Daniel Rao

Jan 31st, 2020

Vince

TCP/IP from Pentester perspective

TCP/IP is the widely adoptive networking model that we use today. The TCP IP model basically consists of a set of rules set that govern the communication between computer networks over the internet. The standard for these protocols was developed in the 1970s and adopted as the protocol standard for our net in the early 1980s.

Alongside TCP IP which uses their architecture roughly in correspondence to the OSI reference model which provides a framework for the various protocols that compromise the suit. Most Network engineers refer to the OSI model when they are trying to diagnose or build a computer network.

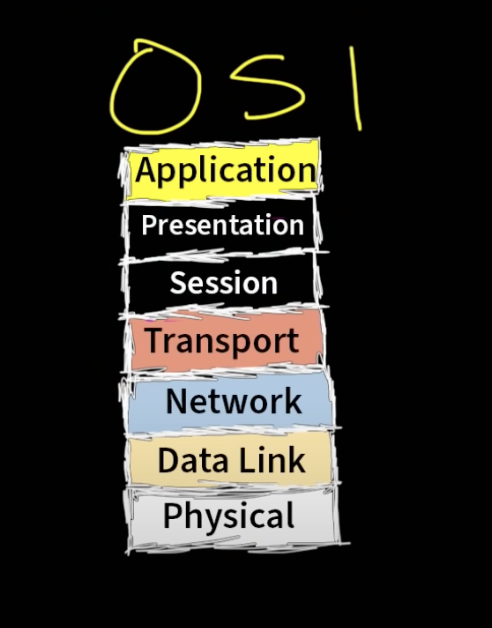
The internet and the TCP/IP are quite closely related to their history that it is difficult to discuss one without also talking about the other. They were developed together with TCP/IP providing the mechanic SIM for implementing the internet stop TCP/IP has over the years continue to evolve to meet the needs of the internet and also smaller private networks that use the same technology.

If we Look at the history TCP/IP was just one of the many protocols that was used to provide Network layer and transport layer functionality post-op as of today there are still other options for internet networking protocol Suites but TCP IP he is still universally accepted as a worldwide standard it's growth in popularity has been due to a number of reasons some of which are historical such as the fact that it tied to the internet as described what others are related due to some of the characteristics which are as follows:

1. **Integrated addressing system:** TCP IP includes within it a system for identifying and addressing devices on both small and large Networks the addressing system is designed to allow devices to be addressed regardless of their lower-level details how each constituent network is constructed (IP addressing). Over the time this mechanism has definitely improved to meet the needs of growing networks around the world. This type of addressing system ensures that each device has a unique address to refer to over the network.
2. **Design for routing:** TCP IP deals more with the connection between the networks then the connection between the devices. TCP IP routers enable data to be delivered between devices on different networks by moving it one step at a time from a network to another post-op a number of supporting Protocols are also included in TCP/IP to allow users to exchange critical information and manage the efficient information from one network to another.
3. **Underlying Network Independence:**  TCP IP operates primarily at layers 3 and above and includes Provisions to allow it to function on almost any lower layer technology including LAN’s, wireless LAN’s of various sorts and WAN’s of various sorts. This flexibility means that one can mix and match a variety of different underlying networks and connect them all using TCP/IP.
4. **Universality and scalability:**  as mentioned above TCP IP standard has been adopted by all networks on the internet. one of the other characteristics is that how scalable this protocol has proven to be. As over the years the internet has grown from a small Network to a few machines to huge internet work with millions of host, TCP IP has proven itself to be much more scalable although some changes has taken over the years to this protocol most of it remains unchanged from its core from what it was originally intended to do.
5. **Standards and developmental process:** the standards are freely available to the public. Furthermore the process used to develop TCP IP standard is also completely open. The TCP IP Protocols are developed and modified using a very Democratic process with all interested parties invited to participate. this ensures whoever is interested is giving a chance to provide an input to the development and also ensures that the world accepts these protocols Suites.

**OSI Model:**

Now if we look at it, most pentesters and network engineers refer to the OSI model as when they work together in teams. If we look at the TCP IP model it almost looks like it has been derived from the OSI model. Because of this reason let's try to understand the OSI model first.



