Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY
Vol. 11. No. 1, March, 2023

Article Citation Format
Nwaocha, V.O. & Oloyede, A. (2023):
Averting DDOS Attacks in Web-Based Applications.
Journal of Digital Innovations & Contemporary Research in Science,
Engineering & Technology.
Vol. 11, No. 1. Pp 51-63
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V11N1P4

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received:27th January, 2023
Review Type: Blind Peer
Final Acceptance: 15th March, 2023

Averting DDOS Attacks in Web-Based Applications

Nwaocha, V.O. & Oloyede, A.
Department of Computer Science
National Open University of Nigeria, Abuja, Nigeria
E-mails: ogochukwuvee@gmail.com

ABSTRACT

Distributed Denial-of-Service attacks are becoming increasingly pervasive, especially in web-based applications, and their impact have been devastating and affect businesses and organisations negatively. This research highlights web-based applications which enables users connect with a remote server via a web browser. The web apps are used on a range of devices, including desktops, laptops, tablets, and smartphones, which are prone to various attacks and predominantly DDoS attacks. Consequently, effective strategies, Mitigation Service are proposed for detecting DDoS attacks and blocking malicious traffic from web-applications.

Keywords: Attacks, Cyber crimes, DDOS, Services, Web, Apps, Traffic, Mitigation, Detection.

1. INTRODUCTION

A Web-Based Application (Web app) is a program that is accessed over a network connection using HTTP, rather than existing within a device's memory (ROUSE,2022). Web-based applications often run inside a web browser with an interface similar to client/server applications. .Web apps can be written in various programming languages and make use of multiple technologies and frameworks. A web-based application will run on the client computer's browser no matter what operating system is installed. This makes web-based apps one of the most universal cross-platform solutions available today.

Web-based applications are also a unique solution that can provide users with a wide variety of multifunctional online tools capable of optimizing countless processes and solving multiple problems. They differ from a standard website because their outer appearance and functionality resemble those of a native application more than a website. And it is mainly designed for interactions with users. A web app doesn't require certain operating systems (e.g. iOS, Android, or Windows). Instead, with a client-side program (a browser) through which users run the web application, it can access remote databases to obtain required information, regardless of device.

Due to the need for information to be fast processed and presented to promptly meet user and business demands in this era, Companies and individuals 52accordingly require a place to congregate all necessary data and directly communicate with users and that brings web apps into play. These Individuals and companies customize web applications as per their ultimate goals and requirements. But generally, these software programs are considered an effective means of communication with users.

For clients, web app help interacts well with organisations through online forms, shopping carts, content management systems, and more through:

i. Online payment systems;
ii. Content management systems that are capable of handling massive data and managing simultaneous projects;
iii. Systems where customers book tickets, accommodation, and other services online;
iv. Online retail/ banking systems that work with user inputs such as login;
v. interactive Internet portals (websites that work with user input such as sign-up information);

Some typical examples NOUN portal, Gmail, Yahoo mail, Google Docs, and Google Sheets among others.

2. HOW A WEB APPLICATION WORKS

There are five integral elements to activate a web application on any device as shown in figure 1 below:

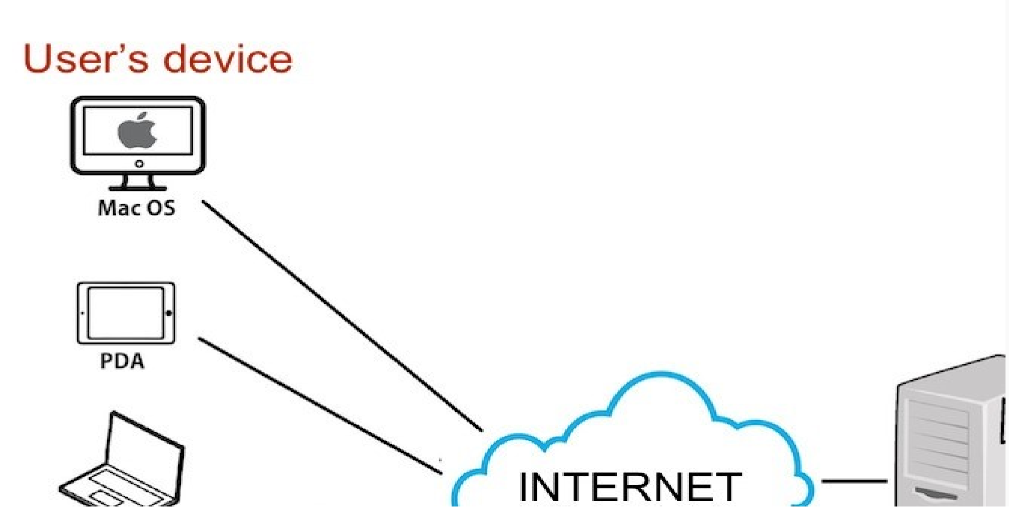

Figure 1: How a WEB APPLICATION WORKS

The integral elements to activate a web application includes:

