Network Traffic Analysis Report

Executive Summary

Executive Summary of Network Traffic Analysis 1. Overview: - Total Packets: 27550 - Duration: 68.31 seconds - Average Packet Rate: 403.31 packets/second 2. Traffic Distribution: - Top Source IP: 192.168.0.2 (15322 packets, 55.62% of total) - Top Destination IP: 192.168.0.1 (15322 packets, 55.62% of total) - Most Active Port: 389 (22550 occurrences) 3. Protocol Analysis: - Primary Protocol: 6 - Protocol Distribution: 6:25086, 170:284, 37:56 4. Packet Size Statistics: - Average: 262.71 bytes - Median: 60.00 bytes - Std Dev: 493.44 bytes 5. Security Concerns: High traffic concentration to 192.168.0.1, potential DDoS High traffic on unusual ports: 389, 43690, 9587 High TCP retransmission rate: 8.10% 6. Key Recommendations: Activate DDoS mitigation measures and investigate traffic to the most targeted IP. Review and potentially restrict traffic on identified unusual ports. Investigate network congestion or potential packet loss issues. This summary provides a high-level overview of the network traffic captured in the PCAP file. For detailed analysis and visualizations, please refer to the full report.

Detailed Analysis

Protocol Distribution:

- 6: 25086 packets (91.06%)
- 170: 284 packets (1.03%)
- 37: 56 packets (0.20%)
- 0: 53 packets (0.19%)
- 115: 51 packets (0.19%)

Top 5 Source IP Addresses:

- 192.168.0.2: 15322 packets (55.62%)
- 192.168.0.1: 8202 packets (29.77%)
- 170.170.170.170: 359 packets (1.30%)
- 192.168.0.37: 61 packets (0.22%)
- 192.168.37.115: 53 packets (0.19%)

Top 5 Destination IP Addresses:

- 192.168.0.1: 15322 packets (55.62%)
- 192.168.0.2: 8144 packets (29.56%)
- 170.170.170.170: 467 packets (1.70%)
- 192.37.115.0: 51 packets (0.19%)
- 192.168.37.115: 50 packets (0.18%)

Top 10 Ports:

- Port 389: 22550 packets (81.85%)
- Port 43690: 609 packets (2.21%)
- Port 9587: 103 packets (0.37%)
- Port 29440: 94 packets (0.34%)
- Port 0: 83 packets (0.30%)
- Port 133: 79 packets (0.29%)
- Port 293: 57 packets (0.21%)
- Port 3361: 54 packets (0.20%)
- Port 4539: 54 packets (0.20%)
- Port 1755: 54 packets (0.20%)

Packet Size Statistics:

- Average: 262.71 bytes

- Median: 60.00 bytes
- Standard Deviation: 493.44 bytes

TCP Flags Distribution:

- PA: 6958 (28.87%)
- A: 6176 (25.62%)
- FA: 2887 (11.98%)
- S: 2511 (10.42%)
- SA: 2369 (9.83%)
- R: 1733 (7.19%)
- SPUC: 603 (2.50%)
- FPA: 118 (0.49%)
- N: 67 (0.28%)
- FSAUEN: 54 (0.22%)
- FRU: 51 (0.21%)
- PAN: 40 (0.17%)
- AN: 30 (0.12%)
- FAN: 22 (0.09%)
- : 22 (0.09%)
- SAN: 19 (0.08%)
- FUEN: 17 (0.07%)
- SN: 15 (0.06%)
- RN: 12 (0.05%)
- AU: 12 (0.05%)
- PAU: 9 (0.04%)
- PAE: 9 (0.04%)
- SAE: 7 (0.03%)
- SPA: 6 (0.02%)
- FAE: 6 (0.02%)
- RPA: 6 (0.02%)
- FSN: 6 (0.02%)
- FAU: 6 (0.02%)
- FSPN: 6 (0.02%)
- FSAUE: 6 (0.02%)
- FSUE: 5 (0.02%)
- SUE: 5 (0.02%)

- SRAE: 5 (0.02%)
- AE: 5 (0.02%)
- FSA: 5 (0.02%)
- F: 5 (0.02%)
- AC: 5 (0.02%)
- FAUE: 5 (0.02%)
- PAC: 5 (0.02%)
- SRPAUEC: 5 (0.02%)
- FSRPAUECN: 5 (0.02%)
- RAUCN: 4 (0.02%)
- FSPUE: 4 (0.02%)
- RA: 4 (0.02%)
- FUE: 4 (0.02%)
- RE: 4 (0.02%)
- SC: 4 (0.02%)
- FPUE: 4 (0.02%)
- SAC: 4 (0.02%)
- FSE: 4 (0.02%)
- FSUEN: 4 (0.02%)
- SE: 4 (0.02%)
- RAUE: 4 (0.02%)
- FSRAE: 4 (0.02%)
- SPAE: 3 (0.01%)
- FRPUE: 3 (0.01%)
- FAC: 3 (0.01%)
- FSRAUE: 3 (0.01%)
- FSAE: 3 (0.01%)
- PU: 3 (0.01%)
- P: 3 (0.01%)
- SRAU: 3 (0.01%)
- SR: 3 (0.01%)
- RU: 3 (0.01%)
- SPN: 3 (0.01%)
- SAU: 3 (0.01%)
- FRUEN: 3 (0.01%)

