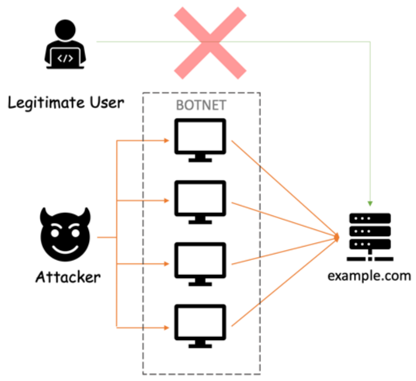
What is Distributed Denial of Service [DDoS] ?



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.

🤓

"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, 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.

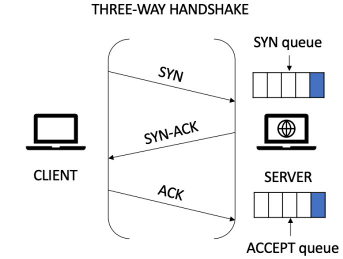
We'll be going to cover the concept related to SYN flood attacks here.

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 😍

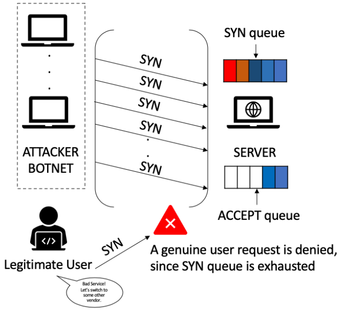
This is required as part of the sequence number synchronization process.

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.


ATTACKER
BOTNET
SYN
SYN
SYN
SYN
SYN
SYN queue
SERVER
ACCEPT queue
Legitimate User
SYN
A genuine user request is denied, since SYN queue is exhausted
Bad Service! Let's switch to some other vendor.