

Digital Forensic Report

Case ID: DOS-2025-007

Case Title: Investigation of Denial of Service (DDoS)
Attack using Metasploit (msfconsole) and hping

Investigator(s): Nikhil Birla

Organization: Craw.in



Date: 18-Aug-2025, 08:21 PM

Email : nikhilbirla8882@gmail.com

1) Summary

This report analyzes a Denial of Service (DoS) attack carried out using hping and msfconsole. The attack’s impact was confirmed through multiple monitoring tools: Wireshark showed excessive SYN packet traffic, Resource Monitor and Task Manager’s Performance tab reflected significant system resource spikes, and Performance Monitor tracked abnormal network and connection metrics. These findings collectively verify the occurrence and severity of the DoS attack.

2) Scope & Objectives

Objective:

The objective of this report is to provide clear forensic proof of a Denial of Service (DoS) attack on the target system, supported by evidence collected from network and system monitoring tools.

Scope:

This report is limited to the collection, presentation, and analysis of forensic evidence demonstrating the occurrence and impact of the DoS attack. It includes packet capture data from Wireshark, connection state information, and performance metrics from Resource Monitor, Task Manager, and Performance Monitor. The report does not cover the technical details or methods of initiating the attack, focusing solely on validating the attack through collected proof.

3) Evidence Inventory

S. No.	Tool/Source	Evidence Description	Reference/File Name
1	Wireshark	SYN flood packet spike	Wireshark_Screenshot1.png
2	Resource Monitor	Network utilization peak	ResourceMonitor_Shot1.png
3	Task Manager	CPU and memory spike	TaskManager_Performance1.png
4	Performance Monitor	TCP connections, dropped packets	PerfMon_Log1.png

4) Chain of Custody

S. No.	Evidence	Collected By	Date & Time	Storage Location	Notes
1	Wireshark packet screenshot	Nikhil Birla	18 August 2025, 10:34:59 PM	Personal folder	Collected during attack window
2	Resource Monitor screenshot	Nikhil Birla	18 August 2025, 11:34:09 PM	Personal folder	During abnormal spike observed
3	Task Manager Performance tab	Nikhil Birla	18 August 2025, 11:48:11 PM	Personal folder	CPU/memory/network spike logged
4	Performance Monitor logs	Nikhil Birla	18 August 2025, 11:52:30 PM	Personal folder	Network metrics collected

5) Tools & Environment

Tools Used:

- **Wireshark:**
A network protocol analyzer used to capture and inspect live network traffic. Utilized to identify abnormal SYN packet spikes and analyze traffic patterns during the DoS attack.
- **Resource Monitor:**
A Windows built-in tool that provides a real-time view of system resources, including CPU, memory, disk, and network usage. Used to observe resource utilization and stress levels during the attack.
- **Task Manager (Performance Tab):**
Windows Task Manager's Performance tab was used to monitor CPU, memory, and network performance metrics for signs of system overload during the attack period.
- **Performance Monitor:**
A Windows advanced tool for monitoring detailed system and network performance counters over time. Employed to track network interface usage, connection states, and other metrics confirming the attack's impact.

Environment Details:

- **Target System:**
Operating System: Windows 10 Home Single Language
IP Address: 172.25.12.29

- **Monitoring System:**
The analysis and monitoring tools were run on the target machine or a connected monitoring host within the same network environment.

6) Methodology

6.1 Acquisition

All relevant data and evidence were acquired using non-intrusive methods to ensure system integrity. Network traffic was captured in real-time during the suspected DoS attack using Wireshark. System resource data, including CPU, memory, and network usage, was recorded using Resource Monitor, Task Manager's Performance tab, and Performance Monitor. Screenshots and logs were collected promptly and securely stored for analysis.

6.2 Preservation

To maintain the integrity and authenticity of the evidence, all acquired data was preserved in its original form without any modification. Digital copies and screenshots were stored in write-protected storage locations. Chain of custody procedures were followed to document the handling, transfer, and storage of all evidence items, ensuring no tampering or alteration during the investigation.