- FPAE: 3 (0.01%)
- RP: 3 (0.01%)
- FRAU: 3 (0.01%)
- FPAU: 2 (0.01%)
- RUE: 2 (0.01%)
- SPAUE: 2 (0.01%)
- PUE: 2 (0.01%)
- SAUE: 2 (0.01%)
- SPE: 2 (0.01%)
- SRPUE: 2 (0.01%)
- FE: 2 (0.01%)
- FREC: 2 (0.01%)
- FPEC: 2 (0.01%)
- FRPE: 2 (0.01%)
- FSPAUEC: 2 (0.01%)
- SPC: 2 (0.01%)
- SRPE: 2 (0.01%)
- FSRPUE: 2 (0.01%)
- FSRC: 2 (0.01%)
- SP: 2 (0.01%)
- FSRPE: 2 (0.01%)
- RAE: 2 (0.01%)
- FSEC: 2 (0.01%)
- RUC: 2 (0.01%)
- SRE: 2 (0.01%)
- FAUEC: 2 (0.01%)
- UEC: 2 (0.01%)
- FS: 2 (0.01%)
- RC: 2 (0.01%)
- FRUEC: 2 (0.01%)
- SRPAE: 2 (0.01%)
- FRPUC: 2 (0.01%)
- FSAC: 2 (0.01%)
- RPUE: 2 (0.01%)
- FSRPC: 2 (0.01%)

- PE: 2 (0.01%)
- FSRAU: 2 (0.01%)
- PAUE: 2 (0.01%)
- SRAUE: 2 (0.01%)
- SRUE: 2 (0.01%)
- FSAU: 2 (0.01%)
- SPUE: 2 (0.01%)
- FC: 2 (0.01%)
- SRPUC: 2 (0.01%)
- PAEC: 1 (0.00%)
- FSRPA: 1 (0.00%)
- FRAUCN: 1 (0.00%)
- FSR: 1 (0.00%)
- RPUC: 1 (0.00%)
- FSPAEN: 1 (0.00%)
- FSPC: 1 (0.00%)
- FRPC: 1 (0.00%)
- FPC: 1 (0.00%)
- FPAN: 1 (0.00%)
- FSPAUN: 1 (0.00%)
- RAEC: 1 (0.00%)
- RAUN: 1 (0.00%)
- RPE: 1 (0.00%)
- AUEC: 1 (0.00%)
- FSRUC: 1 (0.00%)
- RPAUEC: 1 (0.00%)
- SRPAU: 1 (0.00%)
- SRPN: 1 (0.00%)
- SPAU: 1 (0.00%)
- RPC: 1 (0.00%)
- FR: 1 (0.00%)
- FSRPAEC: 1 (0.00%)
- AUE: 1 (0.00%)
- RCN: 1 (0.00%)
- FRAUE: 1 (0.00%)

- FSRPAC: 1 (0.00%)
- RAC: 1 (0.00%)
- FPE: 1 (0.00%)
- AEC: 1 (0.00%)
- SU: 1 (0.00%)
- FRPA: 1 (0.00%)
- SPUEC: 1 (0.00%)
- FSRUE: 1 (0.00%)
- FRPECN: 1 (0.00%)
- RPAEC: 1 (0.00%)
- FRE: 1 (0.00%)
- FSPU: 1 (0.00%)
- SPAN: 1 (0.00%)
- FPUC: 1 (0.00%)
- FRAUC: 1 (0.00%)
- UN: 1 (0.00%)
- SRPUEN: 1 (0.00%)
- RAEN: 1 (0.00%)
- FUCN: 1 (0.00%)
- FSRAC: 1 (0.00%)
- FSPUC: 1 (0.00%)
- FSPAUCN: 1 (0.00%)
- SRU: 1 (0.00%)
- PUC: 1 (0.00%)
- FSPAU: 1 (0.00%)
- FRPAUC: 1 (0.00%)
- RPAUE: 1 (0.00%)
- FRUN: 1 (0.00%)
- FSPE: 1 (0.00%)
- FRAEC: 1 (0.00%)
- FSRE: 1 (0.00%)
- SEC: 1 (0.00%)
- RAN: 1 (0.00%)
- SRPUEC: 1 (0.00%)
- U: 1 (0.00%)

