Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

5 distinct ICMP tunneling attempts detected between 192.168.1.4 (source) and 192.168.1.6 (destination) within a 10-second window
High entropy values (5.85–7.65) observed in ICMP payloads, suggesting potential encrypted/obfuscated data transfer
Zero malicious TCP/UDP/ARP packets detected, indicating focused abuse of ICMP protocol
Risk Assessment
Critical Vulnerabilities

ICMP Tunneling (Severity: Critical)
Abnormal payload sizes (70–528 bytes vs standard 32–64 bytes)
Entropy exceeding 6.5 threshold in 4/5 detections (indicates non-random data patterns)
Persistent Attacker Behavior (Severity: High)
Repeating communication pattern between 192.168.1.4 and 192.168.1.6 across packets #18,57,100,125,130
Threat Observations
Technical Findings

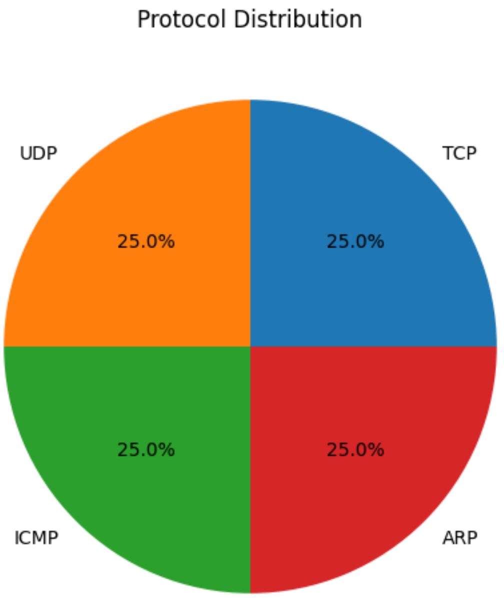
Payload Characteristics
Packet #125: Largest payload (496 bytes) with highest entropy (7.65)
Packet #57: Smallest payload (70 bytes) with lowest entropy (5.85)
Traffic Patterns
Consistent 192.168.1.4 → 192.168.1.6 unidirectional flow
Time clustering between 20:55:00–20:55:08
Protocol Abuse
All malicious packets abused ICMP type/code fields (no ports used)
0% of attacks leveraged TCP/UDP/ARP (per attack_stats)
Recommendations
Immediate Actions

Isolate 192.168.1.4 and 192.168.1.6 for forensic analysis
Implement **ICMP payload inspection** rules targeting:
Payloads >128 bytes
Entropy values >6.0
Repeated ICMP exchanges between same host pairs

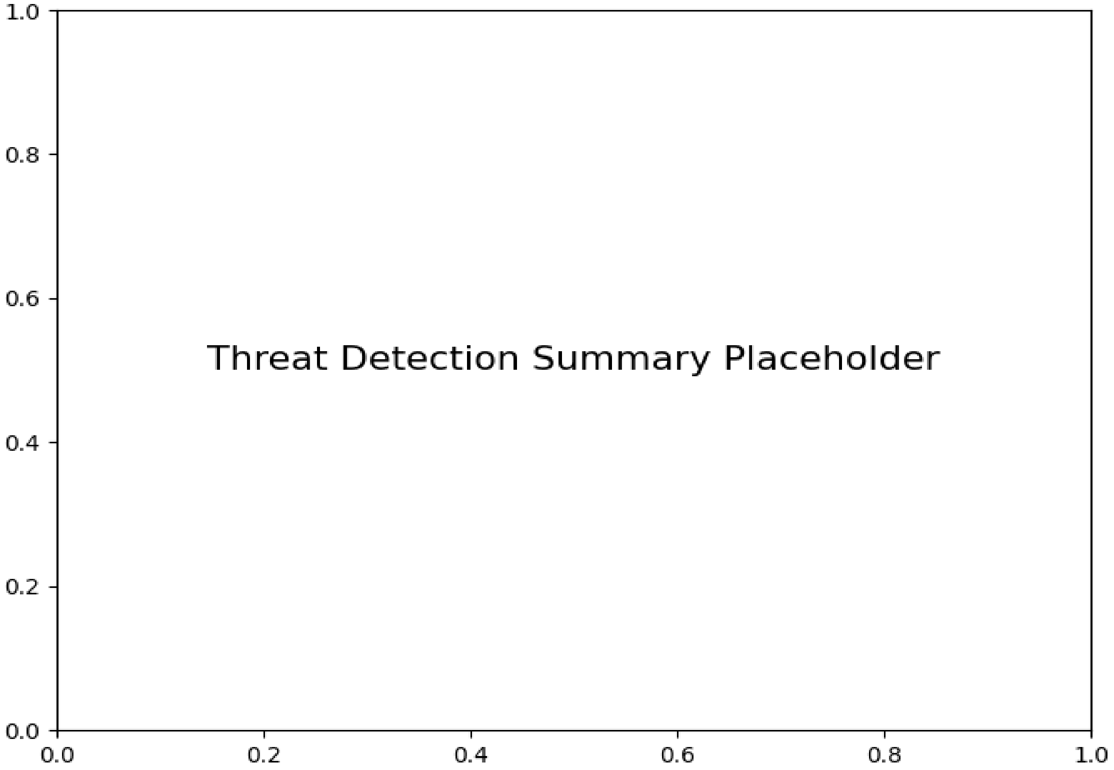
Long-Term Mitigations

Deploy **network segmentation** to restrict ICMP traffic between non-essential devices
Configure **rate limiting** (max 3 ICMP packets/sec per host) to disrupt tunneling
Update IDS/IPS signatures to detect **Shannon entropy anomalies** in ICMP
Conduct **endpoint audits** on 192.168.1.4/.6 for rootkits/C2 tools
Educate staff about ICMP protocol misuse indicators

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential ICMP tunneling detected (byte length=159, entropy=6.78)	1
Potential ICMP tunneling detected (byte length=70, entropy=5.85)	1
Potential ICMP tunneling detected (byte length=233, entropy=7.13)	1
Potential ICMP tunneling detected (byte length=496, entropy=7.65)	1
Potential ICMP tunneling detected (byte length=528, entropy=7.58)	1