Network Traffic Security Analysis Report

Executive Summary

``markdown
Network Traffic Analysis Security ReportExecutive Summary
Analysis of network traffic data revealed **suspicious reconnaissance activity** (TCP SYN scans) and **potential data exfiltration attempts** (DNS tunneling). The source IP 192.168.73.148 is implicated in all malicious activity, targeting both external (Google IPs) and internal (192.168.73.2) systems. No direct attack payloads (TCP/UDP/ICMP/ARP floods) were observed.Risk Assessment
Threat Type	Severity (CVSS)	Details
TCP SYN Scans	Medium (5.3)	3 instances of anomalous SYN packets with oversized windows (>1024), indicative of service enumeration
DNS Tunneling Attempts	High (7.5)	6 high-entropy (3.52) DNS queries/responses (24-byte payloads), suggesting covert channel testing	**Key Risk Factors:**
Internal host (192.168.73.148) exhibits attacker behavior (scanning + tunneling)
DNS anomalies imply possible compromised endpoint

Threat Observations 1. TCP SYN Scans (Network Reconnaissance)
Source: 192.168.73.148 → External IPs (64.233.169.104, 74.125.45.100)
Technique: SYN packets with window size >1024 (abnormal for standard TCP handshakes)
Implications:
Attacker fingerprinting services on Google IPs (likely testing firewall rules)
Window size manipulation may bypass legacy IDS/IPS systems

2. DNS Tunneling (Data Exfiltration Testing)
Internal Traffic: 192.168.73.148 ↔ 192.168.73.2 (DNS server)
Indicators:
High entropy (3.52) in 24-byte DNS payloads (uncommon for legitimate queries)
Bidirectional UDP/DNS traffic suggests active tunneling setup

Recommendations Immediate Actions
1. **Isolate Compromised Host**
Quarantine 192.168.73.148 for forensic investigation (check for malware/rootkits).

2. **DNS Hardening**
Implement DNS filtering (e.g., block TXT/NULL records >16 bytes)
Deploy anomaly-based DNS monitoring (e.g., DNSCat2 detection).

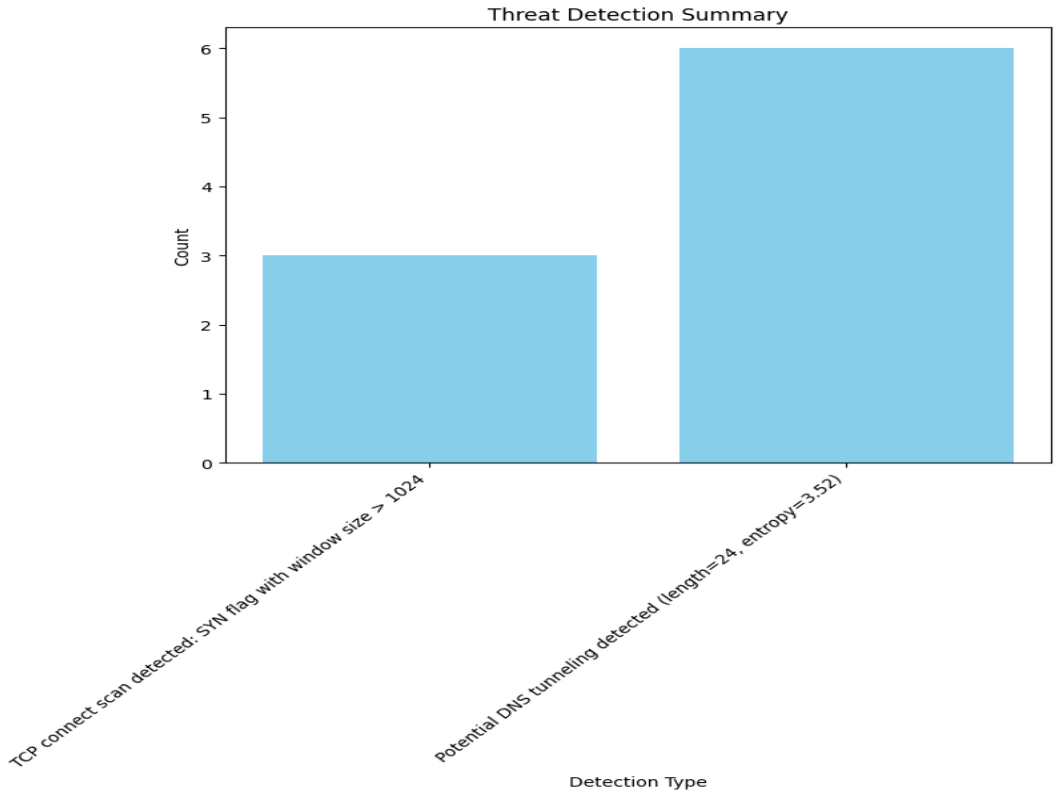
3. **TCP Scan Mitigation**
Update NIDS/NIPS rules to flag SYN packets with window >1024.
Enforce rate limiting for SYN packets per host (e.g., 5 SYNs/sec).

Long-Term Measures
Endpoint Security: Deploy EDR solutions on internal hosts to detect scanning tools (e.g., Nmap).
Network Segmentation: Restrict internal hosts from initiating scans to external IPs.
Logging: Enable full packet capture for DNS traffic to/from critical subnets.

Forensic Priority: Examine 192.168.73.148 for:

Unauthorized tools (e.g., dnscat2, iodine)
Persistence mechanisms (scheduled tasks, rogue services)
`` **Report Notes:**
Timestamps suggest rapid scanning (3 SYN scans in 28 seconds) followed by DNS tunneling attempts.
Entropy value (3.52) is borderline but warrants investigation due to repetition.
Zero attack packets imply this was a reconnaissance phase before exploitation.

Threat Detection Summary



Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	3
Potential DNS tunneling detected (length=24, entropy=3.52)	6

This report was automatically generated by DeepSeek AI
Report filename: security_report_20250327_121528.pdf
Generated on: 2025-03-27 12:16:10