- FSPAUC: 1 (0.00%)
- FRAE: 1 (0.00%)
- SUEN: 1 (0.00%)
- FSRPUN: 1 (0.00%)
- FSRAECN: 1 (0.00%)
- FSRPU: 1 (0.00%)
- RAUEC: 1 (0.00%)
- SPAUEC: 1 (0.00%)
- RAU: 1 (0.00%)
- SRAUC: 1 (0.00%)
- FEC: 1 (0.00%)
- FRPAECN: 1 (0.00%)
- SPAUC: 1 (0.00%)
- E: 1 (0.00%)
- SRAUEC: 1 (0.00%)
- RPAUC: 1 (0.00%)
- FPAECN: 1 (0.00%)
- FP: 1 (0.00%)
- FSRPUEC: 1 (0.00%)
- SRA: 1 (0.00%)
- FRA: 1 (0.00%)
- FPAUE: 1 (0.00%)
- FSRA: 1 (0.00%)
- PC: 1 (0.00%)

Traffic Distribution by Hour:

- Hour 9: 25992 packets (94.34%)

Top 5 Conversations:

- 192.168.0.2 <-> 192.168.0.1: 14166 packets (51.42%)
- 192.168.0.1 <-> 192.168.0.2: 7535 packets (27.35%)
- 170.170.170.170 <-> 170.170.170.170: 359 packets (1.30%)
- 192.168.0.37 <-> 115.0.0.1: 36 packets (0.13%)
- 115.0.0.2 <-> 192.168.0.1: 36 packets (0.13%)

Average TTL: 79.48

Average TCP Window Size: 24891.44 bytes

ICMP Type Distribution:

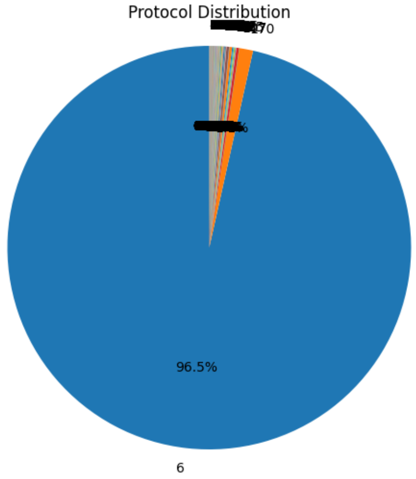
- Type 1: 1 (100.00%)

SSL/TLS Version Distribution:

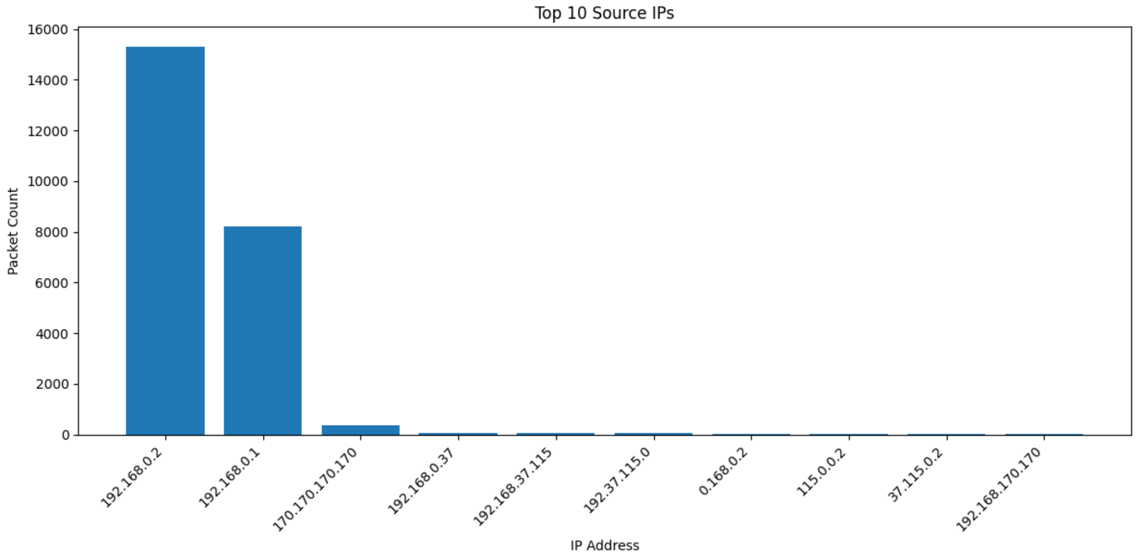
- TLSv1.2: 1 (100.00%)