i. Internet connection
ii. A web browser
iii. A web server
iv. An application server
v. A database

Accordingly, web app works in the same mechanism of action as a website:

i. A request is sent through a web app's interface on any browser (e.g. Google Chrome or Mozilla Firefox) to the database.
ii. On receiving the request, a web server delivers it to an application server that generated the requested file from a database.
iii. Upon obtaining a result from the web server, the application server gives it back to the user's device.
iv. The expected information (dynamic content) is displayed on the web app's user interface.

Like other applications, a web app requires front-end and back-end scripts to function well. They are written in respectively client-side and server-side programming languages which support browsers. Some common technologies include among others - C#, JavaScript and HTML.

3. WHAT IS DISTRIBUTED DENIAL OF SERVICE (DDOS)) ATTACK?

Distributed Denial of Service (DDoS)) attack is one of the most critical issues in network security, it is the main threats that the internet is facing in recent times. According to PEDAMKAR (2023), a Distributed Denial of Service (DDoS)) attack is a cyberattack from a distributed network with a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic and illegitimate requests. These sorts of attacks pose a noteworthy danger to the accessibility of network services for their legitimate users by flooding the bandwidth or network service using various infected computer systems. The targeted servers are overwhelmed with malicious packets or connection requests, causing them to slow down or even crash the server operations which results in preventing genuine users from accessing the service or resources.

Its aim is to render services unresponsive and also make computer resources unavailable to its intended users. Although the means to carry out these attacks, the motives for the attacks, and targets of the Distributed Denial of Service (DDoS) attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Distributed Denial of Service (DDoS) attacks achieve effectiveness by also utilizing multiple compromised computer systems as sources of attack traffic. These exploited machines can include computers and other networked resources such as Internet of Things (IoT) devices (these are Internet-connected devices that are not traditional computers which among others includes phones, fitness trackers, smart watches, cameras, etc.). More simplified, a Distributed Denial of Service (DDoS) attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination as seen in figure 2 below:

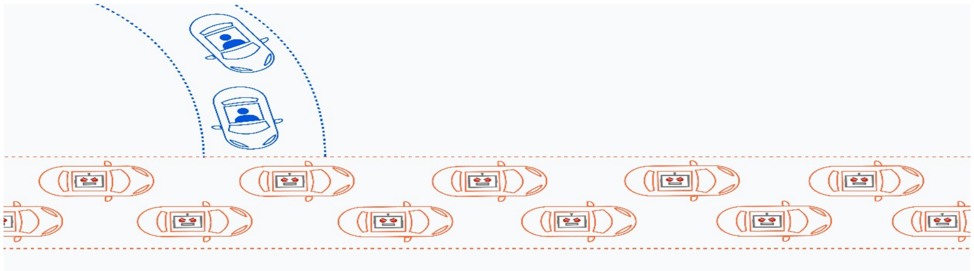

Figure 2: An Illustration of a DDoS Attack

3.1 Components/ Architecture Of A Distributed Denial Of Service Attack

DDoS attack as depicted in Figure 3 below is carried out with networks of Internet-connected machines from the master computer (Attacker). The networks consist of computers and other devices (such as IoT devices) which have been infected with malware (referred to as bots or botnets (group) or zombies, allow them to be controlled remotely by an attacker to further amplify the attacks on the target. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot for amplification.