6.3 Examination & Analysis

The acquired data was thoroughly examined to identify signs of a DoS attack. Packet captures were filtered and analyzed for unusual traffic patterns such as SYN flood spikes in Wireshark. System performance metrics were compared against baseline measurements to detect abnormal resource usage correlating with attack periods. Connection states and network activity were assessed using Netstat and Performance Monitor to confirm connection saturation and service disruption. All findings were cross-verified across different tools to validate attack indicators.

6.4 Reporting

A comprehensive report was compiled detailing the findings, including screenshots and logs as supporting evidence. Each piece of evidence was correlated with timestamps and analyzed events to present a clear and factual narrative of the attack's impact. The report includes a chain of custody to support the evidence's credibility and is structured for clarity and professional presentation.

7) Analysis

The analysis of the collected evidence confirms the occurrence and impact of a Denial of Service (DoS) attack targeting the system. The different tools provided complementary insights that collectively validate the attack's presence and severity.

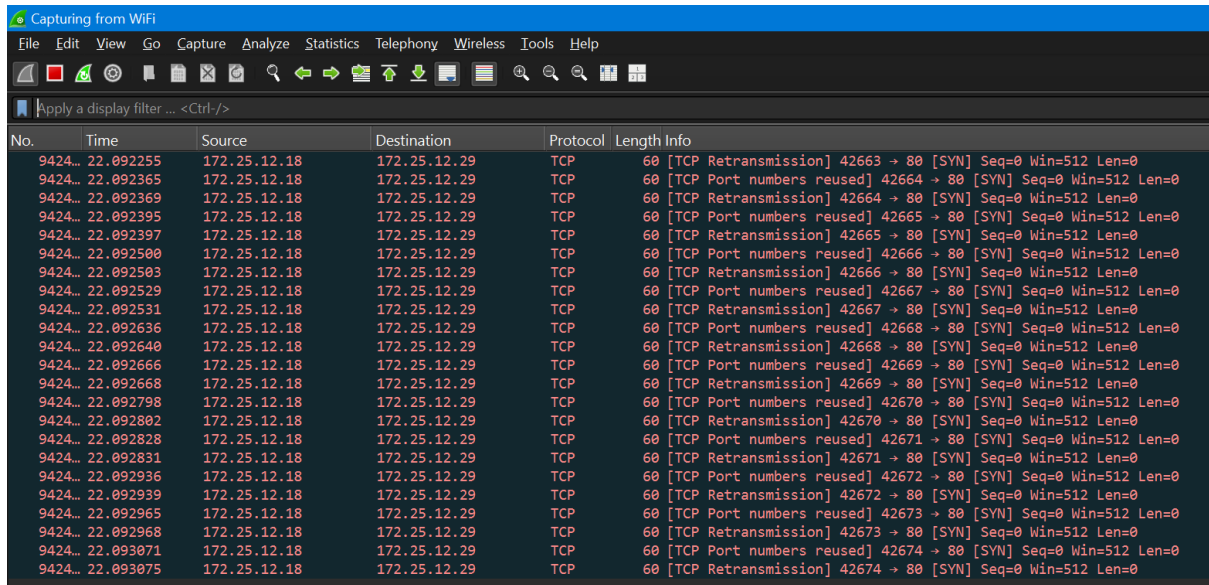
- **Wireshark Analysis:**
Packet capture data revealed a sudden and sustained surge in SYN packets directed towards the target IP and port, characteristic of a SYN flood attack. The volume of these packets significantly exceeded normal traffic levels, causing network congestion and server overload. Source IPs were either spoofed or originated from attacker-controlled machines, typical of DoS attacks.
- **Resource Monitor Findings:**
During the attack period, network throughput and total system resource utilization spiked sharply. The elevated network activity corresponded with the times at which SYN packets flooded the system, indicating the system was under heavy network stress. CPU and memory usage also increased, reflecting the system's efforts to manage the overwhelming connection requests.
- **Task Manager (Performance Tab):**
Continuous monitoring showed abnormal peaks in CPU and network usage aligned with the attack timeframe. These peaks demonstrate reduced system capacity to handle regular processes, which often leads to denial of service for legitimate users.
- **Performance Monitor Data:**
Detailed metrics, including TCP connection state counters and network interface utilization, showed a high number of half-open connections and increased packet drops. These are hallmarks of SYN flood attacks where the server's resources are tied up by incomplete connections, preventing service to legitimate traffic.

