In a Distributed Denial of Service attack (DDoS attack), the incoming data packets come from numerous sources. This traffic floods the targeted server and disrupts its normal traffic. For DDoS attacks, attackers utilize multiple compromised systems as sources of traffic. It becomes impossible to perform sudden security assessments and halt the attack by closing a single source. Unlike other cyberattacks, DDoS attack does not cause any security breach. Rather, a DDoS attack aims to make the victim's web servers unavailable to actual users. DDoS attacks can also act as a cover for other malicious attempts, such as breaching the target's security perimeter or taking down security appliances.

**Tips to Prevent a DDoS Attack**

DDoS attacks are extremely catastrophic to online organizations. It takes them days, weeks, and sometimes even months to recover from it. If the organization does not perform security assessments, it can damage their reputation and can lead them to a huge revenue loss. According to Cloudflare, the average cost to the targeted organization is about $100,000 for every hour the attack lasts. It is better to invest in security assessments and risk minimization before falling victim to an actual attack.

Let us look at some of the ways to prevent DDoS Attacks:

* **Protect your DNS servers:** An attacker may bring the web servers down by attacking Domain Name System servers (DNS servers) with DDoS attacks. For that reason, it is better to move to a cloud-based DNS provider that can offer multiple points-of-presence all around the world.
* **More Bandwidth:** More bandwidth can handle more traffic that can save the server from traffic floods. However, it is not very effective because the attacker only has to overcome the extra bandwidth.
* **Redundancy:** Achieve redundancy with multiple servers located in different areas. When there is a DDoS attack, it spreads across those servers with load balancing systems. The servers must connect to different networks to avoid single-point failures.
* **Network Hardware:** Simple hardware configuration can help prevent a DDoS attack. Configuring your router to drop incoming data packets or block DNS responses from outside can help prevent DNS and ping-based attacks.
* **Strong Network Infrastructure:** Strong security assessments with multi-level protection layers can protect from DDoS attacks. These multi-level protection layers include VPN, anti-spam, firewalls, load balancing, content filtering, and other DDoS defense techniques.

DDoS attacks have become so common that big companies are not the only target now. Small and medium-sized companies are increasingly becoming victims. According to Arbor Networks, more than 2000 DDoS attacks are observed every day. Organizations need to be aware of best prevention techniques and security assessments.