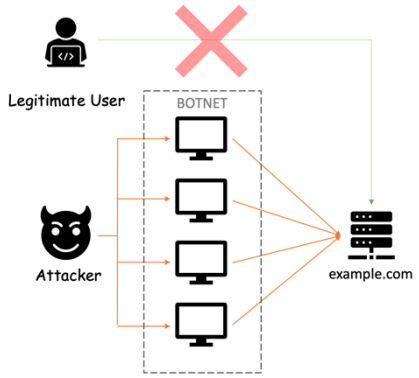
What is Distributed Denial of Service [DDoS] ?



It is an attack towards the service that is exposed via the Internet to deliberately make it unavailable for legitimate users.

How DDoS attack is performed?

By overwhelming the target service by sending a larger number of packets from the malware-infected devices.

So that legitimate user is blocked.
[no resources available at the target service to process the request from legitimate users]

What kind of devices are used as the sources of the attack?

BOTNET !

The group of malware-affected devices is called as BotNet.

! ! ! **Quick Mitigation** ! ! ! => Scaling up services

One can say that, in the cloud computing world, resources are unlimited. We can keep scale our services horizontally to make it available for legitimate users.

True! => This is one of a mitigation techniques.
But unlimited resources do not come for free. More the computing resources we utilize the more we have to pay!

It is that 'easy' to perform DDoS attacks?

Yes!

A person who wants to perform the attack need not be a geek in all technologies that are used in the product, he just needs to have some basic knowledge on ways to perform the attack. If security is not considered as part of our service development, then it is hard to mitigate such attacks.

Who would be interested in such attacks?

- Criminals 😡 who would demand money once they were able to attack successfully. => not to perform attack again/to stop the attack.

[no guarantee that they will not attack again once they are paid, so don't pay instead start gathering information to take legal actions against them]

- Thrill-seekers 😎 who wanted to prove that they have the entire power in the world to stop your business.

- Angry customers [or] ex-employee 😠 of the company who is not in alignment with your business policies.

!!! Popular Attacks !!!

"Mirai"

This attack takes a simple route.

#1 With the help of malicious affected devices, it scans for the IP addresses of IoT devices on the Internet.

#2 Try to establish a connection with the default username and password that comes with factory settings of the IoT devices.

#3 Then inject malicious software into the vulnerable IoT devices and turn it into weapons for attacking services.

How to mitigate attacks like "Mirai"?

First and foremost thing, change the default password to something that is difficult to crack.

... + maintain a whitelist and blacklist of IP addresses.

"IP reputations"

=> use IP blocklists to block known bad guys.

"A chain is as strong as its weakest link"

In today's world, most of our systems are distributed and involves multiple services.

Attackers would be interested in finding the weakest service(s) in our product to which they can perform the attack.

The DDoS attacks are classified based on the nature of the attack and surface area of the attack.

Common Types of Attacks

- Infrastructure Layer
  - Network and Transport Layers
- Application Layer
  - Application and Presentation Layers

Examples of Infrastructure Layers Attack

- SYN Floods => Transport Layer
- UDP Reflection Attacks => Network Layer

Examples of Application Layers Attack

- HTTP floods => Application Layer
- DNS query floods => Application Layer
- TLS abuse => Presentation Layer

⚒ Anatomy of SYN flood attacks ⚒

To understand what is SYN floods attacks in transport layer, we should be familiar with the basics of TCP connection flow.

Basic: TCP is a transport layer protocol that ensures reliable, ordered, error-checked delivery of streams between applications.

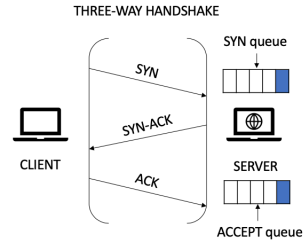
We'll be going to cover the concept related to SYN flood attacks here.

TCP Connection Management

TCP is a stateful protocol. i.e. Both sender and receiver need to maintain states about each other to exchange data.

TCP performs three-way handshake mechanism to establish a connection.

The connection state should be 'ESTABLISHED' at both sender and receiver side to initiate the data transfer.



🤗 THREE-WAY HANDSHAKE 🤗

When the 'SYN' packet is received from the client to the server, the client context is put into the **SYN queue** by replying 'SYN-ACK'.

Upon receiving 'SYN-ACK', the client responds with 'ACK', then the server marks the connection successful by putting the client context to the **ACCEPT queue**. The connection is ready for data transfer now 😍

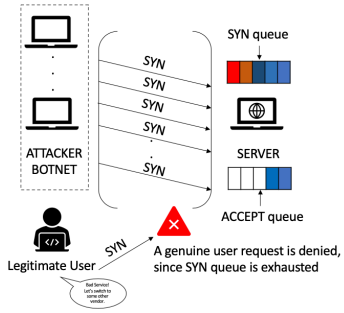
This is required as part of the sequence number synchronization process.

