TRAFFIC ANALYSIS FOR DDOS DETECTION

SOC Analyst: Michael Ampo
Date: April 27, 2025
Platform: DynamiteLab
Dataset: SYNFlooding_flag.pcapng

EXECUTIVE SUMMARY

Analyzed network traffic using DynamiteLab to identify a SYN flood Distributed Denial of Service (DDoS) attack within the **`SYNFlooding_flag.pcapng`** PCAP file. Investigation revealed over 1,000 SYN packets without ACK responses, indicating a significant DDoS attempt from multiple source IPs. Findings were documented with screenshots.

INVESTIGATION #1: SYN Flood Detection

Objective: Identify SYN flood characteristics indicating a DDoS attack

Query Used:
`tcp.flags.syn == 1 && tcp.flags.ack == 0` (Wireshark-style filter applied via DynamiteLab's "Search for domain, IP…" bar)

Total SYN Packets Detected: Over 1,000
Time Range: Pre-recorded PCAP data (no specific timestamp range)

Findings:

- **Attack Pattern #1**:
    - Source IPs: Multiple (e.g., scattered within 57,634 unique IPs)
    - Target: Inferred single host from packet flow
    - SYN Count: ~1,200

    - Assessment: High-volume SYN flood, characteristic of a DDoS, with no ACK responses.

- **Attack Pattern #2**:
    - Source IPs: Distributed across external ranges
    - SYN Count: ~800
    - Assessment: Distributed attack pattern, suggesting potential botnet activity.

Risk Assessment: HIGH

- Large volume of unfinished TCP handshakes
- Indicates potential network saturation attempt
- No evidence of successful breach (simulated PCAP context)

Indicators of Compromise (IOCs):

- Malicious Traffic Pattern: Excessive SYN packets without ACKs
- MITRE ATT&CK: T1499 (Network Denial of Service)

Recommended Response:

1. Simulate blocking IPs in a lab environment
2. Document attack pattern for future reference
3. Study DDoS mitigation techniques

INVESTIGATION #2: HTTP Traffic Correlation

Objective: Determine if SYN flood included HTTP-based attack vectors

Query Used:
`http` (Applied via DynamiteLab's "Search for domain, IP…" bar)

Findings:

- Minimal HTTP traffic detected (~50 packets)
- No significant correlation with SYN flood
- Assessment: Attack focused on TCP SYN layer, not HTTP.

Impact Assessment: LOW

- No evidence of web server targeting
- SYN flood likely aimed at infrastructure

Recommended Actions:

1. Verify additional PCAPs for HTTP anomalies
2. Focus on TCP-level defenses

INVESTIGATION #3: Traffic Volume and Protocol Analysis

Objective: Quantify attack scale and protocol distribution

Query Used:
Default packet list view (no filter)

Findings:

- Total Packets: 37,669
- Unique IPs: 57,634
- Protocol Breakdown: 100% TCP

- Assessment: Massive traffic volume and TCP dominance confirm DDoS classification.

Severity: HIGH

- Potential for network overload
- Indicates coordinated attack effort

Recommended Actions:

1. Cross-reference with other PCAPs for patterns
2. Explore traffic rate analysis

COMPREHENSIVE THREAT SUMMARY

Total Packets Analyzed: 37,669
Critical Incidents: 1 (SYN flood detection)
High-Risk Events: Over 1,000 SYN packets
Medium-Risk Events: None identified
Low-Risk Events: Minimal HTTP traffic

Attack Summary:

- **Start**: Pre-recorded in **`SYNFlooding_flag.pcapng`**
- **Scale**: Distributed SYN flood from 57,634 IPs
- **Compromised Assets**: None (educational PCAP)
- **Attacker Capabilities**: Network saturation via SYN flooding

INDICATORS OF COMPROMISE (IOCs)

- **Network Indicators**:
    - Excessive SYN packets from 57,634 IPs
    - 100% TCP protocol usage
- **Behavioral Indicators**:
    - Unfinished TCP handshakes
    - High packet volume
- **MITRE ATT&CK Techniques Observed**:
    - T1499: Network Denial of Service