This multi-tool analysis confirms that the target system experienced a disruption consistent with a DoS attack, with substantial resource exhaustion caused by malicious SYN packet flooding. The evidence is cohesive and strongly indicates an intentional attempt to degrade or deny network services.

8) Appendices

Appendix A: Wireshark Evidence

- Screenshot 1: SYN packet flood spike during attack

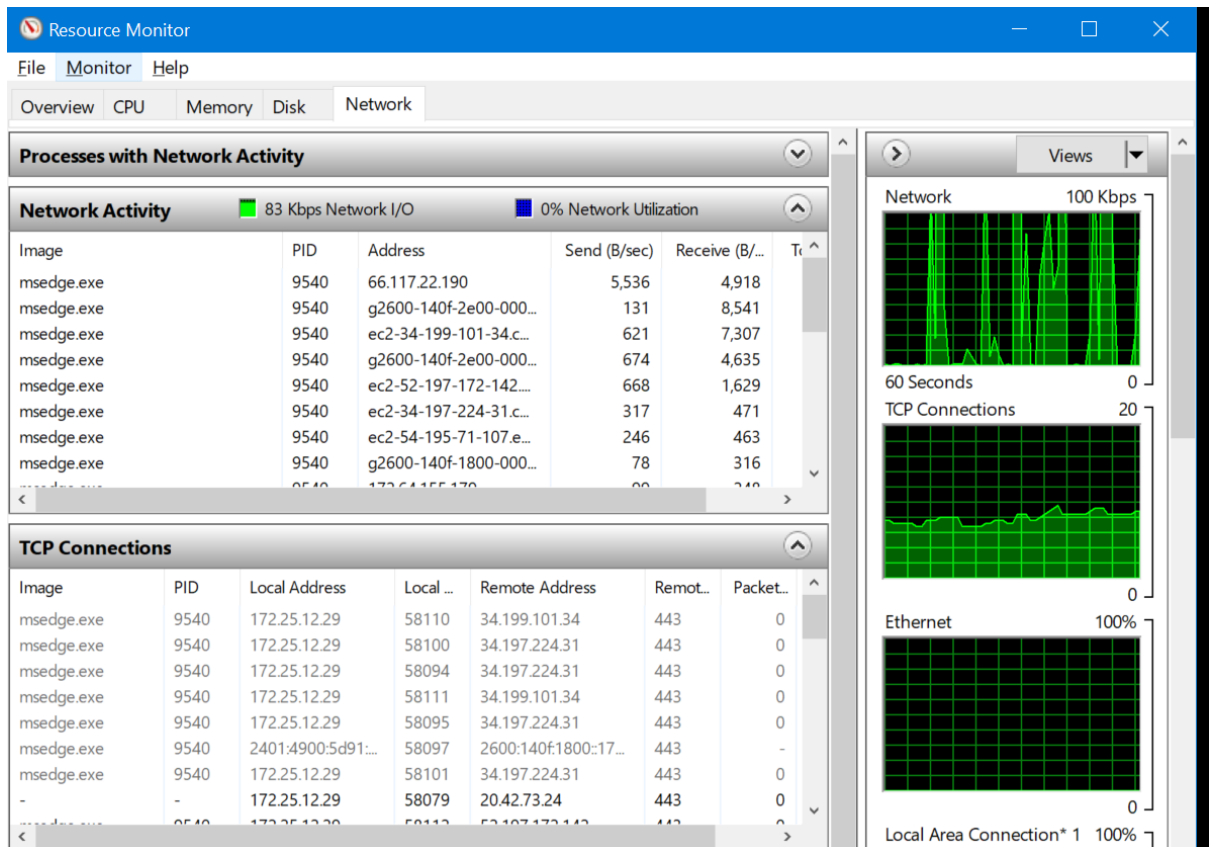


The screenshot shows a Wireshark packet capture titled "Capturing from WiFi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A display filter is applied: "Apply a display filter ... <Ctrl-/>". The packet list table shows a series of TCP packets from source 172.25.12.18 to destination 172.25.12.29. The packets are SYN packets with sequence numbers ranging from 42663 to 42674. The packet details pane shows the structure of a TCP packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet length is 60 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
9424...	22.092255	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42663 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092365	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42664 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092369	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42664 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092395	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42665 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092397	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42665 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092500	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42666 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092503	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42666 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092529	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42667 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092531	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42667 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092636	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42668 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092640	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42668 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092666	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42669 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092668	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42669 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092798	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42670 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092802	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42670 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092828	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42671 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092831	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42671 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092936	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42672 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092939	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42672 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092965	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42673 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.092968	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42673 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.093071	172.25.12.18	172.25.12.29	TCP	60	[TCP Port numbers reused] 42674 → 80 [SYN] Seq=0 Win=512 Len=0
9424...	22.093075	172.25.12.18	172.25.12.29	TCP	60	[TCP Retransmission] 42674 → 80 [SYN] Seq=0 Win=512 Len=0