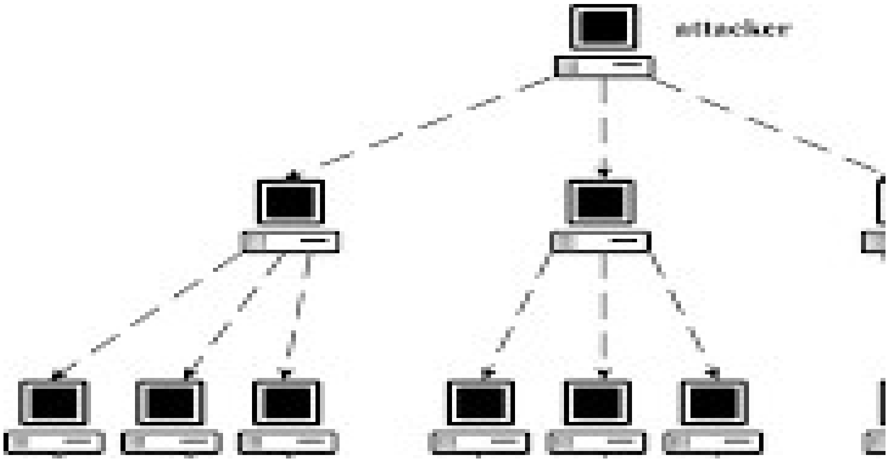

Figure 3: Components of a DDoS Attack

3.2 Execution Of Distributed Denial Of Service Attack

The Distributed Denial of Service (DDoS) attack is usually executed by a **botnet**, which is a group of compromised systems (bots) scattered worldwide.

A bot is a computer or networked device that is controlled by an attacker. Generally, a DDoS attack begins with a hacker manipulating the vulnerability in a computer system, which then becomes the DDoS master bot (attacker). The attacker master bot system finds other weak systems and takes control of them by infecting them with malware or bypassing verification measures. To command the botnet, the hackers generate a command-and-control system. The attacker then floods/overwhelms the target with traffic generated by the infected devices to take down its services.

3.3 Some Examples Of Ddos Attacks

There have been many high-profile DDoS (Distributed Denial of Service) attacks in web applications/ web sites over the years. Here are some few examples:

1. GITHUB: In February, 2018, GitHub was hit by the largest DDoS attack in history, with traffic volumes reaching 1.3Tbps. The attack lasted for about 20 minutes and made the website inaccessible to users in some parts of the world.

2. DYN: In October, 2016, a massive DDoS attack targeted Dyn, a company that provides DNS services to some of the world's largest websites. The attack caused widespread outages for popular sites like Twitter, Netflix, and Spotify.

3. KREBSONSECURITY: In September 2016, the security news website KrebOnSecurity was hit by a DDoS attack that peaked at 620 Gbps. The attack was launched using a botnet made up of Internet of Things (IoT) devices, such as compromised CCTV cameras and routers.

4. BBC: In December, 2015, the BBC's website was taken offline for several hours by a DDoS attack. The attack was claimed by a group called New World Hacking, which said it was targeting ISIS-related content on the site.

5. SPAMHAUS: In March, 2013, Spamhaus, a non-profit organisation that tracks spam and other online abuse, was hit by a massive DDoS attack that peaked at over 300 Bbps. The attack was reportedly launched by a Dutch hosting company called CyberBunker, which was angry at being added to Spamhaus' blacklist.

These are just a few examples of DDoS attacks on web pages and applications. There have also been many other attacks on organisations of all sizes and in various industries.

3.4 Classification Of Distributed Denial Of Service (DDOS) Attacks

Distributed denial of service (DDoS) attack being a broad class of cyberattack that disrupts online services and resources by overwhelming them with traffic, renders the targeted online service unusable for the duration of the DDoS attack. The hallmark of DDoS attacks is the distributed nature of the malicious traffic, which typically originates from a botnet—a criminally-controlled network of compromised machines spread around the globe. Over the years, cybercriminals have developed a number of technical approaches for taking out online targets through DDoS.

The individual techniques tend to fall into three general types of DDoS attacks:

1. Volume-based attacks
2. Protocol layer attacks
3. Application-layer attacks

1. Volume-Based Attacks

It is a classic type of DDoS that employ methods to generate massive volumes of traffic to completely saturate bandwidth, creating a traffic jam that makes it impossible for legitimate traffic to flow into or out of the targeted site. Volumetric attacks (also known as volume-based attacks or attacks on Bandwidth) are perpetrated when massive quantities of illegitimate traffic overwhelm the server, website, or other resources. Simply put, Volumetric attacks are like a traffic jam where every lane on the highway is bumper-to-bumper with cars and one can't get access to the road.