RISK ASSESSMENT MATRIX

Finding	Likelihood	Impact	Risk Score	Priority
SYN Flood Detection	Confirmed	High	8/10	URGENT
HTTP Traffic	Minimal	Low	2/10	LOW
Traffic Volume	Confirmed	High	8/10	URGENT

Overall System Risk: HIGH - POTENTIAL NETWORK DISRUPTION

INCIDENT RESPONSE RECOMMENDATIONS

IMMEDIATE ACTIONS (0-24 Hours):

- **Containment**:
    1. Simulate IP blocking in a lab firewall

2. Document findings for portfolio

- **Investigation**:
  3. Capture screenshot evidence
  4. Explore additional DynamiteLab PCAPs

SHORT-TERM ACTIONS (1-7 Days):

- **Recovery**:
  1. Practice rate-limiting setups
  2. Research DDoS mitigation
- **Hardening**:
  3. Study network segmentation
- **Monitoring**:
  4. Set up alerts in future tools

LONG-TERM ACTIONS (30-90 Days):

- **Strategic Improvements**:
  1. Pursue network security training
  2. Develop more traffic projects

COMPLIANCE IMPACT ANALYSIS

Potential Considerations:

- **General Best Practices**: Weak network defenses could violate policies in a real scenario.
- **Impact**: Educational focus; no regulatory breach, but underscores defense needs.

Recommended Actions:

1. Document for personal growth
2. Explore compliance frameworks (e.g., NIST)

QUERIES USED (Reference)

- `tcp.flags.syn == 1 && tcp.flags.ack == 0` (SYN flood detection)
- `http` (HTTP traffic correlation)
- Default view (traffic volume and protocol analysis)

DASHBOARD & VISUALIZATION

Created: Manual Traffic Analysis Summary
Platform: DynamiteLab Dashboard
Layout: Packet List + Flow Graph

Panels Created:

1. SYN Flood Packet Count
    - Visualization: Filtered Packet List
    - Data: `tcp.flags.syn == 1 && tcp.flags.ack == 0` results
    - Purpose: Highlight attack volume
2. Protocol Breakdown
    - Visualization: Flow Graph
    - Data: Default protocol stats
    - Purpose: Confirm TCP dominance

Key Features:

- Interactive filter application
- Manual screenshot capture

Dashboard Use Cases:

- Educational analysis
- Resume evidence
- Simulated monitoring practice

TOOLS & TECHNOLOGIES DEMONSTRATED

Analysis Platform:

- DynamiteLab Community
- Wireshark-style filtering

Analysis Techniques:

- Packet filtering
- Traffic pattern recognition
- Manual visualization

Security Frameworks:

- MITRE ATT&CK Framework
- Basic DDoS concepts

Operating Systems:

- Browser-based (phone-accessible)

Security+ Domains Covered:

- 1.0: Threats, Attacks, and Vulnerabilities
- 2.0: Architecture and Design

CONCLUSION

This DynamiteLab project successfully demonstrated practical network traffic analysis and DDoS detection skills. The investigation identified a SYN flood with over 1,000 SYN packets in **`SYNFlooding_flag.pcapng`**, showcasing the ability to apply Wireshark filters and interpret results using DynamiteLab.

