# MODULE 11 WEB DDOS ATTACK AND ITS PREVENTION

## What is DOS attack

Cyber-attacks have become a fact of life, with data breaches of high-profile businesses and organizations making headline news practically on a daily basis. One common type of cyber threat is a denial of service (DoS) that—as its name implies—renders websites and other online resources unavailable to intended users.

DoS threats come in many flavors, with some directly targeting the underlying server infrastructure. Others exploit vulnerabilities in application and communication protocols.

Unlike other kind of cyber-attacks, which are typically launched to establish a long-term foothold and hijack sensitive information, denial of service assaults do not attempt to breach your security perimeter. Rather, they attempt to make your website and servers unavailable to legitimate users. In some cases, however, DoS is also used as a smokescreen for other malicious activities, and to take down security appliances (e.g., web application firewalls).

A successful DoS attack is a highly noticeable event impacting the entire online user base. This makes it a popular weapon of choice for hacktivists, cyber vandals, extortionists and anyone else looking to make a point or champion a cause.

DoS assaults often last for days, weeks and even months at a time, making them extremely destructive to any online organization. They can cause loss of revenues, erode consumer trust, force businesses to spend fortunes in compensations and cause you to suffer long-term reputation damage.

## DoS vs. DDoS

The differences between DoS and DDoS are substantive and worth noting. In a DoS attack, a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU).

On the other hand, distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved. Unlike single-source DoS attacks, DDoS assaults tend to target the network infrastructure in an attempt to saturate it with huge volumes of traffic.

DDoS attacks also differ in the manner of their execution. Broadly speaking, DoS attacks are launched using homebrewed scripts or DoS tools (e.g., Low Orbit Ion Canon), while DDoS attacks are launched from botnets—large clusters of connected devices (e.g., cellphones, PCs or routers) infected with malware that allows remote control by an attacker.

## Types of DOS attacks –

DoS attacks can be divided into two general categories:

1. Application layer attacks (a.k.a., layer 7 attacks) can be either DoS or DDoS threats that seek to overload a server by sending a large number of requests requiring resource-intensive handling and processing. Among other attack vectors, this category includes HTTP floods, slow attacks (e.g., Slowloris or RUDY) and DNS query flood attacks.
   The size of application layer attacks is typically measured in requests per second (RPS), with no more than 50 to 100 RPS being required to cripple most mid-sized websites.

2. Network layer attacks (a.k.a., layer 3–4 attacks) are almost always DDoS assaults set up to clog the "pipelines" connecting your network. Attack vectors in this category include UDP flood, SYN flood, NTP amplification and DNS amplification attacks, and more.

   Any of these can be used to prevent access to your servers, while also causing severe operational damages, such as account suspension and massive overage charges.

   DDoS attacks are almost always high-traffic events, commonly measured in gigabits per second (Gbps) or packets per second (PPS). The largest network layer assaults can exceed 200 Gbps; however, 20 to 40 Gbps are enough to completely shut down most network infrastructures.

## Attacker Motivations

DoS attacks are launched by individuals, businesses and even nation-states, each with their own particular motivation:

**Hacktivism** – Hacktivists use DoS attacks as a means to express their criticism of everything from governments and politicians, including "big business" and current events. If they disagree with you, your site is going to go down (a.k.a., "tango down").

**Cyber vandalism** – Cyber vandals are often referred to as "script kiddies"—for their reliance on premade scripts and tools to cause grief to their fellow Internet citizens. These vandals are often bored teenagers looking for an adrenaline rush, or seeking to vent their anger or frustration against an institution (e.g., school) or person they feel has wronged them. Some are, of course, just looking for attention and the respect of their peers.

**Extortion** – An increasingly popular motivation for DDoS attacks is extortion, by which a cybercriminal demands money in exchange for stopping (or not carrying out) a crippling DDoS attack. Several prominent online software companies—including MeetUp, Bitly, Vimeo, and Basecamp—have been on the receiving end of these DDoS notes, some going offline after refusing to succumb to the extortionists' threats.

Similar to cyber vandalism, this type of attack is enabled by the existence of stresser and booter services.

**Personal rivalry** – DoS attacks can be used to settle personal scores or to disrupt online competitions. Such assaults often occur in the context of multiplayer online games, where players launch DDoS barrages against one another, and even against gaming servers, to gain an edge or to avoid imminent defeat by “flipping the table.”

