DoS in Action: Comparing the Effectiveness of Four Common Attacks

Ben Raden, Logan Swillinger, Taj Adams, Jack Gottschalk

Abstract:

This poster investigates the effectiveness of four DoS attacks (Scapy SYN Flood, Slowloris, SYN Flood, and UDP Flood) against Google Gruyere and the Apache default page. While **SYN** and **UDP Floods** caused disruption, only the Slowloris attack crashed the server. Packet volume did not determine success. This poster also compares ChatGPT's predictions to real outcomes, showing the need for hands-on testing to accurately assess DoS attacks.

What are SYN Flood, UDP Flood, Slowloris, and Scapy Dos Attacks?

A **Denial of Service (DoS)** attack disrupts access to a computer system or online service by overwhelming it with traffic [1]. These attacks can damage a company's reputation, cause financial loss, and even risk public safety in critical systems.

A **SYN Flood** exploits the TCP handshake by sending repeated SYN requests without completing the connection [2]. This fills up the server's connection queue, blocking legitimate users from connecting.

The **Slowloris attack** sends incomplete HTTP requests and keeps connections open, causing the server to wait indefinitely [3]. This low-bandwidth attack can overwhelm and crash vulnerable web servers by exhausting connection slots.

UDP Flood sends a large volume of connectionless UDP packets, overloading the target's network and forcing it to respond or drop traffic [2]. This can quickly exhaust resources and disrupt service availability.

Using **Scapy**, a Python-based tool, attackers can craft and send large volumes of spoofed SYN packets [4]. This simulates a SYN Flood attack, consuming server resources and potentially denying access to users.

Research Questions:

1. How do different types of DoS attacks (using Slowloris, Scapy-based, SYN flood, and UDP flood) compare in their ability to degrade or disrupt the availability of Google Gruyere/Apache default page?
2. What are the differences in the number of packets transmitted and lost across the four types of DoS attacks?

Methodology:

This project uses a **Mixed-Methods approach**, combining **qualitative** data (site responsiveness, crash behavior) with **quantitative** metrics (packets transmitted/lost, attack duration). This allows for a more complete evaluation of each DoS attack's effectiveness. Each attack was launched from Kali Linux using command-line tools (such as hping3) and Python scripts (Scapy and Slowloris).

ChatGPT Attack Predictions and Results:

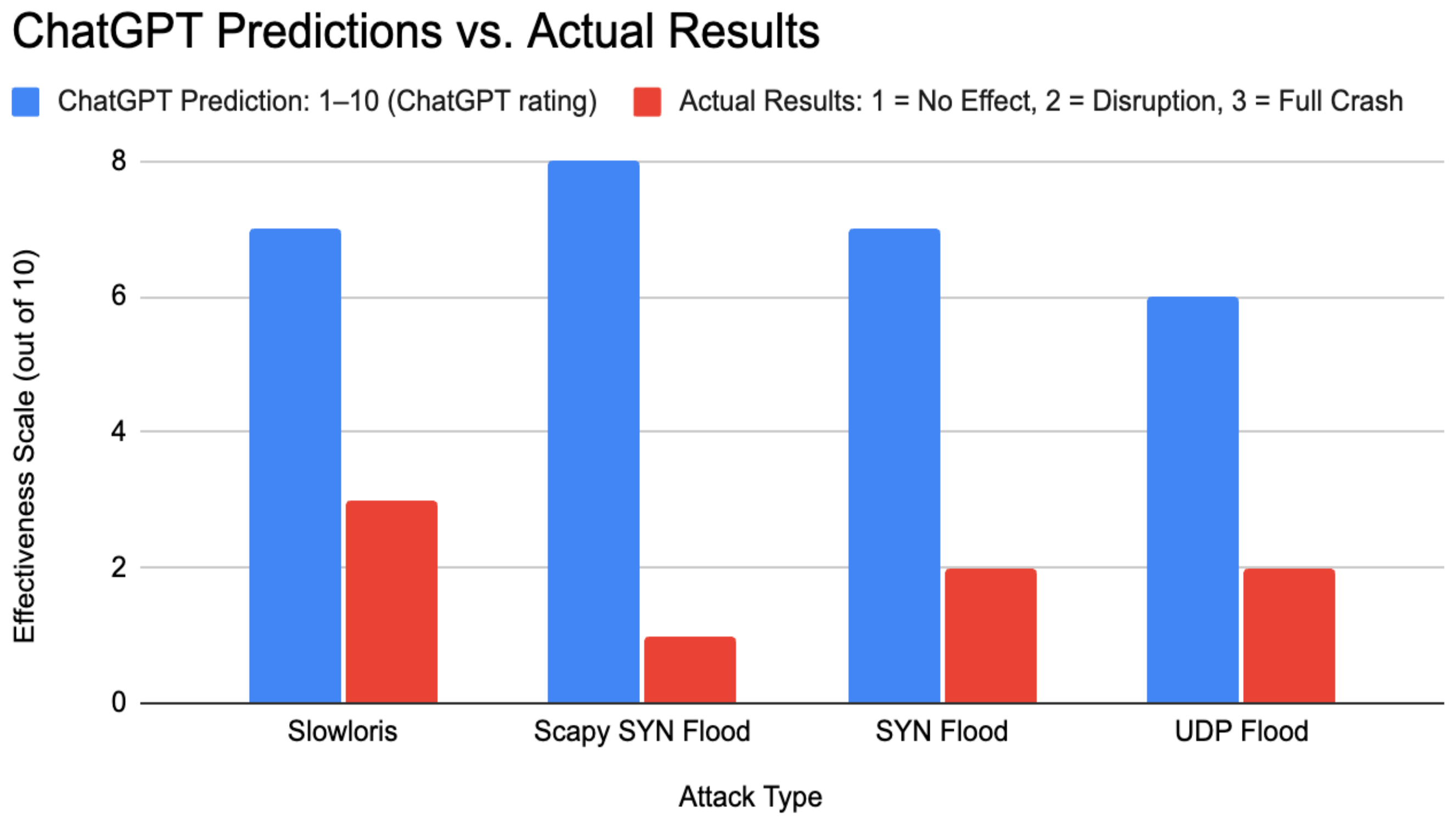

Figure 1. This graph compares ChatGPT's predicted effectiveness of the four DoS attacks with the actual outcomes observed during testing. While ChatGPT rated **Scapy SYN Flood** as most effective, it had no impact. In comparison, the **Slowloris attack**, predicted to be only moderately effective, was the only attack that crashed the target. The graph shows that AI-generated predictions can be inaccurate, and that real-world testing is essential to truly understand how DoS attacks behave.

