Alexander Ratcliffe Cell: 703-498-7477

Security Assesment

1. Executive Summary

This security assessment focused on analyzing a network packet capture to investigate unusual traffic patterns targeting the internal IP address **10.10.10.10**. Using Wireshark, the analysis uncovered several critical indicators of potentially malicious activity, including a high volume of SYN packets from multiple external IP addresses, suspiciously rapid packet timing, and malformed packet structures. These findings suggest possible reconnaissance behavior, a SYN flood Denial of Service (DoS) attempt, or a prelude to an exploitation campaign.
The traffic pattern revealed signs of automated scanning and probing, potentially exposing vulnerabilities in the network infrastructure. Immediate and long-term mitigation strategies were recommended to enhance the organization's resilience against similar threats in the future.

---

2. Scope of Assessment

Clearly define what was assessed and why.

- **Date(s) of Assessment:** March 2025
- **Assessment Type:** ☑ Internal ☐ External ☐ Web App ☐ Cloud ☐ Wireless
- **Environment Assessed:**
    - ☐ Workstations
    - ☑ Servers
    - ☑ Firewalls / Routers
    - ☐ Cloud Resources (e.g., AWS)
    - ☐ Applications / Endpoints
- **Assets in Scope:**
    - IP Range(s): 10.10.10.0/24
    - Hostnames: Not explicitly identified; focused on internal IP 10.10.10.10
    - URLs / Cloud Services: N/A (local/internal traffic only)

- **Objective of the Assessment:**
  To investigate abnormal traffic behavior targeting internal IP 10.10.10.10, identify potential security gaps, and analyze evidence of possible reconnaissance or Denial of Service (DoS) activity. The goal was to simulate attacker tactics and assess the organization's network monitoring and threat detection readiness.

---

3. Tools and Methodology

Detail the tools, scripts, and frameworks used.

Tool / Framework	Purpose
Wireshark	Packet capture and deep traffic analysis; used to identify SYN flood patterns, malformed packets, and suspicious timing behaviors targeting internal assets.
Nmap	Port scanning and network discovery to correlate observed traffic with open services and identify potential exposure.
MITRE ATT&CK	Used to map observed behaviors (e.g., reconnaissance, exploitation) to known adversary TTPs for clearer threat context.
Manual Inspection	Configuration and log review to verify anomalous traffic behavior, correlate events, and confirm indicators of compromise.

---

4. Key Findings

Summarize your most important findings and their impact.

Severity	Vulnerability / Misconfiguration	Affected Asset	CVE / Reference	Risk Description
High	SYN Flood / DoS Behavior	10.10.10.10	N/A	Repeated SYN packets from multiple external IPs could overwhelm the target system, causing service disruption.
High	Malformed Packet Patterns	10.10.10.10	N/A	Abnormal TCP flags and packet headers suggest reconnaissance or exploitation attempts, possibly bypassing security tools.
Medium	Unrestricted Port Exposure	10.10.10.10	N/A	Port scanning behavior indicates that multiple ports were accessible, increasing the attack surface for potential exploits.

---

5. Risk Mapping & Controls

Map findings to known cybersecurity frameworks.

Framework	Control Reference	Description
NIST 800-53 Rev 5	AC-17, SC-7, SC-13	Remote Access Controls, Boundary Protection, Cryptographic Protection to safeguard network traffic and prevent external scanning or DoS activity.
CIS Controls v8	Control 4, 7, 8, 13	Secure Configuration of Enterprise Assets (4), Continuous Vulnerability

		Management (7), Audit Log Management (8), and Network Monitoring & Defense (13).
MITRE ATT&CK	T1046, T1499, T1040	T1046 (Network Service Scanning), T1499 (Endpoint Denial of Service), T1040 (Network Sniffing). Mapped based on observed behaviors and traffic patterns.

---

6. Mitigation Recommendations

Immediate Actions

- **Implement Rate Limiting:** Throttle excessive incoming connection requests to reduce exposure to SYN flood attacks.
- **Block Malicious IPs and Traffic Patterns:** Use behavior-based detection systems to identify and block abnormal traffic rather than relying solely on IP blacklists.
- **Close Unused Ports:** Perform a port audit and disable all non-essential services to reduce the attack surface.
- **Enable Strict Packet Filtering:** Configure firewalls to detect and drop malformed packets and unusual TCP flag combinations.