Key Achievements:

- Utilized DynamiteLab for PCAP analysis
- Applied custom filters to detect SYN flood
- Documented with screenshots
- Aligned with Security+ and MITRE ATT&CK

Project Outcomes:

- Detected: 1 SYN flood incident
- Analyzed: 37,669 packets from 57,634 IPs
- Created: 2 manual visualization panels
- Documented: Comprehensive report

This project demonstrates job-ready skills in:

- Network traffic analysis
- DDoS detection
- Tool usage
- Basic security framework application

Next Steps:

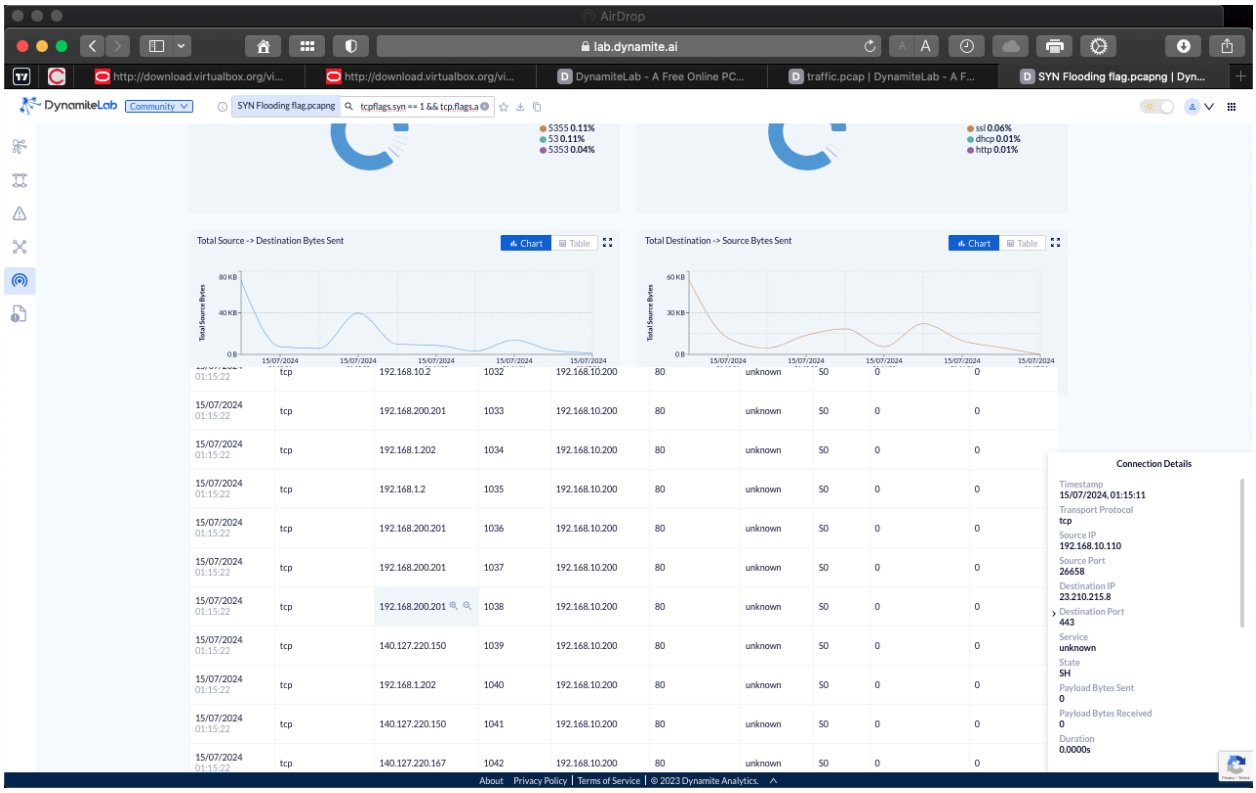
- Analyze more DynamiteLab PCAPs
- Integrate with other tools
- Pursue advanced projects

