Cyber-Security-Bootcamp-Mulearn-OWASP-Kerala

Prepared By: Yedhukrishna

Date: Sept 21, 2025

For: Cybersecurity Bootcamp – Task 7

Task 7 — DDoS Attack Analysis

Objective: Analyze the threat of five recent DDoS attacks (short summaries) and then investigate **one chosen incident** in detail. This canvas contains: 1) brief summaries of five recent attacks, 2) a full investigation of the selected attack (technical details, motive, impact, defenses), and 3) guidance for adding screenshots/images and final resources.

Five Recent DDoS Attacks (Short Summaries)

1. **Microsoft Azure (November 2021)**
    a. **What:** One of the earliest hyper-volumetric attacks publicly disclosed, peaking at ~3.47 Tbps and ~340M pps.
    b. **How it worked (brief):** Massive volumetric flood using distributed sources and reflection/amplification techniques.
    c. **Why it matters:** Showed that cloud providers and critical infrastructure can be targeted with record-scale volumetric attacks.
2. **HTTP/2 Rapid Reset Attacks (Aug–Oct 2023)**
    a. **What:** A new class of application-layer DDoS that abused HTTP/2 stream reset behavior to exhaust server resources (CVE-2023-44487).

    b. **How it worked (brief):** Attackers opened large numbers of HTTP/2 streams and repeatedly reset them, causing state and CPU pressure on servers and proxies.
    c. **Why it matters:** Revealed protocol-level weaknesses where small botnets could cause outsized impact.
3. **GorillaBot / New Botnet Campaign (Sep–Oct 2024)**
    a. **What:** A Mirai-inspired IoT botnet (nicknamed Gorilla) that launched hundreds of thousands of DDoS commands across many targets and countries.
    b. **How it worked (brief):** Compromised insecure IoT devices (default credentials, unpatched firmware) and issued high-frequency attack commands.
    c. **Why it matters:** Demonstrated how easy it is to scale attacks using cheap IoT devices and leaked botnet code.
4. **Record 7.3 Tbps Attack (May 2025 — Cloudflare mitigation)**
    a. **What:** Cloudflare reported mitigating a 7.3 Tbps attack that delivered tens of terabytes of traffic in seconds to a hosting provider.
    b. **How it worked (brief):** Mostly UDP-based volumetric flood using many distributed IPs; reflection/amplification elements suspected.
    c. **Why it matters:** Continued trend of hyper-volumetric attacks that stress global DDoS mitigation capacity.
5. **Record 11.5 Tbps Attack (Sep 2025 — Cloudflare mitigation)**
    a. **What:** Cloudflare announced mitigation of an unprecedented 11.5 Tbps/5.1B pps attack (short but intense), representing the new scale of DDoS threats.
    b. **How it worked (brief):** Multi-vector attack combining UDP floods and spoofed traffic across cloud and IoT sources.
    c. **Why it matters:** Shows rapid escalation in attack scale and the need for automated, global mitigation systems.

Selected Incident for Deep Investigation

Selected Incident: *HTTP/2 Rapid Reset Attacks (Aug–Oct 2023)*

Rationale for selection: The HTTP/2 Rapid Reset attack is technically interesting because it exploited protocol behavior (not simply more bandwidth or larger botnets). It influenced

vendors and services to patch and offered concrete, actionable mitigation strategies that can be reproduced and explained in lab settings.

1) Target

- **Typical targets:** Web servers, reverse proxies, API gateways, and any service exposing HTTP/2 (examples included cloud providers and large web services).
- **Nature of impact:** Application-layer denial-of-service — legitimate connections could be starved or the server could exhaust resources handling stream state.

2) Technology / Techniques Used

- **Protocol abused:** HTTP/2 multiplexing and stream lifecycle (RST_STREAM frames).
- **Attack pattern:** Open many HTTP/2 streams per TCP connection; repeatedly send RST_STREAM frames to force servers to allocate and tear down internal state; keep resources tied up long enough to prevent service to legitimate users.
- **Why it was effective:** HTTP/2's multiplexing meant a small number of TCP connections could carry many streams; some implementations did expensive work on stream reset, enabling an attacker to amplify impact without huge botnets.

3) Attacker Motive

- **Possible motives:** Disruption (political/ideological), extortion (ransom DDoS), testing of novel techniques by threat actors or researchers, and making low-cost attacks with high impact.
- **Evidence in the wild:** Multiple cloud providers and vendors observed exploit attempts (some attributed to script kiddies and others to more organized actors experimenting with the new technique).

4) Overall Impact

- **Operational:** Service outages or severe degradation for targeted web services and APIs; higher CPU and memory usage on affected servers; connection exhaustion on reverse proxies and load balancers.
- **Economic:** Potential revenue loss for e-commerce and SaaS providers during outages; mitigation and forensic costs.
- **Security landscape effect:** Prompted multiple vendors (Google, AWS, Cloudflare, NGINX) to add mitigation logic and pushed for CVE disclosures and vendor patches.

5) Defensive Strategies That Could Have Mitigated It

- **Protocol hardening / patching:** Apply vendor patches for HTTP/2 stacks (web servers, proxies) that avoid expensive work on RST_STREAM and better manage stream lifecycles.
- **Rate limiting and connection limits:** Enforce per-IP or per-connection stream limits and timeouts; cap the number of concurrent streams per connection.
- **HTTP/2-aware WAFs / proxies:** Use WAFs and load balancers that understand HTTP/2 internals and drop abusive patterns (rapid resets, abnormal reset frequency).
- **Anomaly detection & traffic shaping:** Detect sudden spikes in RST frames or unusual HTTP/2 behavior and automatically throttle suspected clients.
- **Use of DDoS Scrubbing services / CDNs:** Place critical services behind CDNs or scrubbing networks that can absorb and filter malicious traffic at scale.
- **Monitoring & Playbooks:** Maintain observability on stream-level metrics and have a playbook to escalate, apply mitigations, or reroute traffic.

Resources

- Vendor CVE / advisories on HTTP/2 Rapid Reset (CVE-2023-44487)
- Cloudflare blog posts on large DDoS mitigations (2024–2025)
- Microsoft Azure DDoS protection reports (Nov 2021 attack)
- NSFOCUS / TheHackerNews coverage of Gorilla botnet (2024)
- Technical writeups from Google / AWS / NGINX on HTTP/2 abuses