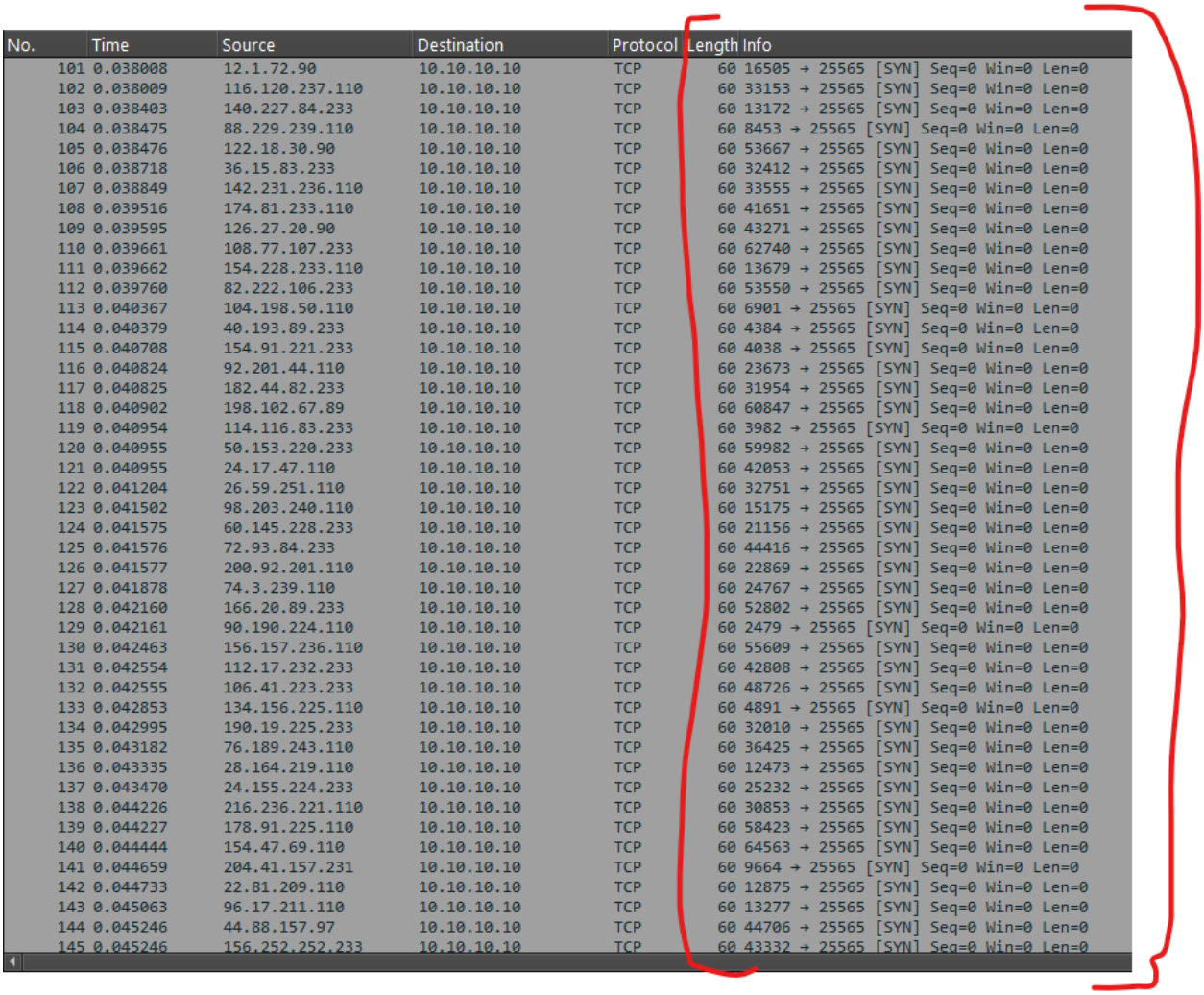
Long-Term Security Measures

- **Deploy an Intrusion Prevention System (IPS):** Use an IPS to actively detect and block port scans and malformed packet-based probes.
- **Enhance Network Monitoring and Alerting:** Utilize tools like Suricata or Snort alongside Wireshark for real-time anomaly detection and automated alerting.
- **Conduct Regular Internal Traffic Analysis:** Periodically perform packet capture and flow analysis to detect early indicators of reconnaissance or DoS behavior.
- **Implement Network Segmentation:** Isolate critical systems (e.g., 10.10.10.10) behind stricter internal firewalls to prevent lateral movement if compromised.
- **Develop & Test Incident Response Playbooks:** Establish clear steps for identifying, containing, and responding to similar network-based attacks in the future.

Alexander Ratcliffe Cell: 703-498-7477

7. Screenshots and Evidence

- **SYN Packet Counts**: Multiple IP addresses repeatedly sent SYN packets to 10.10.10.10.