Unlike a traffic jam, however, network traffic doesn't just wait in line. Users will see the dreaded "No Connection Error," or the load times will be slow to the point of causing frustration and causing users to abandon their original request. The attacks are conducted by bombarding a server with so much traffic that its bandwidth gets completely exhausted. Volumetric distributed denial of service (DDoS) attacks are distinct from the other two types of DDoS attacks—Protocol DDoS Attacks and Application layer DDoS attacks—because they're based on brute force techniques (hacking method that uses trial and error to crack passwords, login credentials and encryption keys) that flood the target with data packets to consume bandwidth and resources.

The other two attack types generally use considerably less bandwidth and are also more focused on specific aspects of their targets such a particular protocol or a service. Hackers usually launch volumetric DDoS attacks using IoT botnets. These attacks are often used in concert with other DDoS attack types as a cover for other hacking techniques such as penetration attempts, which make web application security monitoring as difficult as possible. These attacks can also be used to disable the security infrastructure of the victim by overwhelming it and making way for other attacks to slide through.

Examples Of Volumetric Ddos Attacks

Common volumetric DDoS attacks include ICMP flood attack, UDP flood attack and DNS Amplification attack, among others.

A. ICMP (Internet Control Message Protocol) Flood Attack

An ICMP ping flood is a distributed denial of service attack in which the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic. When the attack traffic comes from multiple devices, the attack becomes a distributed denial of service attack.

The Internet Control Message Protocol (ICMP), which is utilized in a Ping Flood attack, is an internet layer protocol used by network devices to communicate. Commonly, ICMP echo-request and echo-reply messages are used to ping a network device for the purpose of diagnosing the health and connectivity of the device and the connection between the sender and the device.

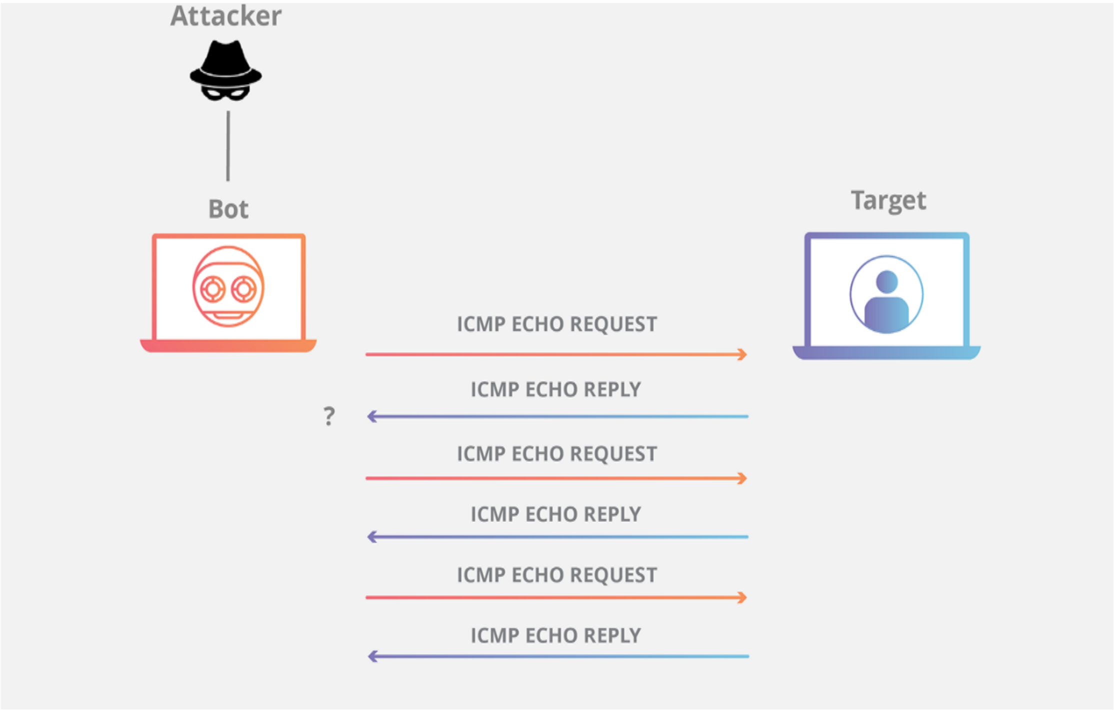

Figure 4: An ICMP Flood Attack

An ICMP request requires some server resources to process each request and to send a response. The request also requires bandwidth on both the incoming message (echo-request) and outgoing response (echo-reply). The Ping Flood attack aims to overwhelm the targeted device's ability to respond to the high number of requests and/or overload the network connection with bogus traffic. By having many devices in a botnet target the same internet property or infrastructure component with ICMP requests, the attack traffic is increased substantially, potentially resulting in a disruption of normal network activity. Historically, attackers would often spoof in a bogus IP address in order to mask the sending device.