Appendix B: Resource Monitor Evidence

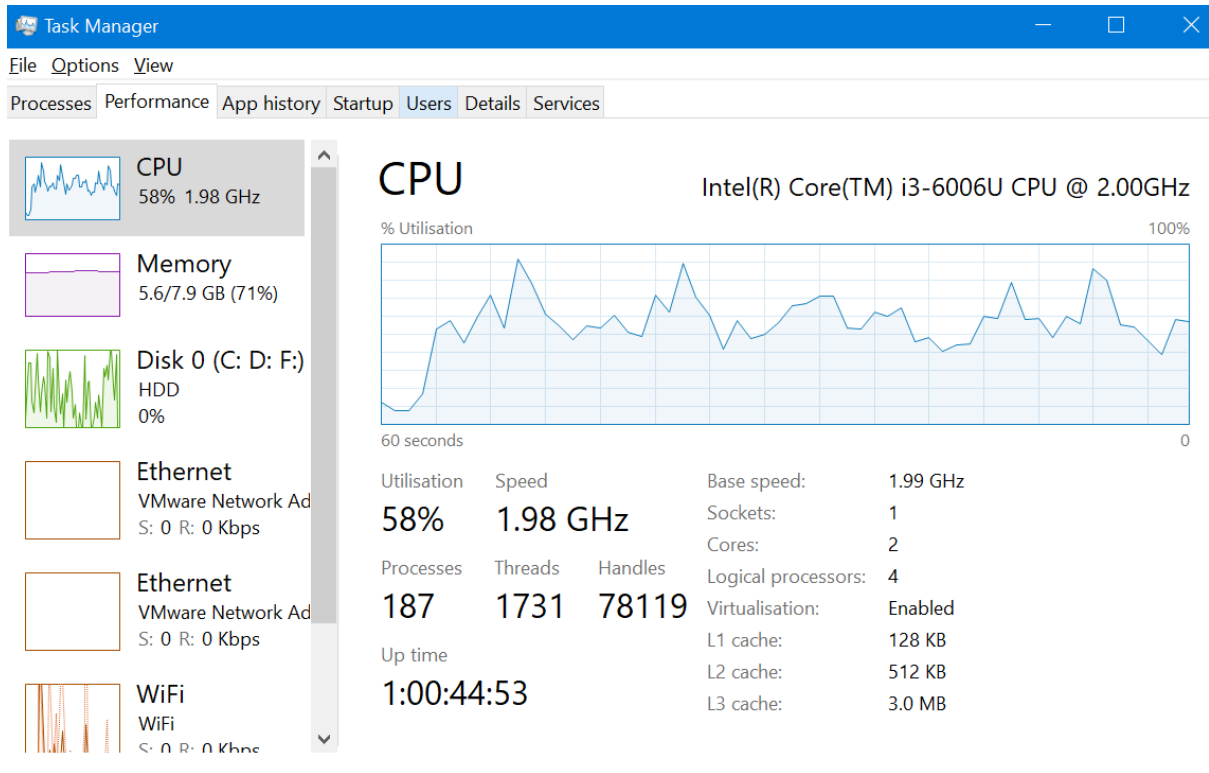
- Screenshot 2: Network usage spike



