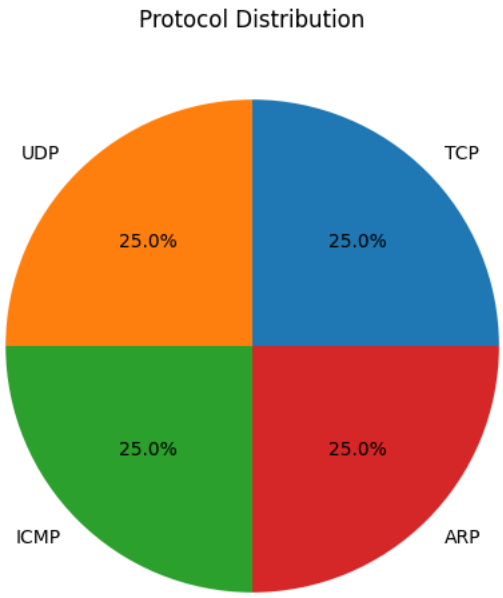
Network Traffic Security Analysis Report

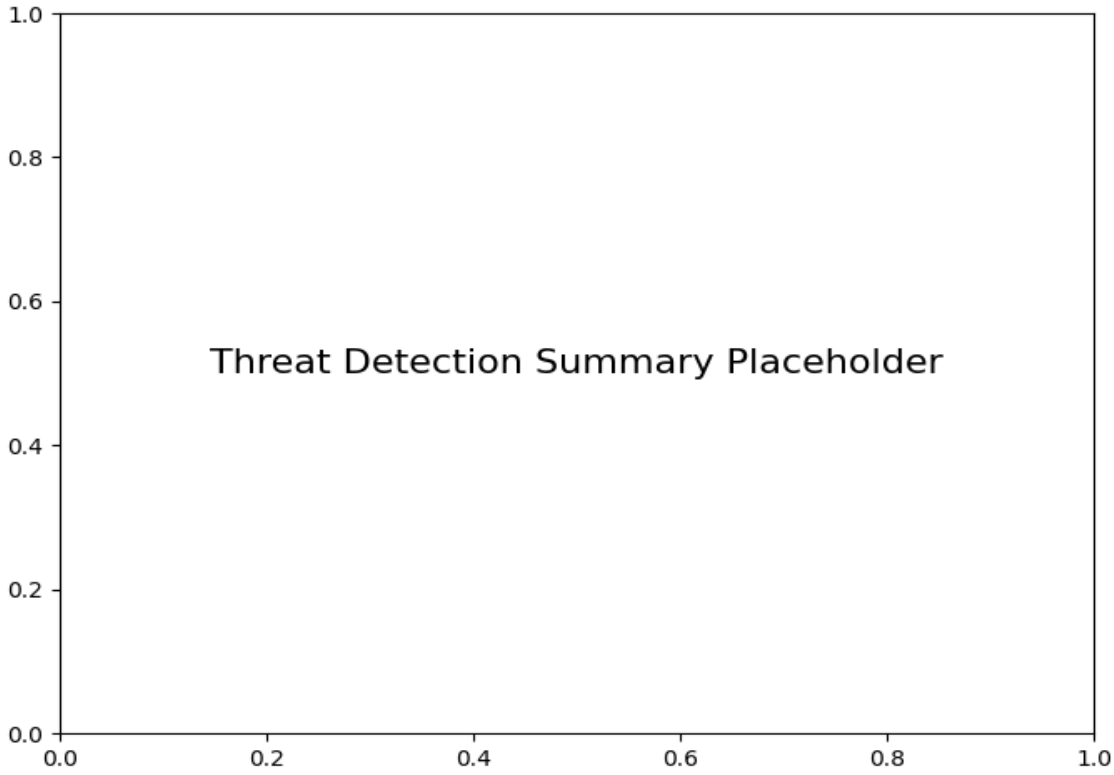
Executive Summary

Network Traffic Analysis Security Report Executive Summary **6 instances of Potential DNS tunneling** detected between internal IPs 192.168.73.148 and 192.168.73.2. No TCP/ICMP/ARP-based attacks observed (0 packets flagged for these protocols). All malicious activity occurred via UDP/DNS protocols within a 7-second timeframe (02:02:58 - 02:03:05). Risk Assessment **Critical Risk**: DNS tunneling attempts indicate **potential data exfiltration or C2 communication**. **High Severity**: Bidirectional DNS traffic between internal hosts (192.168.73.148 ↔ 192.168.73.2) suggests **compromised endpoint communication**. **Medium Risk**: Null port values in DNS traffic may indicate **non-standard protocol implementation**. Threat Observations **DNS Tunneling Patterns**: 5 consecutive malicious packets (159-167) with alternating source/destination IPs Repeating UDP/DNS traffic bursts (Packet 159 → 160 → 165 → 166 → 167) Consistent 1-5 second intervals between malicious packets **Host Analysis**: 192.168.73.148 initiated 3 outbound DNS requests 192.168.73.2 responded with 2 DNS replies **Protocol Anomalies**: 100% of flagged traffic used UDP encapsulation No observed port numbers despite DNS standard using port 53 Recommendations **Immediate Actions**: **Quarantine host 192.168.73.148** for forensic analysis Block all non-essential DNS traffic between internal hosts **Detection Enhancements**: Deploy DNS-specific IDS rules (e.g., domain length checks, entropy analysis) Implement DNS query logging with alert thresholds **Network Hardening**: **Enforce port validation** for all DNS traffic (block null-port transactions) Configure firewall rules to restrict internal DNS resolution to authorized servers **Investigation Priorities**: Review firewall logs for historical communication between 192.168.73.148 and 192.168.73.2 Analyze DNS payload contents from packet captures 159-167

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6