**What is Dos attack**

A DoS (Denial of Service) attack is a type of cyber-attack in which a malicious actor seeks to make a computer or network resource unavailable to its intended users by overwhelming it with traffic or requests that exceed its capacity to handle. The goal of a DoS attack is to disrupt the normal functioning of a website, server, or network by flooding it with so much traffic that it becomes inaccessible to legitimate users. DoS attacks can be difficult to prevent because they often use a distributed network of compromised devices or systems to generate the attack traffic, making it hard to trace the source of the attack and block it.

**Step 1: Map Vulnerable Assets**

The ancient Greeks said that knowing thyself is the beginning of wisdom.

**Step 2: Assess Potential Damages**

After listing all potentially vulnerable assets, figure out how much they are worth to you.

**Step 3: Assign Responsibility**

once you create an inventory of potentially vulnerable assets, and then assign a dollar-figure (or any other currency…) to how much they are worth for you, the next step is to decide who is responsible for protecting them.

**Step 4: Set Up Detection Mechanisms**

Now that you’ve evaluated which assets you must protect and who’s responsible for protecting them, the next step is to set up measures that will alert you to when you come under attack.

**Step 5: Deploy a DDoS Protection Solution**

Finally, after you’ve assessed your vulnerabilities and costs, and set up attack detection mechanisms, now is the time to deploy actual protection.