The OSI model as shown above consists of 7 layers. These layers include:

1. Application (Layer 7):

This layer deals with human to computer interaction where applications can access the network. It provides protocols that allow software to send and receive information and present meaningful data to users.

A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

1. Presentation (Layer 6):

The presentation layer prepares data for the application layer. It defines how two devices should encode data, for example PDF, JPG, TIFF, XML or HTML, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

1. Session (Layer 5):

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends.

The session layer is responsible for 3-way hand shake and make sure the communication protocols are followed.

1. Transport (Layer 4):

This layer is kind of like what service we wanna use as we transport our data. The two main services include TCP and UDP where:

1. TCP: It's more accurate and reliable. This service is mainly taken into account when the server needs to send an HTML file on a GET request by the host. Another example could be the host trying to send an email over the internet. It's used to make sure that the other network receives the data. Therefore one sending of the packet and verification of receiving by the other network which makes the process slow.
2. UDP: This service is mainly taken into account when sending data for which its integrity does not need to be made sure by the other network. For example a regular voice call may lose some of the packets received by the other network or maybe even a video call does not necessarily need to be protected. Therefore UDP is more faster
3. Network (Layer 3):

Routers are layer 3 devices that operate only on IP address. This layer consists of IP address and port of the source along with IP address and port of the destination to which the communication is taking place.

1. Data Link (Layer 2):

Switches, WAP (wireless Access Point) and HUBs operate on this layer. These devices only understand MAC (Media Access Control Address). This type of address is also called burned addresses which helps to identify the device.

1. Physical (Layer 1):

On this layer devices such as ethernet or network cards come in. This is where the transmission of raw data takes place through cables.

**TCP/IP model:**

Now that we know the OSI model, understanding the TCP/IP model isn't very difficult as it's just the derivation of the OSI model as Mentioned above. The layers in the TCP/IP carry the exact same tasks as of the OSI model. The OSI model on the other hand makes it more distinct.

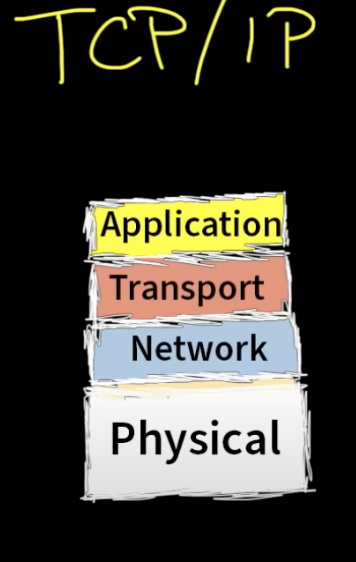
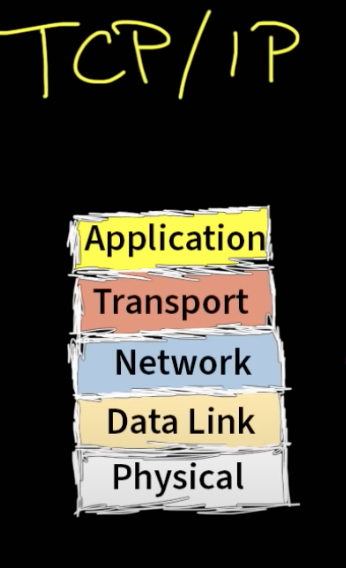
Most textbooks associate TCP/IP to be broken down into 4 layers which are

1. Application
2. Transportation
3. Network
4. Physical

In the above model the Application layer is thought to consist and perform the job of session and presentation. Some textbooks break down this model into 5 layers where data Link has a completely separate layer from the physical layer which was infused into one from the above model.