With modern botnet attacks, the malicious actors rarely see the need to mask the bot's IP, and instead rely on a large network of un-spoofed bots to saturate a target's capacity.
The DDoS form of a Ping (ICMP) Flood can be broken down into 2 repeating steps:

1. The attacker sends many ICMP echo request packets to the targeted server using multiple devices.
2. The targeted server then sends an ICMP echo reply packet to each requesting device's IP address as a response.

The damaging effect of a Ping Flood is directly proportional to the number of requests made to the targeted server. Ping Flood attack traffic is symmetrical; the amount of bandwidth the targeted device receives is simply the sum of the total traffic sent from each bot.

B. UDP (User Datagram Protocol) Floods Attack

A UDP flood is a type of distributed denial of service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server from numerous attacker machines with the aim of overwhelming these devices' ability to process and respond. The firewall protecting the targeted server(s) can also become exhausted as a result of UDP flooding, resulting in a distributed denial of service to legitimate traffic.

A UDP flood works primarily by exploiting the steps that a server takes when it responds to a UDP packet sent to one of its ports. Under normal conditions, when a server receives a UDP packet at a particular port, it goes through two steps in response:

1. The server first checks to see if any programs are running which are presently listening for requests at the specified port.
2. If no programs are receiving packets at that port, the server responds with a ICMP (ping) packet to inform the sender that the destination was unreachable.

As each new UDP packet is received by the server, it goes through steps in order to process the request, utilizing server resources in the process. When UDP packets are transmitted, each packet will include the IP address of the source device. During this type of DDoS attack, an attacker will generally not use their own real IP address, but will instead spoof the source IP address of the UDP packets, impeding the attacker's true location from being exposed and potentially saturated with the response packets from the targeted server.

As a result of the targeted server utilizing resources to check and then respond to each received UDP packet, the target's resources can become quickly exhausted when a large flood of UDP packets are received, resulting in denial of service to normal traffic.

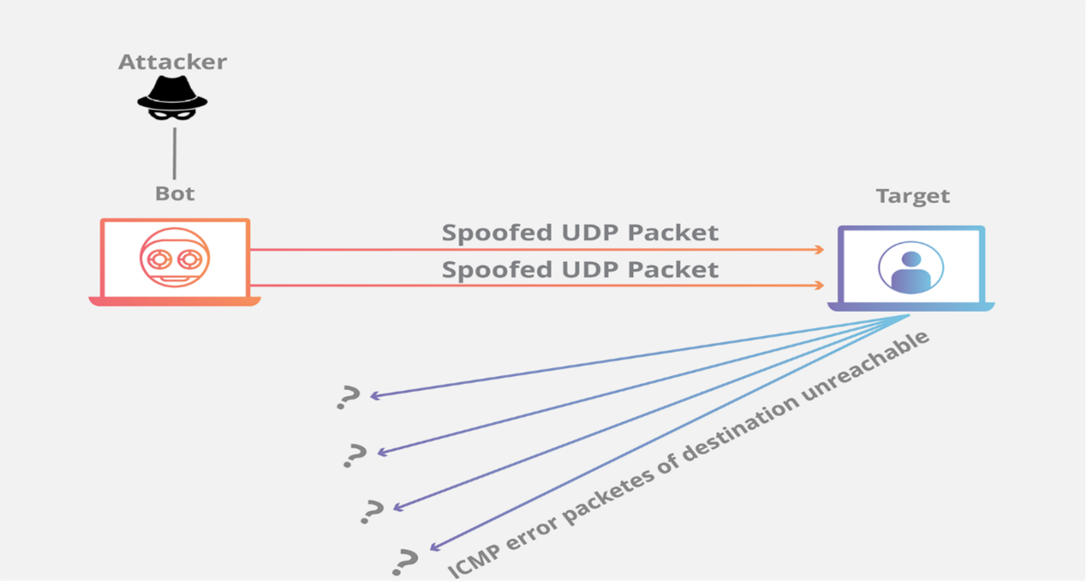

Figure 5: A UDP Flood Attack

2. Protocol Layer Attacks

Protocol attacks are designed to eat up the processing capacity of network infrastructure resources like servers, firewalls, and load balancers by targeting Layer 3 and Layer 4 protocol communications with malicious connection requests. Protocol attacks occur when an infrastructure, or parts of an infrastructure, is flooded with excessive numbers of packets. It is also known as network-layer attacks. Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible. Different types of protocol attacks include: Smurf DDoS and SYN Floods (TCP Connection) Attacks.