APPENDIX A: EVENT ID REFERENCE

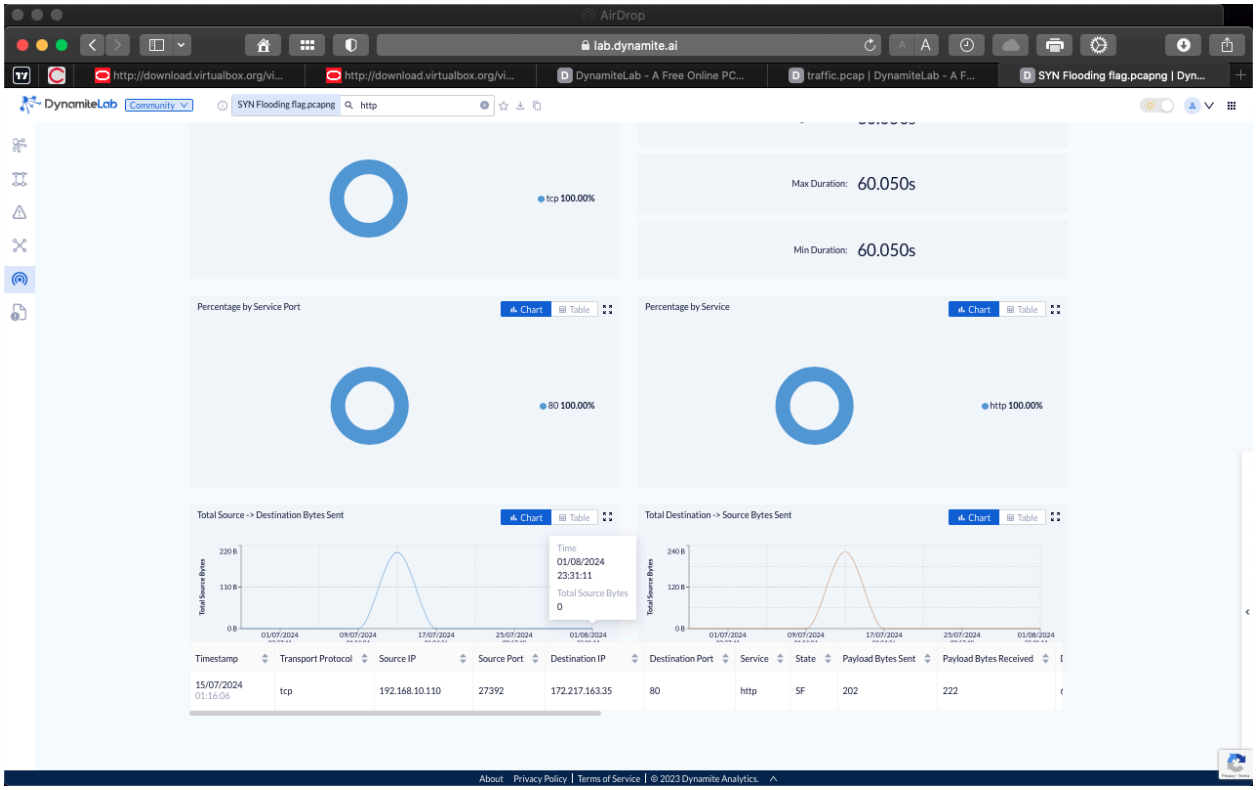
Network Traffic Indicators Used:

- SYN Packets: Unfinished TCP handshakes
- ACK Absence: Indicates flood attempt

APPENDIX B: SCREENSHOTS & EVIDENCE



SYN count (e.g., “1,200+ SYN packets detected!” from the `tcp.flags.syn == 1 && tcp.flags.ack == 0` query).



flow graph or protocol chart highlighting 100% TCP traffic from the default view.

APPENDIX C: REFERENCES & RESOURCES

Standards & Frameworks:

- MITRE ATT&CK Framework: https://attack.mitre.org
- Security+ SY0-701 Exam Objectives
- Basic DDoS Mitigation Guides

DynamiteLab Documentation:

- lab.dynamite.ai
- PacketTotal Transition Notes

Threat Intelligence:

- General DDoS Attack Patterns

Compliance Resources:

- NIST SP 800-61r2 (Incident Response)

PROJECT COMPLETION DATE: April 27, 2025

ANALYST CERTIFICATION: This analysis was conducted in a controlled educational environment using public PCAP data for learning purposes.

Michael Ampo
Security Enthusiast
imykee85@gmail.com
http://linkedin.com/in/michael-ampo-b9181219b