No.	Time	Source	Destination	Protocol	Length	Info
101	0.038008	12.1.72.90	10.10.10.10	TCP	60	16505 → 25565 [SYN] Seq=0 Win=0 Len=0
102	0.038009	116.120.237.110	10.10.10.10	TCP	60	33153 → 25565 [SYN] Seq=0 Win=0 Len=0
103	0.038403	140.227.84.233	10.10.10.10	TCP	60	13172 → 25565 [SYN] Seq=0 Win=0 Len=0
104	0.038475	88.229.239.110	10.10.10.10	TCP	60	8453 → 25565 [SYN] Seq=0 Win=0 Len=0
105	0.038476	122.18.30.90	10.10.10.10	TCP	60	53667 → 25565 [SYN] Seq=0 Win=0 Len=0
106	0.038718	36.15.83.233	10.10.10.10	TCP	60	32412 → 25565 [SYN] Seq=0 Win=0 Len=0
107	0.038849	142.231.236.110	10.10.10.10	TCP	60	33555 → 25565 [SYN] Seq=0 Win=0 Len=0
108	0.039516	174.81.233.110	10.10.10.10	TCP	60	41651 → 25565 [SYN] Seq=0 Win=0 Len=0
109	0.039595	126.27.20.90	10.10.10.10	TCP	60	43271 → 25565 [SYN] Seq=0 Win=0 Len=0
110	0.039661	108.77.107.233	10.10.10.10	TCP	60	62740 → 25565 [SYN] Seq=0 Win=0 Len=0
111	0.039662	154.228.233.110	10.10.10.10	TCP	60	13679 → 25565 [SYN] Seq=0 Win=0 Len=0
112	0.039760	82.222.106.233	10.10.10.10	TCP	60	53550 → 25565 [SYN] Seq=0 Win=0 Len=0
113	0.040367	104.198.50.110	10.10.10.10	TCP	60	6901 → 25565 [SYN] Seq=0 Win=0 Len=0
114	0.040379	40.193.89.233	10.10.10.10	TCP	60	4384 → 25565 [SYN] Seq=0 Win=0 Len=0
115	0.040708	154.91.221.233	10.10.10.10	TCP	60	4038 → 25565 [SYN] Seq=0 Win=0 Len=0
116	0.040824	92.201.44.110	10.10.10.10	TCP	60	23673 → 25565 [SYN] Seq=0 Win=0 Len=0
117	0.040825	182.44.82.233	10.10.10.10	TCP	60	31954 → 25565 [SYN] Seq=0 Win=0 Len=0
118	0.040902	198.102.67.89	10.10.10.10	TCP	60	60847 → 25565 [SYN] Seq=0 Win=0 Len=0
119	0.040954	114.116.83.233	10.10.10.10	TCP	60	3982 → 25565 [SYN] Seq=0 Win=0 Len=0
120	0.040955	50.153.220.233	10.10.10.10	TCP	60	59982 → 25565 [SYN] Seq=0 Win=0 Len=0
121	0.040955	24.17.47.110	10.10.10.10	TCP	60	42053 → 25565 [SYN] Seq=0 Win=0 Len=0
122	0.041204	26.59.251.110	10.10.10.10	TCP	60	32751 → 25565 [SYN] Seq=0 Win=0 Len=0
123	0.041502	98.203.240.110	10.10.10.10	TCP	60	15175 → 25565 [SYN] Seq=0 Win=0 Len=0
124	0.041575	60.145.228.233	10.10.10.10	TCP	60	21156 → 25565 [SYN] Seq=0 Win=0 Len=0
125	0.041576	72.93.84.233	10.10.10.10	TCP	60	44416 → 25565 [SYN] Seq=0 Win=0 Len=0
126	0.041577	200.92.201.110	10.10.10.10	TCP	60	22869 → 25565 [SYN] Seq=0 Win=0 Len=0
127	0.041878	74.3.239.110	10.10.10.10	TCP	60	24767 → 25565 [SYN] Seq=0 Win=0 Len=0
128	0.042160	166.20.89.233	10.10.10.10	TCP	60	52802 → 25565 [SYN] Seq=0 Win=0 Len=0
129	0.042161	90.190.224.110	10.10.10.10	TCP	60	2479 → 25565 [SYN] Seq=0 Win=0 Len=0
130	0.042463	156.157.236.110	10.10.10.10	TCP	60	55609 → 25565 [SYN] Seq=0 Win=0 Len=0
131	0.042554	112.17.232.233	10.10.10.10	TCP	60	42808 → 25565 [SYN] Seq=0 Win=0 Len=0
132	0.042555	106.41.223.233	10.10.10.10	TCP	60	48726 → 25565 [SYN] Seq=0 Win=0 Len=0
133	0.042853	134.156.225.110	10.10.10.10	TCP	60	4891 → 25565 [SYN] Seq=0 Win=0 Len=0
134	0.042995	190.19.225.233	10.10.10.10	TCP	60	32010 → 25565 [SYN] Seq=0 Win=0 Len=0
135	0.043182	76.189.243.110	10.10.10.10	TCP	60	36425 → 25565 [SYN] Seq=0 Win=0 Len=0
136	0.043335	28.164.219.110	10.10.10.10	TCP	60	12473 → 25565 [SYN] Seq=0 Win=0 Len=0
137	0.043470	24.155.224.233	10.10.10.10	TCP	60	25232 → 25565 [SYN] Seq=0 Win=0 Len=0
138	0.044226	216.236.221.110	10.10.10.10	TCP	60	30853 → 25565 [SYN] Seq=0 Win=0 Len=0
139	0.044227	178.91.225.110	10.10.10.10	TCP	60	58423 → 25565 [SYN] Seq=0 Win=0 Len=0
140	0.044444	154.47.69.110	10.10.10.10	TCP	60	64563 → 25565 [SYN] Seq=0 Win=0 Len=0
141	0.044659	204.41.157.231	10.10.10.10	TCP	60	9664 → 25565 [SYN] Seq=0 Win=0 Len=0
142	0.044733	22.81.209.110	10.10.10.10	TCP	60	12875 → 25565 [SYN] Seq=0 Win=0 Len=0
143	0.045063	96.17.211.110	10.10.10.10	TCP	60	13277 → 25565 [SYN] Seq=0 Win=0 Len=0
144	0.045246	44.88.157.97	10.10.10.10	TCP	60	44706 → 25565 [SYN] Seq=0 Win=0 Len=0
145	0.045246	156.252.252.233	10.10.10.10	TCP	60	43332 → 25565 [SYN] Seq=0 Win=0 Len=0