A. Smurf Attacks

A Smurf attack is a form of distributed denial of service (DDoS) attack that occurs at the network layer. It sends ICMP echo request traffic with a spoofed source address of the target victim to a number of IP broadcast addresses. Most hosts (like the target victim) on an IP network will accept ICMP echo requests and reply to the source address.

DDoS smurf attacks are similar in style to ping floods, which are a form of denial of service (DoS) attack. A hacker overloads computers with Internet Control Message Protocol (ICMP) echo requests, also known as pings. The ICMP determines whether data reaches the intended destination at the right time and monitors how well a network transmits data. A Smurf attack also sends ICMP pings but is potentially more dangerous because it can exploit vulnerabilities in the Internet Protocol (IP) and the ICMP.

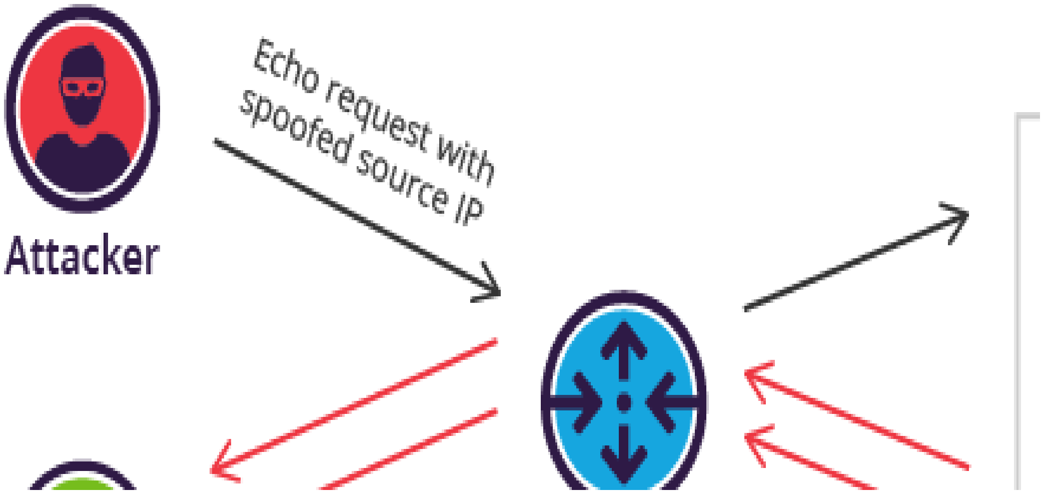

Figure 6: A Smurf Attack

A Smurf attack works through the following three-step process:

1. The DDoS Smurf malware creates a network data packet that attaches to a false IP address. This is known as spoofing.
2. The packet contains an ICMP ping message, which commands network nodes to send a reply.
3. This process, known as ICMP echoes, creates an infinite loop that overwhelms a network with constant requests.

B. SYN Flood

It is a type of denial of service (DDoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.
SYN flood attacks work by exploiting the handshake process of a TCP connection.

Under normal conditions, TCP connection exhibits three distinct processes in order to make a connection.

1. First, the client sends a SYN packet to the server in order to initiate the connection.
2. The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.
3. Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.

SYN Floods (also known as TCP Connection Attacks) target what's called a three-way handshake connection (SYN, SYN-ACK and ACK). This common TCP connection point is the vulnerability the attack exploits.

During an SYN Flood, a "handshake" request is sent to a targeted server, but it's never completed. The targeted port is then unavailable to respond to any requests. The attack spreads from there as more and more requests are sent until servers go down.

