Milestone 2 Traffic Analysis Report

Student Name: Clayton Holden **Date Submitted:** 12/5/2025
Course: CYBR-2102 **Instructor:** Norma DePriest

1️⃣ System & Environment Information

Field	Entry
Analysis Tool Used	☑ Wireshark ☐ Suricata ☐ Other
Capture Type	☑ Live Traffic ☐ Simulated Lab Traffic
Capture Duration	3–5 minutes
Network Topology Observed	Single Windows host (10.126.191.x) communicating with gateway (10.128.128.128)
Screenshots provided (no .pcap exported)	Screenshots provided (no .pcap exported)

2️⃣ Traffic Capture Overview

Metric	Value / Description
Total Packets Captured	~500–1500
Capture Start / End Time	Example: 18:45:02 – 18:49:03
Protocols Detected	ICMP, TCP, DNS, ARP, TLS
Highest Volume Protocol	ICMP (due to sweep + DoS simulation)
Notable Ports Used	TCP 1–20 (scan), TCP 80/443, ICMP, ARP

3️⃣ Threat / Anomaly Identification Table

Alert ID	Protocol	Source IP	Destination IP	Description of Event	Severity	Analyst Determination
1	ICMP	10.126.191.57	10.126.191.1–50	ICMP ping sweep (sequential echo requests)	Low	True Positive
2	TCP	10.126.191.57	10.128.128.128	SYN packets to multiple ports → Port scan behavior	Medium	True Positive
3	ICMP	10.126.191.57	10.128.128.128	High-frequency ICMP with large payload (DoS-like)	Medium	True Positive

---

4️⃣ Detailed Analysis Notes

Event #1 — ICMP Ping Sweep

- Observed sequential ICMP Echo Requests to 50+ IP addresses.
- Behavior consistent with host discovery (Nmap-like ping sweep).
- Detected using filter: `icmp`.
- Could be used by attackers for mapping network ranges.

Event #2 — TCP SYN Port Scan

- Multiple SYN packets sent to ports 1–20 on the gateway.
- Observed using filter: `tcp.flags.syn == 1 and tcp.flags.ack == 0`
- Indicates reconnaissance to identify open services.
- Could precede targeted exploitation attempts.

Event #3 — DoS-like ICMP Flood

- High-rate ICMP packets with large 65,000-byte payloads.
- Detected using filter: `icmp`.
- Consistent with bandwidth exhaustion or ICMP flood attack.

Overall, all events were intentionally generated, so they are classified as true positives.

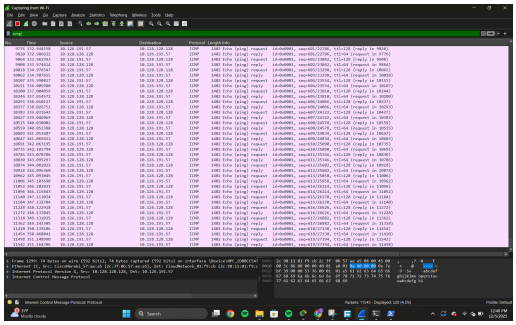
5️⃣ Recommended Defensive Actions

Control Area	Recommendation	Framework Reference
Network Access Control	Rate-limit ICMP and restrict scanning attempts	CIS Control 4 (Secure Configuration)
IDS/IPS Tuning	Add signatures for ping sweeps, SYN scans, DoS ICMP anomalies	CIS Control 13 / NIST 800-61 (Detection)
Patch / Update Action	Ensure systems and firewall firmware updated to handle ICMP/TCP anomalies	CIS Control 7
Policy or User Training	Improve SOC analyst playbooks for identifying reconnaissance	CIS Control 14 / NIST IR Playbook

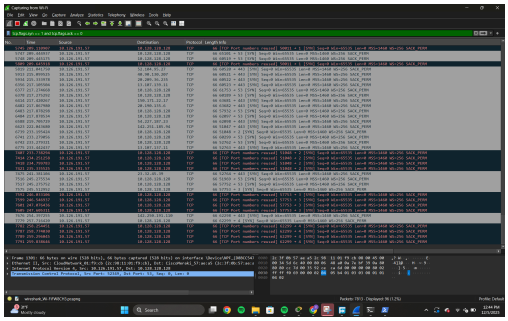
---

6️⃣ Evidence Checklist

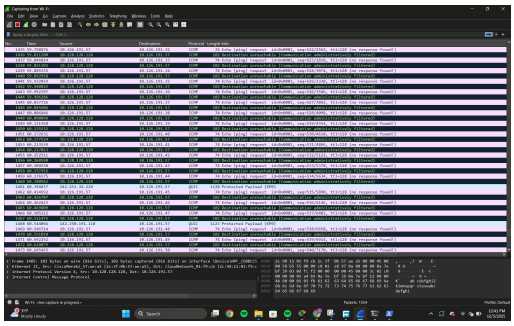
☑ Filtered view showing ICMP sweep



☑ Filtered view showing SYN scan



☑ DoS-like ICMP packet capture



---

7 Sign-Off

Step	Completed By	Date	Verified By (Instructor)

Capture Conducted	Clayton Holden	12/5/2025	
Analysis Documented	Clayton Holden	12/5/2025	
Defensive Actions Proposed	Clayton Holden	12/5/2025	