The sequence number is the one that ensures no packet loss and reordering concepts.

What happens in the SYN floods attack case?

Attacker's BotNet would keep sending SYN requests, but will not respond to the SYN-ACK request which results in SYN queue exhaustion at the server-side.

Note: The legitimate user would be denied that could result in customer loss for the service provider.



Anatomy of UDP reflection attacks

Basics: The UDP is a transport layer protocol.

- It is an unreliable and connectionless protocol.

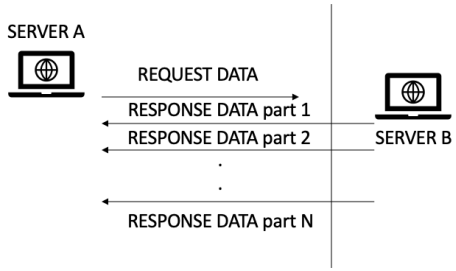
That means no connection establishment is required before starts transferring the data (unlike TCP).

This attack exploits the nature of the UDP mechanism at the network layer. That is why it is classified as a Network Layer attack. We'll see how!

Normal UDP Flow

We have seen that UDP is a stateless protocol. So the flow would look like this.

- Server A asks for DATA by sending a request. Then Server B starts responding with requested DATA to the Server B.



Loop Hole - IP Spoofing

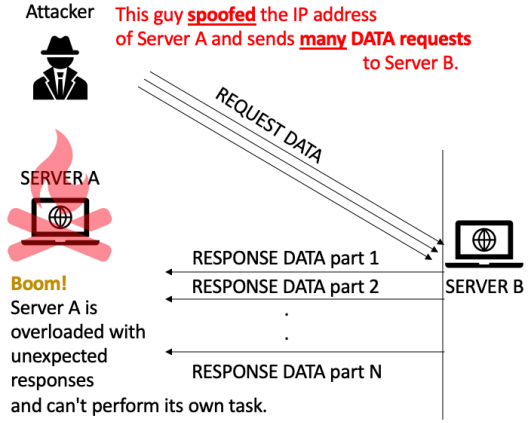
What is IP spoofing?

It is a method in which a system sends UDP packets (requests) to servers with a fake IP address.

'fake IP address' ?

Yes, address other than its own IP address. **So what ?**

PROBLEM



⚒ Anatomy of HTTP attacks ⚒

As compared to other attacks, this looks a little straight-forward.

We use Facebook, we use a sports tracker app like Cricbuzz, we use weather forecast app and many more.

Almost all of the services that we are interacting in day-to-day life are built on top of the HTTP protocol.

Damn Sure! You have experienced this.

Have you ever wondered why did a website ask us to confirm that we are not a robot?

- just like me!

It is meant to identify whether requests are coming from a genuine user or group of robots [Botnet]

Remember "Mirai" ? 

The mechanism behind HTTP attacks!

#1 What if I run a script that triggers infinite 'refresh' action against a website?

#2 What if I keep clicking a link to the home page of a particular site? Like this many triggers!

You might be guessing right now, yes! It floods a lot of HTTP GET requests to a web-service. *And attackers are smart enough to stress the cache also!* That could cause service to go unavailable as all resources might be allocated to my script [Botnet]. 😱

⚒ Anatomy of DNS query floods attacks ⚒

Basics: 📝

DNS is the phonebook of the Internet.

- Humans access information online through domain names, like nytimes.com or espn.com.
- Web browsers interact through Internet Protocol (IP) addresses.

Turning domain names into an IP address

- E.g. google.com => 19.3.2.15

Subdomains in DNS

Subdomains are prefixes to domain names that allow administrators to provide different web services to users but do so using the same namespace so that it is easier to remember.

e.g.

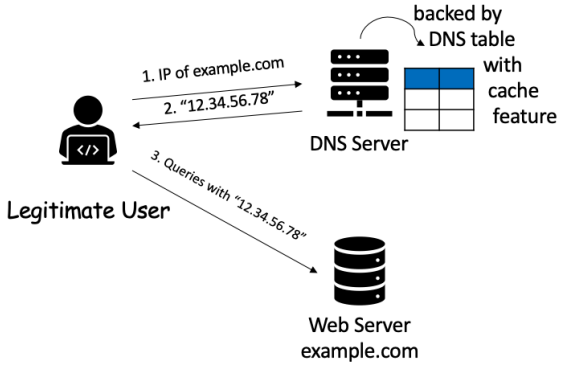
example.com => domain

mail.example.com => subdomain that points to mail server

contacts.example.com => subdomain that points to contact details to a particular organization.

DNS Flow

DNS Cache: to serve the user faster with cached records of recently visited domains.