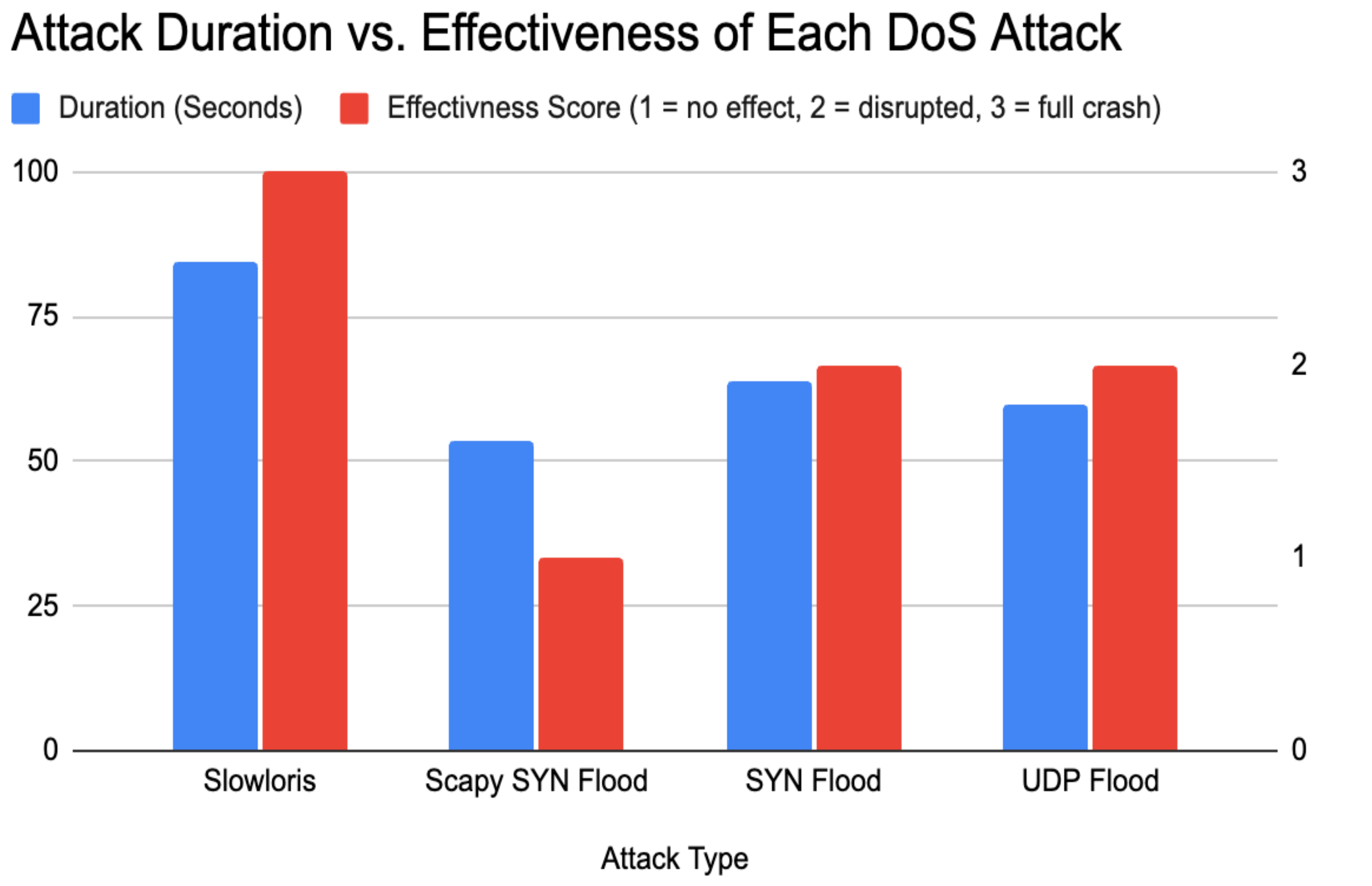

Figure 2. This graph compares the duration and effectiveness of each DoS attack. While **SYN** and **UDP Floods** caused disruption, only the **Slowloris attack**, which also lasted the longest, successfully crashed the server. The graph shows that attack length alone does not determine success. All the attacks lasted for similar durations (1:00 to 1:20 minutes) but each had different levels of effectiveness.