Attacks against players are often DoS assaults, executed with widely available malicious software. Conversely, attacks against gaming servers are likely to be DDoS assaults, launched from stressers and booters.

**Business competition** – DDoS attacks are increasingly being used as a competitive business tool. Some of these assaults are designed to keep a competitor from participating in a significant event (e.g., Cyber Monday), while others are launched with a goal of completely shutting down online businesses for months.

One way or another, the idea is to cause disruption that will encourage your customers to flock to the competitor while also causing financial and reputational damage. An average cost of a DDoS attack to an organization can run $40,000 per hour.

Business-feud attacks are often well-funded and executed by professional "hired guns," who conduct early reconnaissance and use proprietary tools and resources to sustain extremely aggressive and persistent DDoS attacks.

**Cyber warfare** – State-sponsored DDoS attacks are being used to silence government critics and internal opposition, as well as a means to disrupt critical financial, health and infrastructure services in enemy countries.

Backed by nation-states, these well-funded and orchestrated campaigns are executed by tech-savvy professionals.

## Preparing for DoS Attacks

You can’t prevent DoS assaults. The fact is that cybercriminals are going to attack. Some are going to hit their targets, regardless of the defenses in place.

However, there are steps you can take to spot a brewing storm, including:

- Monitoring your traffic to look for abnormalities, including unexplained traffic spikes and visits from suspect IP address and geolocations. All of these could be signs of attackers performing “dry runs” to test your defenses before committing to a full-fledged attack. Recognizing these for what they are can help you prepare for the onslaught to follow.

- Keep an eye on social media (particularly Twitter) and public wastebins (e.g., Pastebin.com) for threats, conversations and boasts that may hint on an incoming attack.
- Consider using third-party DDoS testing (i.e., pen testing) to simulate an attack against your IT infrastructure so you can be prepared when the moment of truth arrives. When you undertake this, test against a wide variety of attacks, not just those with which you are familiar.
- Create a response plan and a rapid response team, whose job is to minimize the impact of an assault. When you plan, put in place procedures for your customer support and communication teams, not just for your IT professionals.

## Mitigation –

This first step in preparing your organization to deal with a DDoS incident is to assess your risk. Important basic questions include:

- Which infrastructure assets need protection?
- What are the soft spots, or single points of failure?
- What is required to take them down?
- How and when will you know you're targeted? Will it be too late?
- What are the impacts (financial and otherwise) of an extended outage?

Armed with this information, it's then time to prioritize your concerns, examining various mitigation options within the framework of your security budget.

If you're running a commercial website or online applications (e.g., SaaS applications, online banking, e-commerce), you're probably going to want 24×7, always-on protection. A large law firm, on the other hand, may be more interested in protecting its infrastructure—including email servers, FTP servers, and back office platforms—than its website. This type of business may opt for an "on demand "solution.

The second step is to choose the method of deployment. The most common and effective way to deploy on-demand DDoS protection for your core infrastructure services across an entire subnet is via border gateway protocol (BGP) routing. However, this will only work on demand, requiring you to manually activate the security solution in case of an attack.

Consequently, if you're in need of an always-on DDoS protection for your web application, you should use DNS redirection to reroute all website traffic (HTTP/HTTPS) through your DDoS protection provider's network (usually integrated with a content delivery network,). The advantage of this solution is that most CDNs offer on-call scalability to absorb volumetric attacks, at the same time minimizing latency and accelerating content delivery.

## Mitigating Network Layer Attacks

Dealing with network layer attacks required requires additional scalability—beyond what your own network can offer.

Consequently, in the event of an assault, a BGP announcement is made to ensure that all incoming traffic is routed through a set of scrubbing centers. Each of these has the capacity to process hundreds of Gbps worth of traffic. Powerful servers located in the scrubbing centers will then filter out malicious packets, only forwarding the clean traffic to the origin server through a GRE tunnel.

This method of mitigation provides protection against direct-to-IP attacks and is usually compatible with all types of infrastructures and communication protocols (e.g., UDP, SMTP, FTP, and VoIP).

## Mitigating Application Layer Attacks

Mitigation of application layer attacks relies on traffic profiling solutions that can scale on demand, while also being able to distinguish between malicious bots and legitimate website visitors.

For traffic profiling, best practices call for signature-based and behavior-based heuristics, combined with IP reputation scoring and a progressive use of security challenges (e.g., JS and cookie challenges).

Together, these accurately filter out malicious bot traffic. Protecting against application layer attacks without any impact to your legitimate visitors.