To expose our services to the public, we all would need to integrate DNS into our product. Unfortunately, that is considered one of the weakest links in the chain for the DDoS attack. An attacker would try to send many well-formed DNS queries by changing subdomains frequently [to bypass cache] so that our DNS server gets exhausted with resources.

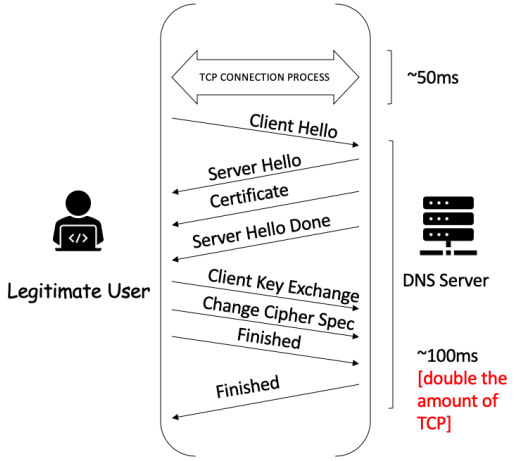
Albeit resources of DNS server get exhausted, will eventually legitimate users can't access our services since they won't get IP addresses for our service.

⚒ Anatomy of TLS/SSL abuse attacks ⚒

Secure Socket Layer [SSL] is a cryptographic protocol that is to provide security over internet communication. => HTTPS

Conceptually, SSL runs above TCP/IP, providing security to users communicating over other protocols by encrypting communications and authenticating communicating parties.

SSL Flow



SSL attacks

It is popular because each SSL session handshake consumes 15 times more resources from the server-side than from the client-side.
[check the time consumption too in previous pic]

Attackers can also choose to attack the TLS/SSL negotiation process.

By sending unintelligible data !

Multi-vector Attacks

Of course, since the goal of the attacker is to make the service unavailable to other users, the attack can be a combination of the different types for multi-vector attacks

It could be a combination of attacks such as SYN floods, UDP reflections, DNS query floods, HTTP(S) attacks targeting one or more weakest links of our services.

Attacks are not only performed by a single Botnet.

It is performed by a group of botnets [cluster].

In most cases, it is clusters of botnets.

That makes it more difficult to detect and mitigate the attack.

We have seen a few examples of DDoS attacks. How to detect that there is an attack against our services?

This is a great challenge, right? We observed all traffic comes to our service is well-formed ones. It is really hard to differentiate good and bad traffic! But that is the task we have to commit to ourselves in the first place to strengthen our system.

There is 'no one size fits all' strategy!

While preparing against a DDoS attack, our mindset should be like Arya Stark from Game of Thrones. 😜

"I know death (DDoS). He's got many faces. I look forward to seeing this one!"

On a high-level, detection strategy is classified into the following categories.

- Poll-based monitoring and detection
- Flow-based network parameters detection
- Network mirrors and deep packet inspection
- Anomalies and frequency-based detection

We would need to consider almost all detection strategies that are possible to keep fighting our war against DDoS attacks! All of these strategies to some extent, it relies on computing resources info such as bandwidth, CPU, memory.,. We'll explore a little more on each detection strategy from here.

› Poll-based monitoring and detection

Simple Network Management Protocol – SNMP

We would need a management system in place to poll SNMP query towards monitoring devices for CPU, packets per second, rate of packet loss. With these stats, we could guess if there is any unexpected resource utilization due to a DDoS attack by comparing stats with our sunny day scenario!

The limitation with this approach is, polling and pulling information itself would cause extra CPU cycles.

› Flow-based network parameters detection

push-based approach => FastNetMon is one of the popular tools.

Here in this approach, the required info would be extracted from forwarding tables and interface counters and aggregated in ASIC as 1 in N sampling and would be sent to the exporter and then to the collector. Then the analysis is done to detect the DDoS attack. This approach is much faster compared to SNMP, credits to features like TCAM.

The limitation of this approach is 1 in N sampling, the more the value of N, the lesser the accuracy.

› Network mirrors and deep packet inspection

In most cases, just looking at HEADERS of the packet is not sufficient, it is needed to inspect the packet in detail. With the emergence of SDN, machine learning, big data, and cloud, we could set-up a mirror network for our traffic, we can inspect each and every packet without affecting the original flow and then gather and store the required info that can train our machine learning model to find the attacks.

› Anomalies and frequency-based detection

This approach takes the information collected from the SNMP, flow, logs, and more sources and indexes it using tools like elastic search, then apply a machine learning model to detect the attacks.

There are chances that at the beginning it could detect some false positive cases but as time flies with more training, it becomes a very effective strategy to detect DDoS attacks.

Mitigation Strategies

Classified into two:

-> Proactive

-> Reactive

-> Proactive

Processing each packet in detail to detect the threat, and take actions.