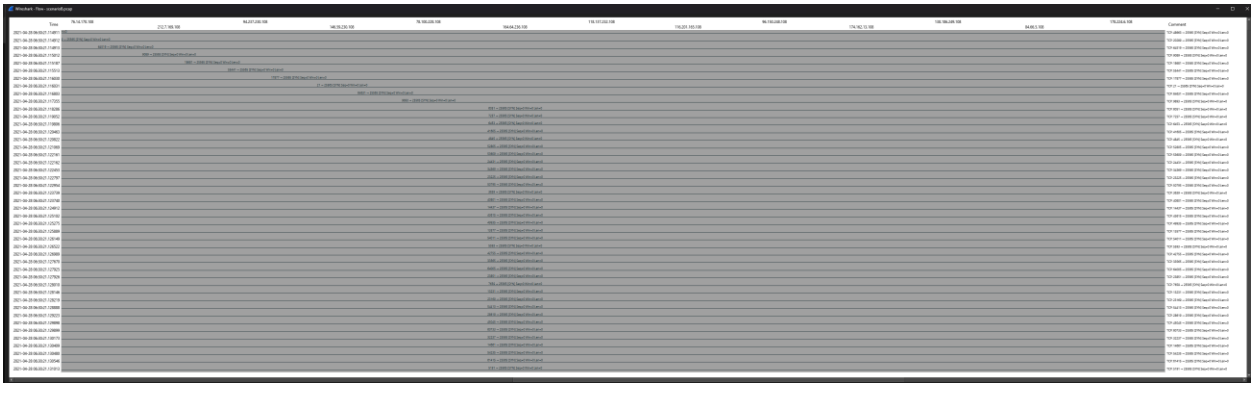
- **Malformed Packet Indicators**: Anomalous packets with incorrect headers or conflicting flags were identified, serving as IoCs.