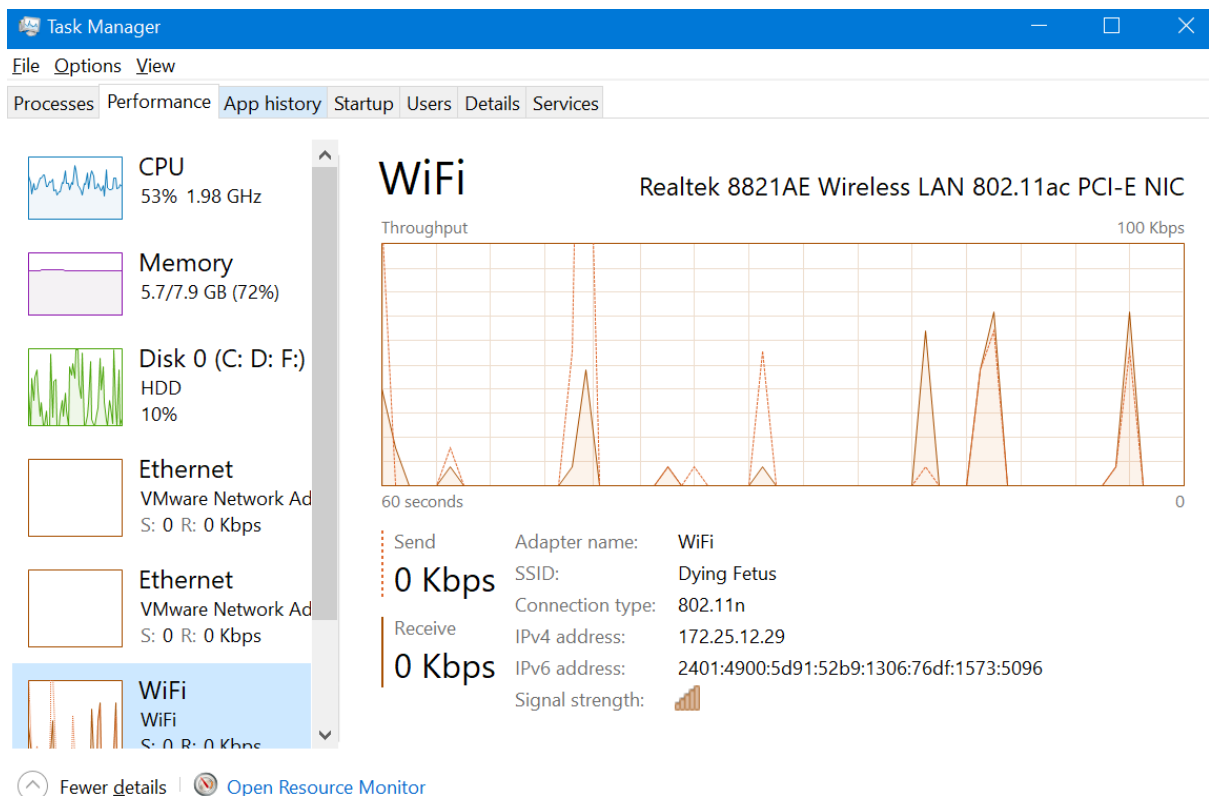
Appendix C: Task Manager Performance Tab Evidence