- The advantage of this approach is very fast (real-time)
- The limitation of this approach is infrastructure costs, almost we have to map a monitoring device with mitigation tool one-to-one.

-> Reactive

Flow-based approach, gather information, aggregate, detect attacks, take actions.

- The advantage of this approach is that, cost-effective as compared to proactive.
- The limitation of this approach is that, not real-time, slow comparatively.

"I made a promise to defend the wall and I have to keep it because that's what men do"

When we say detect and define mitigation actions, what kind of actions we are talking about?

Actions are not magic that we need to perform but actions could be anything that we need to define to filter out the intrusion.

Action could be a set of

Network ACL, IP Tables & firewalls

that could provide facilities to define policies that can drop (or) accept the packets.

Actions could be a feature

"Anti-spoofing" & "BCP-38"

that helps in validating the source & destination IP address of the packet.

Actions could be a

Simple Tap settings => **rate limiter rules**

that could throttle the rate at which data are transferred from a particular source.

Actions could be the

NULL route in the BGP world

that would drop the packets => Remotely Triggered Black Hole.

And many more…

Thanks to the emergence of technologies like SDN and OpenFlow that would be very helpful in achieving these actions in a smarter way.

We have covered some basics on what is DDoS and types of attacks and some mitigation strategies.

But how do we do that all? I mean, setting up a system that can monitor, detect using artificial intelligence, and apply mitigate actions?

That's where DDoS appliances will come into the picture. Yes, there are specialized systems that could co-ordinate all these things for us.

These DDoS appliances come with both hardware and software variants.

Two kinds,

- on-premises
  &
- cloud-based

solutions.

We have to choose based on various factors like

- cost
- control
- scalability
- security & data privacy
- customization
- performance
- flexibility

and more!

Packets per Second is a very very important factor in the DDoS universe. As we know attacks are made using packet floods, so it is must that DDoS system should be capable of handling that many packets per second (millions of millions) packets per second.

From the management perspective, it is very important to have **event reporting tools** configured in real-time to learn about the system and its traffic pattern **and to alert** the customers.

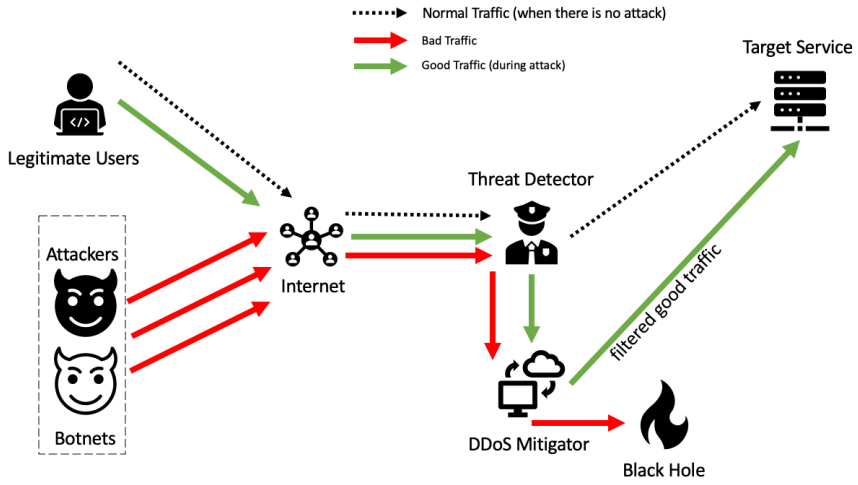
The growth of the internet is tremendous. **Data takes a long route** to reach the cloud from the originating device in-between that, there are many layers of the network infrastructure is involved. To detect a DDoS attack in case of a cloud-based solution, data doesn't need to travel all way through to the core data centre. Attacks have to be **mitigated as closer to the source** device. In that way, **we reduce a lot of stress** on our entire infrastructure. This opens up the DDoS discussion in **Edge Computing** aspects.

Consider exploring **hybrid solutions** if possible to mitigate DDoS attacks by mix and matching all those variants we discussed so far.

Additionally, instead of waiting for attacks to happen, we could take our defence to another level by allowing only IP addresses ranges that are supported in our region of business. Let's say if your area of business is in India (Asia-Pacific), then there is no point in allowing IP addresses from other regions.

It is highly recommended to take steps on improving (keep improving) the testbeds that can stress our DDoS system to make it trustworthy.
[when the situation really pops out]

Typical Flow of DDoS Systems



DDoS defence objectives

#1 Ensure availability to legitimate users.

#2 Prevent system from fail-over due to DDoS attacks.

If you change this order at any time (even in your dreams), then you would become a real mad king like in the GoT world.

The purpose of the DDoS mitigation strategy itself is lost if we prepare ourselves in reverse order, legitimate users only will get denied.

Happy fighting!