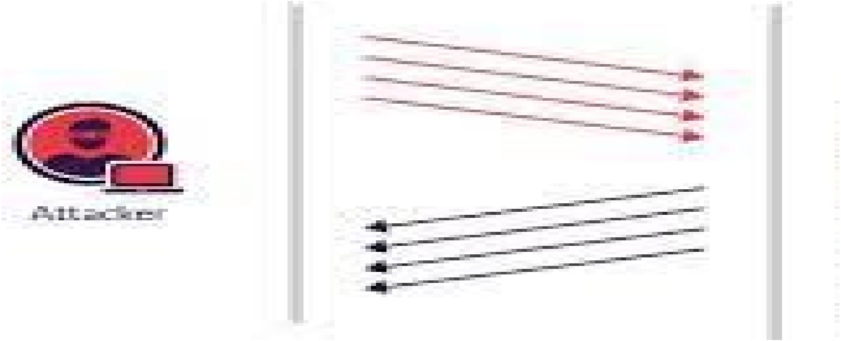

Figure 7: A SYN Flood Attack

To create denial of service, an attacker exploits the fact that after an initial SYN packet has been received, the server will respond back with one or more SYN/ACK packets and wait for the final step in the handshake. Here's how it works:

1. The attacker sends a high volume of SYN packets to the targeted server, often with spoofed IP addresses.
2. The server then responds to each one of the connection requests and leaves an open port ready to receive the response.
3. While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new open port connection for a certain length of time, and once all the available ports have been utilized the server is unable to function normally.

3. Application-Layer Attacks

Application Layer Attacks account for nearly 60% of all DDoS attacks! They are complex and typically target a specific aspect of an organisation's website or online service. By bringing down this critical component, attackers can cause serious disruptions and downtime. Application layer DDoS attacks, also known as Layer 7 DDoS attacks, are dangerous and sophisticated tools used to attack user-facing applications and networks. These malicious attacks target application layer protocols such as HTTP and DNS, often with the intention of disrupting services or hijacking application protocols. Because application layer attacks focus on the application layer, they can go undetected by traditional defense systems while still taking down websites or networks.

Protecting user-facing applications or networks from these application layer attacks should be a priority for any organisation looking to stay secure in the digital space!

How Application Layer Attacks Work:

Application Layer attacks are a type of Distributed Denial of Service (DDoS) attack that targets application-layer services such as web servers and application firewalls. Such an attack can lead to website service disruption, or even complete website shutdown. An application layer attack takes advantage of the communication protocols used to exchange data between two applications running over the internet.

It generally requires fewer resources to mount a successful application layer attack compared to other DDoS attack types since it causes more damage due to its customized nature aimed at specific services or protocols for example HTTP, SMTP or FTP. This makes application layer attacks a common tactic for disrupting critical services. As one of the more sophisticated DDoS attacks, it exploits weaknesses in the application layer (Layer 7) of the OSI model by opening connections and initiating process and transaction requests that consume finite resources like disk space and available memory.

Application-layer attacks overwhelm applications with malicious requests, affecting the layer of service where web pages are generated, and HTTP requests are made. Application-layer attacks tend to advance in a slower fashion than traditional volumetric attacks. This slower rate allows the requests to appear legitimate until they have sufficiently overwhelmed an application. The goal of these attacks is to exhaust the target's resources to create a denial of service. The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. A single HTTP request is computationally cheap to execute on the client side, but it can be expensive for the target server to respond to, as the server often loads multiple files and runs database queries in order to create a web page.Layer 7 attacks are difficult to defend against, since it can be hard to differentiate malicious traffic from legitimate traffic. Some of the popular types of application-layer DDoS attacks are HTTP Floods Attack, Slowloris, among others.

A. HTTP Floods

This attack is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial of service. This type of attack ranges from simple to complex. Simpler implementations may access one URL with the same range of attacking IP addresses, referrers and user agents. Complex versions may use a large number of attacking IP addresses, and target random URLs using random referrers and user agents. The hacker utilizes apparently valid HTTP POST or GET queries to target a web server or an application in an HTTP flooding assault.

