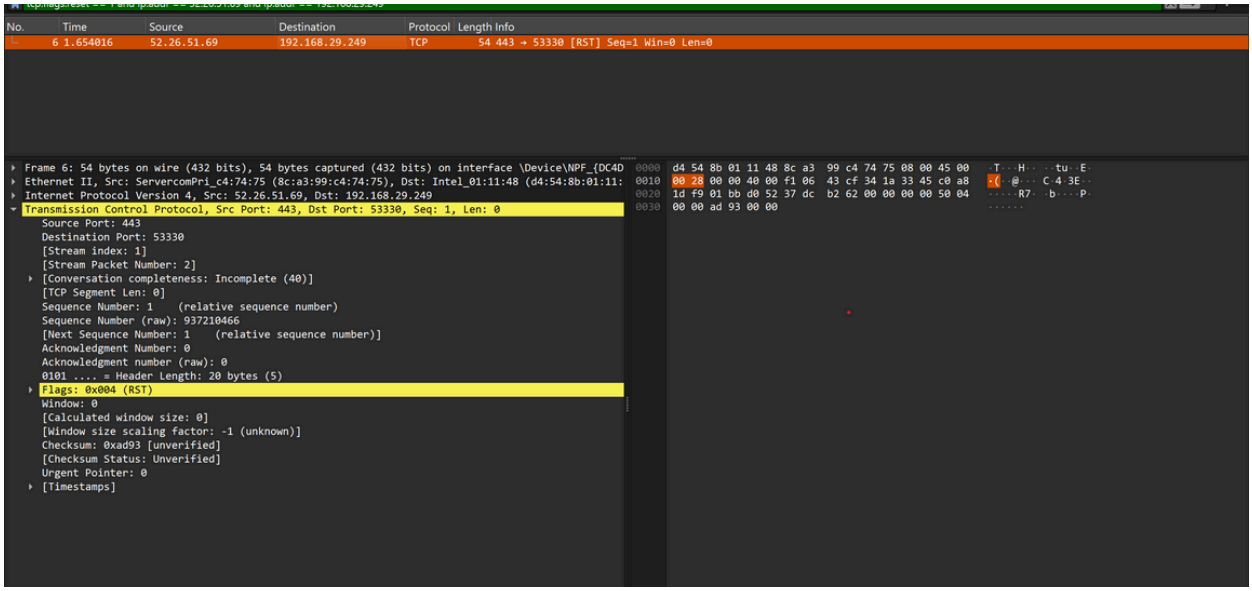
Suspicious Port 1514 Traffic: This screenshot highlights the unusual TCP communication between 192.168.29.249 and 103.162.246.81 on port 1514 (Packets 1, 2, 26, 27). Port 1514 is not a standard service port and this traffic warrants further investigation.

Screenshot Showing TLS (HTTPS) Traffic on Port 443



TLS (HTTPS) Traffic on Port 443:This screenshot shows examples of the TLSv1.2 "Application Data" packets (e.g., Packets 10, 11, 33, 34) observed in the capture. While HTTPS is common, the volume and destinations require further analysis to determine if it's related to normal web browsing or potentially malicious activity.

Screenshot Showing TCP reset traffic:



TCP Reset (RST) Packet: Packet 6 in the capture is a TCP Reset (RST) packet sent from 52.26.51.69:443 to 192.168.29.249:53330. This indicates a TCP connection reset, which could be due to a connection rejection or network issue and needs to be considered in the analysis.