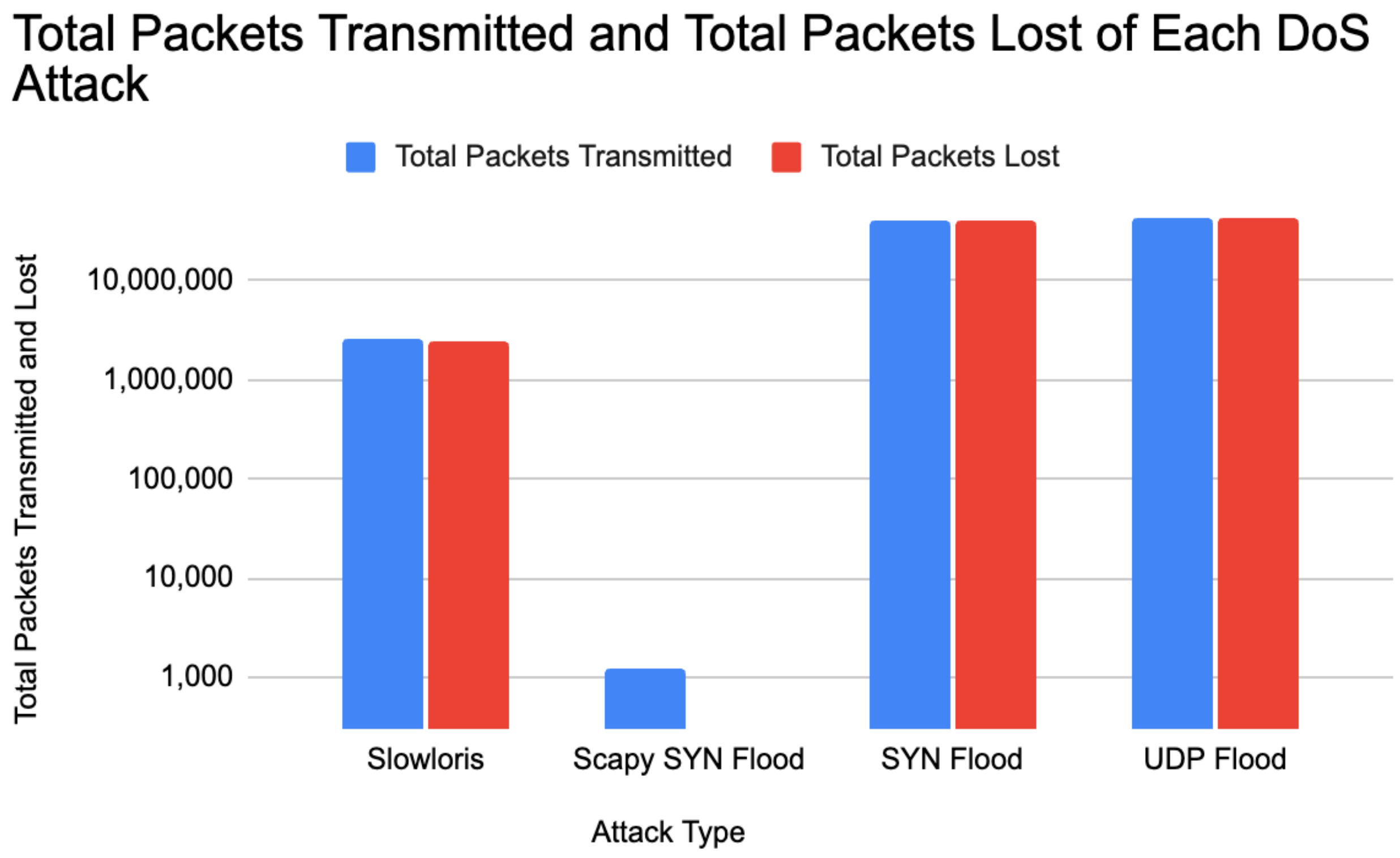

Figure 3. This graph compares packets transmitted and lost for four DoS attacks. **SYN** and **UDP Floods** each sent over 40 million packets with 100% loss, showing high disruption. **Slowloris** had fewer losses and a moderate impact. **Scapy SYN Flood** sent the fewest packets and had minimal effect.

Characteristics of Each DoS Attack Table:

Type of DoS Attack	Duration of Attack	Packets Transmitted	Packets Lost	Prevented Loading/Refreshing?	Crashed Google Gruyere/Apache Default Page?
Slowloris Attack	1:24.54 seconds	2,500,000	2,371,852	Yes	Yes
Scapy SYN Flood Attack	53.41 seconds	1,222	297	No	No
SYN Flood Attack	1:03.61 seconds	40,150,388	40,150,388	Yes	No
UDP Flood Attack	59.70 seconds	41,526,985	41,526,985	Yes	No

Table 1. This table shows the results of four DoS attacks, including duration, packet data, and impact. Only **Slowloris** crashed the server, despite sending fewer packets. **SYN** and **UDP Floods** sent over 40 million packets each, disrupted access, but did not cause a full crash.

Why Did These Results Happen?

- **Slowloris** targets the application layer, holding connections open with incomplete HTTP requests, this overwhelmed the server and caused a crash with fewer packets.
- **SYN** and **UDP Floods** were high volume but likely filtered or rate-limited by the host system, which prevented a full crash.
- **Scapy SYN Flood** sent very few packets, making it too weak to overwhelm the target or trigger any noticeable impact.
- The effectiveness of an attack depends more on the method and layer targeted than the number of packets sent.
- Modern servers are better at handling large amounts of traffic, but they can still be vulnerable to low-traffic attacks that slowly exhaust resources, like **Slowloris.**

Conclusion:

We tested four DoS attacks to evaluate their real-world impact. Only **Slowloris**, despite sending fewer packets, crashed the server, proving that attack method and target layer matter more than traffic volume. In contrast, **SYN** and **UDP Floods**, while sending over 40 million packets each, only disrupted access. **Scapy SYN Flood** had no noticeable effect due to its low packet count.

These results highlight that application-layer attacks can be more effective than high-volume floods, especially against vulnerable systems. They also emphasize the need for hands-on testing, as ChatGPT's predictions did not fully match the actual test results.

References:

1. Ramanauskaite, Simona, and Antanas Cenys. "Taxonomy of DoS attacks and their countermeasures." *Central European Journal of Computer Science* 1 (2011): 355-366.
2. Gu, Qijun, and Peng Liu. "Denial of service attacks." *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications* 3 (2007): 454-468.
3. Sabri, Shima, Noraini Ismail, and Amir Hazzim. "Slowloris DoS attack based simulation." In *IOP Conference series: materials science and engineering*, vol. 1062, no. 1, p. 012029. IOP Publishing, 2021.
4. Görtz, S., Fischer, S., & Hackenberg, R. (2023). Generation of Distributed Denial of Service Network Data with Phyton and Scapy. *CLOUD COMPUTING 2023*, 17.