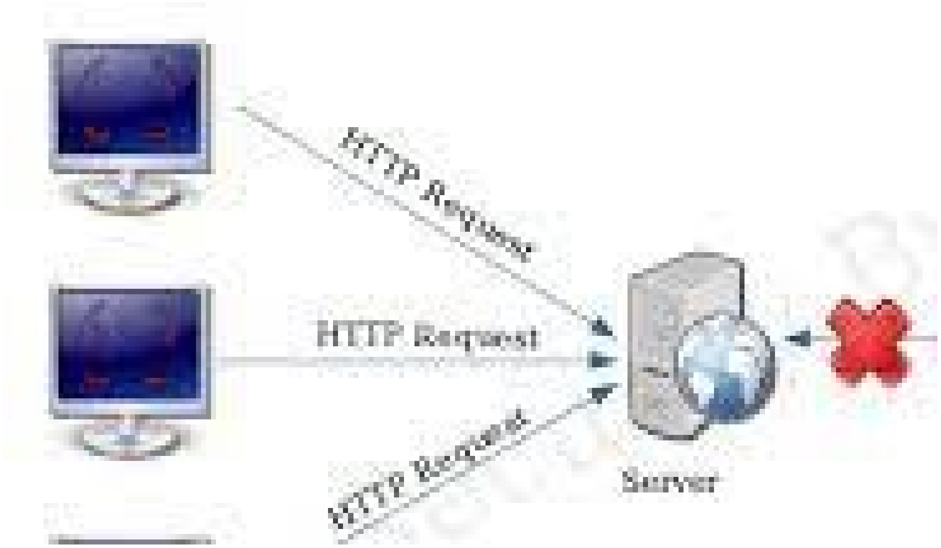

Figure 8: An HTTP Floods Attack

4. PREVENTIVE MEASURES FOR DDOS ATTACKS

When it comes to protecting the server from a potential DDoS attack, it's important to be vigilant from a proactive *perspective*. Some useful concepts to consider in the realm of DDoS protection include:

1. Use Of A Web Application Firewall (WAF)

A Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks.

2. Content Delivery Network (CDN)

Content Delivery Network (CDN) is a distributed network of servers that can efficiently deliver web content to users. A CDN store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

3. DDOS Mitigation Services

DDoS mitigation refers to the process of successfully protecting a targeted server or network from a distributed denial-of-service (DDoS) attack. By utilizing specially designed network equipment or a cloud-based protection service, a targeted victim is able to mitigate the incoming threat.

5. CONCLUSION

In a DDoS attack, a single host is targeted by many computer systems from various locations using multiple IP addresses. Hackers can shut down the victim services for a specific period of time using a DDoS attack, which can last for a number of days, weeks, or months, reliant upon the type of DDoS attack. DDOS attacks are designed to make a computer or network resource inaccessible to their authorized users. Despite the years of researchers coping with DDoS attacks, they continue to exist even with more intensity and have more impact. Different types of DDoS attacks as well as the motivations behind them have been discussed.

Detailed classification of DDoS attacks and their consequences have also been discussed. In addition, this seminar covers the defense approaches for the different levels of the DDoS attacks as well. It is concluded that the attackers can cause the following damage to the target: Economic loss to the victim since users will be unable to utilize services during the attack, Negative impact on the victim's future: the target would appear to have security flaws, causing customers to lose faith and If user information has been breached or the target failed to satisfy service-level agreements because of the attack, there would be a legal prospect, among others.

To avoid all these and more, implementation of proper countermeasures should be engaged to combat DDoS attacks which in this seminar paper we have highlighted some cutting-edge defense techniques which are currently being utilized to quickly defend against DDoS attacks to minimize the damage to the targeted web applications and its legitimate users.

REFERENCES

1. Chickowski, E. (2020). *Types of DDoS attacks explained*. Retrived from https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained/
2. Kime, C. (2023). *Complete Guide to the Types of DDOS Attacks.* Retrieved from https://www.esecurityplanet.com/networks/types-of-ddos-attacks/
3. Kime, C. (2023). *How to Prevent DDoS Attacks.* Retrieved from https://www.esecurityplanet.com/networks/how-to-prevent-ddos-attacks/
4. Lutkevich, B. (2021). *distributed denial of service (DDOS) attack.*
5. Retrieved from https://www.techtarget.com/Search Security/ definition/distributed-denial-of-service-attack/
6. Nagathan, M. (2023). *What is Web Application?*Retrieved from https://www.educba.com/ What-is-Web-Application/
7. Pedamkar, P. (2023) *What is DDOS Attack?* Retrieved from https://www.educba.com/ What- is-DDOS- Attack/
8. Rouse, M. (2022). *Web-Based-Application.*Retrieved from https://www.technopedia.com/definition/26002/Web-Based-Application/
9. Velimirovic, A. (2021). *How to Prevent DDoS Attacks.* Retrieved from https://www.phoenixnap.com/blog/prevent-ddos-attacks/