Here is the **most comprehensive, sentence-by-sentence study note breakdown** of the uploaded document **“DoS and DDoS Notes.docx”**, written in bullet-point format for clarity and retention, with **no omitted information**, and enhanced with **deep explanations** for **CompTIA A+ 220-1102 (Core 2)** exam preparation under **Domain 2.0: Security** — particularly **Objective 2.5: Common threats and attacks**.

**✅ 1. Concept Overview**

A **Denial of Service (DoS)** attack attempts to make a system or network **unavailable to its intended users** by **overwhelming it with traffic or resource requests**.

A **Distributed Denial of Service (DDoS)** attack is the **same type of attack**, but launched from **many devices simultaneously**, usually forming a **botnet**.

**📘 2. Exam Relevance**

* **CompTIA A+ 220-1102**
* **Domain 2.0: Security**
* **Objective 2.5: Threats and vulnerabilities**
  + Understand what DoS and DDoS attacks are
  + Identify how they work and their effects
  + Know basic defense strategies and mitigation tools

**📋 3. Sentence-by-Sentence Study Notes**

**🧨 Denial of Service (DoS) – Definition**

* DoS is not **one single attack**, but a **category** of attacks.
* Purpose: **Make services or devices unavailable**.
  + Can affect **computers**, **networks**, **servers**, **routers**, and **switches**.

**🌊 DoS Example – Flooding a Server**

* A basic example: An attacker sends multiple requests (e.g., 12).
* A server can easily handle 12, but:
  + **1,200 or 12,000+** requests could **flood** the system, taking it down.
  + The server becomes overwhelmed and **crashes or becomes unresponsive**.

**🔁 SYN Flood Attack (DoS Variant)**

* Uses **incomplete TCP handshakes** to exhaust server resources:
  1. Attacker sends multiple **SYN packets** (start of handshake).
  2. Server replies with **SYN-ACK**, waiting for the **ACK**.
  3. ACK never comes (because IPs are spoofed).
* Server **reserves memory** for each half-open connection, which **never completes**.
* Eventually, the server **runs out of resources** → legitimate users can’t connect.

**🚨 DoS = Service Interruption**

* Any attack that:
  + **Shuts down or slows down services**
  + **Crashes a system**
  + Or causes **permanent damage**
* → can be categorized as **DoS**

**🧠 Modern DoS Countermeasures**

* Today’s systems are **resilient** enough that a **single DoS attack** often **isn’t enough**.
* So attackers use **DDoS instead**…

**🌐 Distributed Denial of Service (DDoS)**

* A **DDoS** uses **hundreds or thousands of devices** to **flood a target server** with traffic.
* Goal: **Force the target offline**.

**⚙️ DDoS Components:**

* Devices used in DDoS are typically:
  + **Zombies** or **bots**
  + Controlled as part of a **botnet**
* Most of these infected devices **don’t even know** they’re being used in an attack.

**💥 DNS Amplification Attack (Specialized DDoS)**

* A **type of DDoS** that:
  + **Spoofs** the IP of the victim (pretending to be them).
  + Sends **DNS queries** to DNS servers.
  + DNS servers send **large responses** back to the **spoofed (victim) address**.
* The attack is “amplified” because:
  + A **small request** generates a **large response**.
  + Multiplied by **thousands of requests**, the victim’s server gets **flooded** with traffic.

**🧮 Real-World DDoS Example: GitHub Attack (2018)**

* GitHub was hit with the **largest DDoS attack recorded** (at that time).
* Attackers used **tens of thousands of endpoints** to spike traffic to:
  + **1.35 terabits per second**
* Result:
  + GitHub went offline for **5 minutes**
  + Demonstrates how **powerful yet short-lived** DDoS attacks can be

**🛡️ Mitigating or Defending against DoS/DDoS Attacks**

**🔒 1. Blackholing or Sinkholing**

* Identifies **attacker IP addresses**
* Routes their traffic to a **null interface** (non-existent server).
* **Effectively blocks the attack**
* **Limitation**: Attacker can **change IPs** and restart the attack.

**🧠 2. Intrusion Prevention Systems (IPS)**

* Can detect and block **small-scale DoS attacks**.
* Won’t be effective against **large-scale DDoS** due to processing limits.

**☁️ 3. Elastic Cloud Infrastructure**

* System **scales up** automatically to handle increased load.
* Good for **riding out attacks**.

**💸 Cost Caveat:**

* Cloud providers **charge for extra usage**.
* A DDoS uses up **huge bandwidth and processing** = **high costs**.
* You’re **paying for traffic** that brings **no business value**.

**🌍 4. Third-Party DDoS Protection Services**

* Providers like **Cloudflare** and **Akamai** offer:
  + **Web application filtering**
  + **Content distribution networks (CDNs)**
  + **Layered defenses** (across OSI model)
* Purpose: Keep services **online** during large attacks

**🔄 Summary Points for Rapid Review**

| **Term** | **Definition / Action** |
| --- | --- |
| **DoS** | Attack that tries to **disable a service or system** by overwhelming it |
| **DDoS** | Multiple systems/bots used together to **amplify a DoS attack** |
| **Botnet** | Network of infected devices (**zombies**) used in a DDoS |
| **SYN Flood** | Attack using **incomplete TCP handshakes** to exhaust server memory |
| **DNS Amplification** | Spoofed DNS request returns **huge responses**, flooding victim |
| **Blackholing** | Routes bad traffic to **null IP** (temporary block) |
| **Elastic Infrastructure** | Automatically scales server resources to **withstand load** (costly) |
| **Cloudflare / Akamai** | Third-party DDoS mitigation providers |

**🧾 4. Exam Inclusion Notification**

✅ **Yes**, this material is directly tested on the **CompTIA A+ 220-1102 Exam**, under:

* **Domain 2.0: Security**
* **Objective 2.5:** Threats and vulnerabilities
  + DoS and DDoS are **explicitly named attack types**
  + Understanding mitigation and behavior is **critical**

You are expected to:

* Define and identify DoS and DDoS
* Recognize related terms (botnets, amplification, zombies)
* Recommend basic prevention strategies