Alexander Ratcliffe Cell: 703-498-7477

No.	Time	Source	Destination	Protocol	Length	Info
7024	0.298500	95.175.138.56	10.10.10.10	TCP	60	33570 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
2287	0.201134	94.151.139.181	10.10.10.10	TCP	60	33485 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
9175	0.332763	92.36.220.24	10.10.10.10	TCP	60	17570 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
7225	0.302306	92.195.18.20	10.10.10.10	TCP	60	9056 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
19286	0.471025	92.186.127.45	10.10.10.10	TCP	60	41612 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
11542	0.367363	91.67.202.205	10.10.10.10	TCP	60	62444 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
31208	3.892679	91.166.43.86	10.10.10.10	TCP	60	14289 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
19608	0.475831	90.243.27.161	10.10.10.10	TCP	60	60822 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
5832	0.276674	88.84.68.222	10.10.10.10	TCP	60	30237 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
21003	0.492392	88.36.73.154	10.10.10.10	TCP	60	42415 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
36359	4.225510	88.213.88.157	10.10.10.10	TCP	60	7362 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
30487	3.883596	85.232.245.213	10.10.10.10	TCP	60	25994 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
20236	0.484123	85.110.215.50	10.10.10.10	TCP	60	54324 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
22389	0.901445	84.148.106.172	10.10.10.10	TCP	60	31071 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
11913	0.372125	83.135.157.165	10.10.10.10	TCP	60	14797 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
28614	3.859765	82.159.131.161	10.10.10.10	TCP	60	11351 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
32603	3.910799	80.78.218.92	10.10.10.10	TCP	60	11251 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
20867	0.490950	8.48.118.78	10.10.10.10	TCP	60	10342 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
1445	0.169825	79.62.32.13	10.10.10.10	TCP	60	3005 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
16476	0.431058	79.148.172.248	10.10.10.10	TCP	60	55214 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
22485	0.902434	78.240.8.151	10.10.10.10	TCP	60	38796 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
20546	0.487557	75.82.27.52	10.10.10.10	TCP	60	51522 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
23414	0.997802	75.33.146.125	10.10.10.10	TCP	60	8747 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
31808	3.900165	75.11.208.142	10.10.10.10	TCP	60	34089 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
17776	0.450430	72.54.126.224	10.10.10.10	TCP	60	35184 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
9632	0.339798	71.84.38.158	10.10.10.10	TCP	60	56189 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
23073	0.993928	70.116.122.36	10.10.10.10	TCP	60	64961 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
30819	3.887819	70.1.194.182	10.10.10.10	TCP	60	37499 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
8059	0.315437	67.27.167.76	10.10.10.10	TCP	60	59635 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
10979	0.359482	65.239.206.37	10.10.10.10	TCP	60	35980 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
23808	1.198688	63.30.94.92	10.10.10.10	TCP	60	33518 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
5757	0.275301	61.63.243.136	10.10.10.10	TCP	60	42620 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
24903	3.812160	59.151.76.166	10.10.10.10	TCP	60	44734 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
9897	0.343643	59.151.48.81	10.10.10.10	TCP	60	49120 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
18328	0.458945	55.6.114.45	10.10.10.10	TCP	60	43723 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
16197	0.427468	54.251.43.254	10.10.10.10	TCP	60	57536 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
12926	0.385728	53.120.105.43	10.10.10.10	TCP	60	40139 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
24211	1.204008	49.159.55.164	10.10.10.10	TCP	60	13095 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
953	0.146021	46.244.34.152	10.10.10.10	TCP	60	[TCP Retransmission] 34508 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
672	0.123249	46.244.34.152	10.10.10.10	TCP	60	34508 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
5056	0.261972	46.162.121.228	10.10.10.10	TCP	60	25017 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
2180	0.197326	46.115.6.90	10.10.10.10	TCP	60	42811 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
3881	0.238696	45.43.212.63	10.10.10.10	TCP	60	19222 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
22068	0.897630	45.246.40.166	10.10.10.10	TCP	60	26061 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]
3762	0.236212	44.86.82.107	10.10.10.10	TCP	60	31507 → 25565 [SYN] Seq=0 Win=0 Len=0[Malformed Packet]

- **Traffic Timing Analysis**: Minimal time difference between packets suggests automated attack behavior, indicating a potential DoS attempt.
    - The timing differences between packets targeting 10.10.10.10 were minimal, indicating a high likelihood of an automated attack designed to overwhelm the server with requests.
    - Detailed statistics on the packet timing differences were gathered, indicating a mean time difference of 0.000626 seconds, highlighting the rapid nature of the attack.

- Attached Traffic Flow Visual:



-

---

8. References

- **NIST SP 800-53 Revision 5 – Security and Privacy Controls**
  https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- **CIS Controls v8 – Center for Internet Security**
  https://www.cisecurity.org/controls/cis-controls-list

- **MITRE ATT&CK Framework**
  https://attack.mitre.org

- **Wireshark Documentation – User Guide and Analysis Techniques**
  https://www.wireshark.org/docs/

- **T1499 – MITRE ATT&CK: Endpoint Denial of Service**
  https://attack.mitre.org/techniques/T1499/

- **T1046 – MITRE ATT&CK: Network Service Scanning**
  https://attack.mitre.org/techniques/T1046/
