Distributed Denial of Service (DDoS) Attacks

Jonny (Jianhua) Yu (000483746) and

Alice (Yee Sin) Yu (000488835)

Department of Computer Systems Technology, Vancouver Community College

CSTP 2106: Intro to Computer Security

Professor Rahim Virani

December 8, 2025

Distributed Denial of Service (DDoS) Attacks

In the world today, organizations of all sizes, government agencies, and individuals rely heavily on online services in their daily lives. A DDoS attack is one of the most common cyberattacks, and it uses a large amount of traffic to flood websites and networks, preventing real users from accessing the services. It started with a simple trick and has now evolved into a serious weapon used by criminals and even nation-states.

Cloudflare's Q4-2024 report says that the DDoS attacks increased a lot during 2024. Some of the DDoS attacks reached a record 5.6 terabits per second. According to Stormwall's 2024 Review, the number of DDoS attacks worldwide increased by 108% in 2024 compared to 2023, nearly doubling in just one year. Before going through how DDoS attack works, we should understand why it matters in computer security.

Why DDoS Matters in Computer Security

According to Ciampa (2022), the CIA triad consists of Confidentiality, Integrity, and Availability. A DDoS attack targets mainly the "availability" by overloading a system and preventing real users from accessing services. However, its impact can extend beyond service disruption. Attackers often use DDoS attacks as a smokescreen to hide other malicious activities, such as installing malware or exfiltrating data, thereby threatening all three principles of the CIA triad at the same time.

Since DDoS attacks are the major threat used by cybercriminals, they lead to financial loss, operational disruption, and reputational damage to organizations around the world. Understanding DDoS attacks becomes important for the Computer Security course. The course prioritized both lab works and concepts to help understand the real-world threats and the importance of learning computer security. Connecting these concepts to practical lab exercises allows us to better understand how DDoS attacks work and how they can be mitigated.

What Are DDoS Attacks?

According to the Canadian Centre for Cyber Security (2024), DDoS attacks fall into three categories based on network layers:

1. Volumetric Attacks (Layer 3): They flood the network with data requests to exhaust the bandwidth and the processing capacity, commonly use DNS amplification and UDP floods.
2. Protocol Attacks (Layer 4): Protocol attacks target the weaknesses in data transfer protocols. They overload server resources and network equipment, such as firewalls. Most commonly known is SYN flood attacks the target servers by send connection requests with fake IP addresses.
3. Application Layer Attacks (Layer 7): These attacks target on the application and are difficult to detect. Examples include HTTP floods and SQL injection attacks that exhaust server resources while appearing as real user activity.

DDoS attacks have become more complex. Attackers now use advanced techniques to analyze network behavior and adjust their attacks in real time to avoid detection (NSFOCUS, 2024). They combine multiple attack types and switch between them quickly to overcome defenses.

Industry Threats and Impacts

DDoS attacks have grown significantly throughout 2024 per Stormwall's review, the number of DDoS attacks worldwide grew to about twice as much in just one year. NSFOCUS's 2024 analysis mentioned attackers are using AI tools to make DDoS attacks more effective and more difficult to detect.

The H1-2024 radar report from Gcore listed that the gaming industry accounted for almost half of all DDoS attacks in the H1-2024. Attackers use DDoS as a competitive tactic in tournaments and matches, intentionally targeting opponents to gain advantages.

Government agencies got heavy attacks accounting for 19% in 2024, mainly due to geopolitical conflicts. CISA emphasizes that government and public infrastructure systems experience ongoing DDoS

threats that can disrupt essential services (CISA, 2021). Attacks on infrastructure like power grids and emergency services are particularly dangerous as they can cause real-world damage.

Technology companies shared 15% of the annual attacks count in 2024. Especially the cloud services providers, they are facing the compounding threats since disruptions affect all their customers at the same time. The financial industry shared 12% of annual attacks count, as the industry must stay online 24/7, as one minute of interruption can cost millions of dollars lost in transactions and reputational damage. At the same time, "Ransom DDoS" attacks have emerged, where attackers threaten service shutdowns to extort payments.

Project Demonstration

The lab demonstrated on an isolated virtual environment with a few virtual machines (VMs): an attacker (Kali Linux), a victim (Xubuntu) and an observer (Ubuntu, optional). Tools include:

- DDoS Attack Script – a Python-based script (ddos-attack.py) simulates a high-volume traffic flood toward a target IP and port. Penetration testers often use Python tools to simulate DDoS attacks in red-team/blue-team training.
- Apache2 Web Server – Apache2 runs on the victim VM to simulate a production web server. It is one of the most widely deployed web servers, and it is essential for security professionals to understand how servers behave under attack.
- Monitoring Tools – Tools such as "top" shows CPU usage and process activity. "iftop / nload" provides live network bandwidth analysis, and "iptraf-ng" offers detailed network statistics. These tools allow administrators to quickly spot unusual and suspicious traffic patterns and respond effectively during potential security incidents.
- Defensive Tools – Using "XDP" and "nftables" to defend, "XDP" is a high-performance packet-processing framework, which used for traffic filtering before it reaches to the main network. "nftables" provides an efficient framework for managing complex firewall rules and stateful traffic.

Conclusion

This project allowed us to explore both the technical and conceptual aspects of the topic in depth. Through our research and hands-on experimentation, we gained a clearer understanding of how the system works and why the concepts behind it are important. We found it particularly interesting to see how theory connects to real-world applications, and how different tools or methods can influence the final outcome. Some parts of the process were challenging, especially when unexpected errors or technical limitations appeared but overcoming those difficulties was also very rewarding. Overall, this experience strengthened my problem-solving skills and deepened my knowledge of the subject. Our work was supported by the references I consulted, which provided valuable insight and guided my analysis.

Reference

Canadian Centre for Cyber Security (2024). *Defending Against Distributed Denial of Service (DDoS) Attacks – ITSM.80.110*. https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110

CISA (2021). *Understanding Denial-of-Service Attacks.* https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Ciampa, M. D. (2022). *CompTIA Security+: Guide to Network Security Fundamentals (7th ed.)*. Cengage.

Cloudflare (2024). *Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4.* https://blog.cloudflare.com/ddos-threat-report-for-2024-q4

Gcore (2024). *DDoS Attack Trends for Q1–Q2 2024: Insights from Gcore Radar Report.* https://gcore.com/blog/radar-q1-q2-2024-insights

NSFOCUS (2024). *2024 Global DDoS Attack Trends: Insights, Challenges, and Defense Strategies.* https://nsfocusglobal.com/2024-global-ddos-attack-trends-insights-challenges-and-defense-strategies/

StormWall (2024). *2024 in Review: DDoS Attacks Report by StormWall.* https://stormwall.network/resources/blog/ddos-attack-statistics-2024