Detailed PCAP Analysis Report

This report provides a detailed analysis of the captured network traffic. It includes protocol usage, communication patterns, port distribution, and potential security concerns identified in the packet capture.

Summary

Total Packets Captured: 1745

Protocol Analysis

Protocol	Count
IP	1743
TCP	581
UDP	1162
ICMP	0
ARP	2
Other	0

The table above shows the distribution of protocols. High TCP/UDP traffic is common in normal networks. Significant ICMP or ARP traffic may suggest scanning or ARP spoofing attempts.

Top Source IPs

IP	Count
142.250.71.100	725
192.168.226.129	574
142.250.192.3	98
142.250.71.106	51
142.250.194.3	41

The table above shows which IP addresses communicated the most. Heavy talkers may represent servers, scanners, or malicious hosts depending on context.

Top Destination IPs

IP	Count
192.168.226.129	1169
142.250.71.100	183
142.250.192.3	56
142.250.194.3	47
142.250.71.106	40

The table above shows which IP addresses communicated the most. Heavy talkers may represent servers, scanners, or malicious hosts depending on context.

Top Ports

Port	Count
443	1585
47033	879
80	106
43354	105
53	52
33998	41
39155	38
59674	38
52562	37
55596	34

The ports above indicate which services were most frequently accessed. Common ports (80/443) usually represent web traffic, while unusual or high ports could indicate custom applications or scanning activity.

Potential Security Findings

No obvious suspicious activity was detected in this capture.

Conclusion

This concludes the automated analysis of the PCAP file. For deeper insights, further manual review with Wireshark or intrusion detection systems (IDS) is recommended.