Visual Analysis

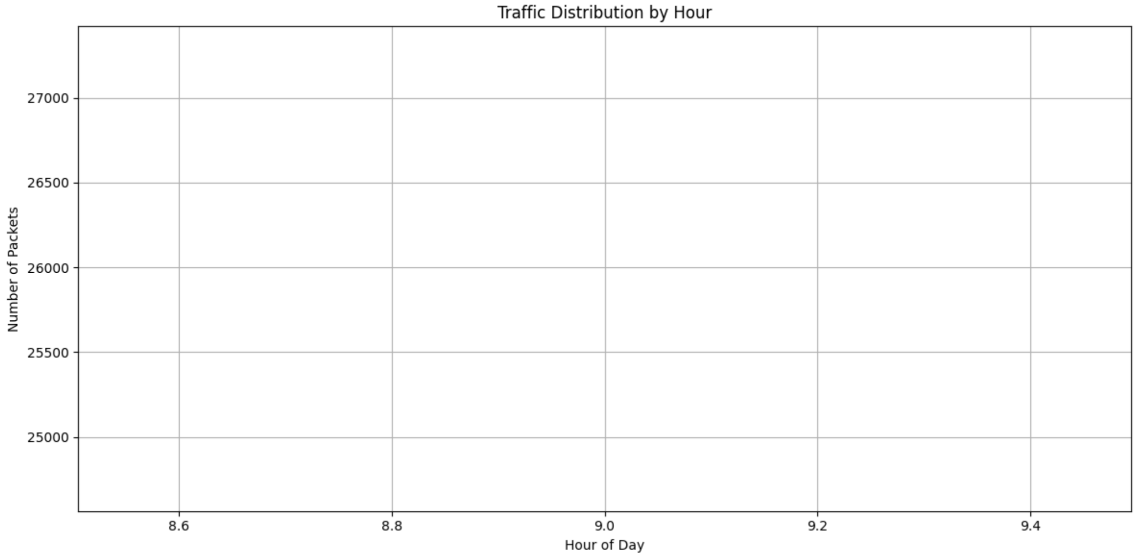
Protocol Distribution



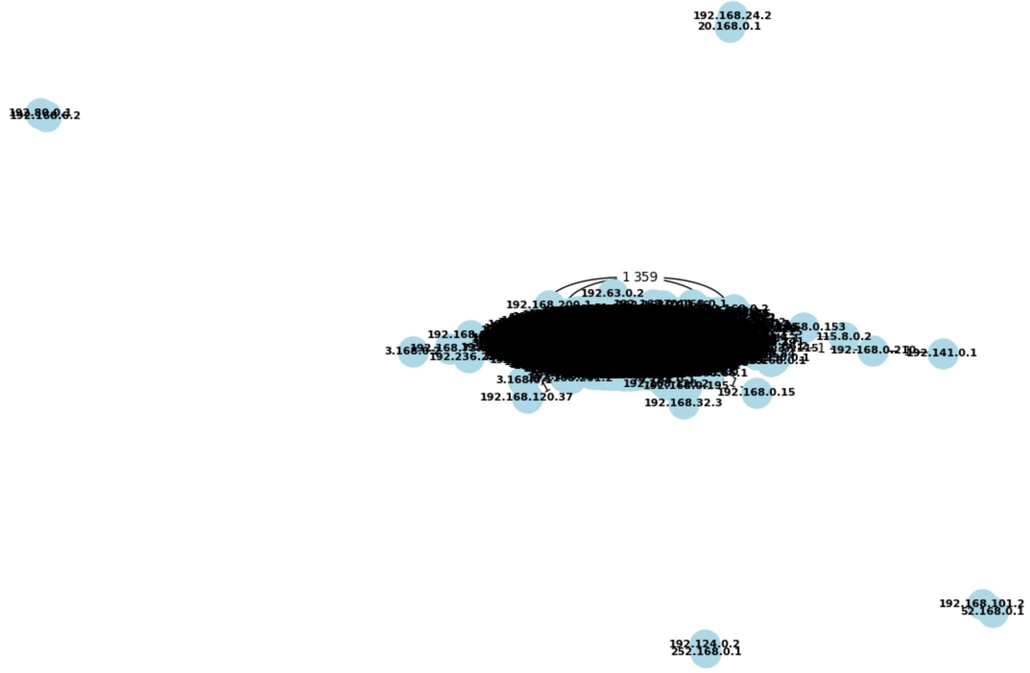
Top 10 Source IPs



Traffic Distribution by Hour



Network Communication Graph



Security Concerns

- High traffic concentration to 192.168.0.1, potential DDoS
- High traffic on unusual ports: 389, 43690, 9587
- High TCP retransmission rate: 8.10%

Recommendations

- Activate DDoS mitigation measures and investigate traffic to the most targeted IP.
- Review and potentially restrict traffic on identified unusual ports.
- Investigate network congestion or potential packet loss issues.