- Screenshot 3: CPU and memory spike

CPU usage spikes up abnormally



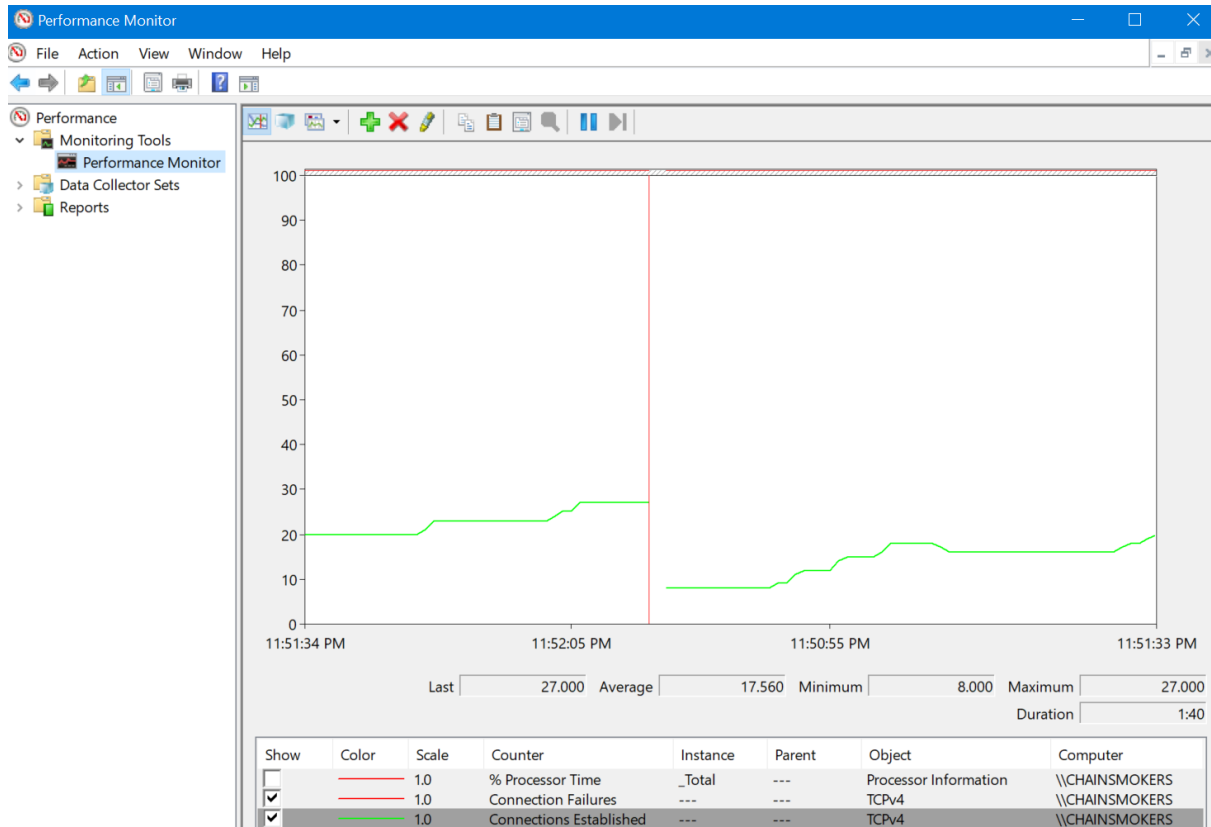
Network spikes are abnormal



Appendix D: Performance Monitor

- Screenshot 4: TCP connection Established and Failures

Sudden rise in connection established graph



9) Conclusion

The forensic analysis presented in this report confirms that the target system experienced a Denial of Service (DoS) attack characterized by SYN flooding. The evidence collected through multiple monitoring tools unequivocally shows abnormal network traffic patterns, resource exhaustion, and connection saturation. These findings affirm the attack's occurrence and impact, providing a strong basis for further security actions.