1. Application
2. Transportation
3. Network
4. Data Link
5. Physical

Below are the pictures of the two Networking model as described above:

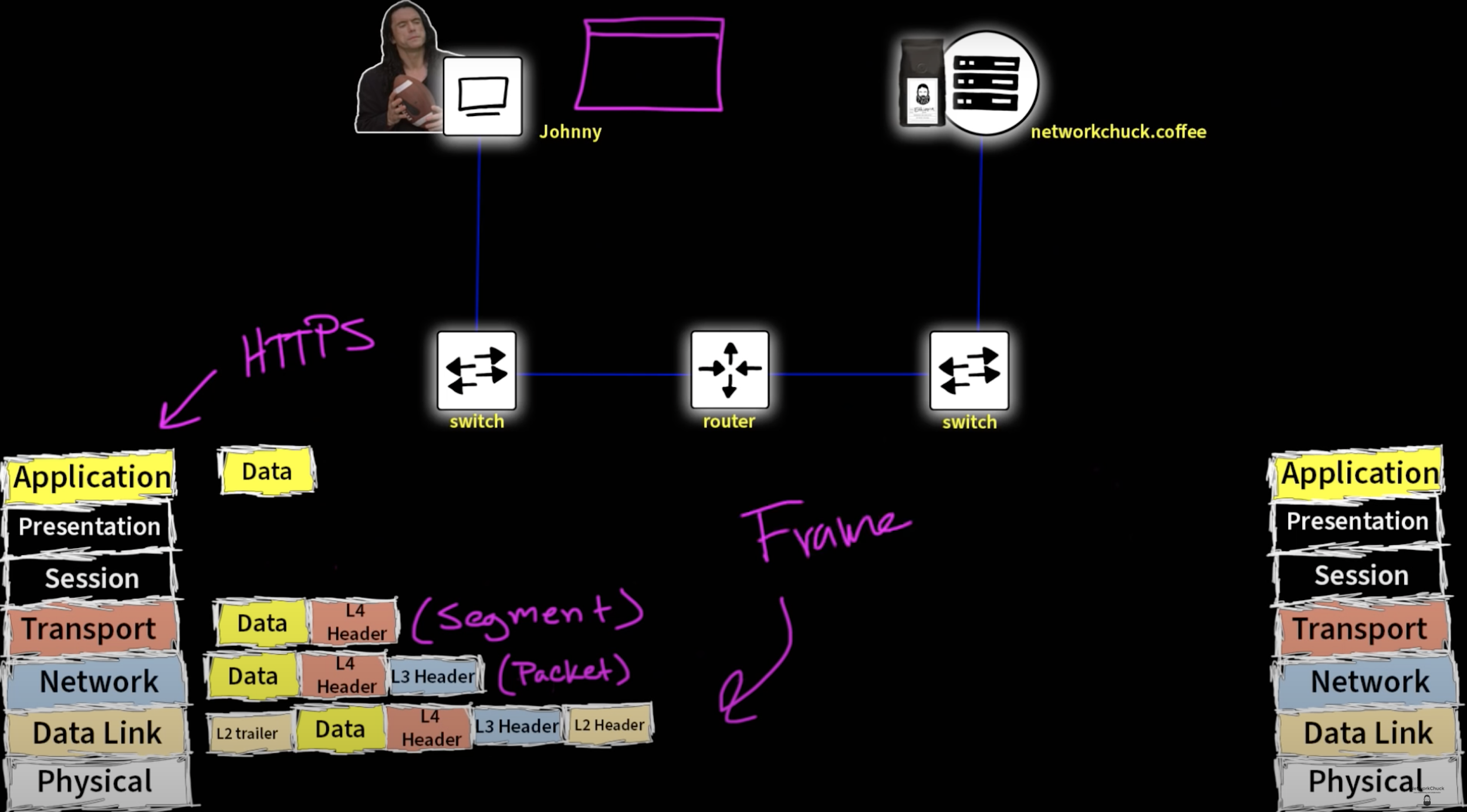
Now as a pentester we would need to know both the models to understand the flow of the data through the internet and how the communication is established. Now consider an example, Johnny wants to access the youtube server. If we disregard everything else and try to understand the communication in an isolated model it will be easier to understand how the communication takes place between the host and the server.

**Communication Flow:**

The get request first travels to the application layer. Say Bob typed the ip address of “youtube.com” Now we know that its a GET HTTP request. Therefore the data gets encapsulated inside a box. Now as we move down to the transport layer the data is put inside another header which tells us if the transport is going to be TCP or UDP. The data encapsulated here is named Segment Further we again encapsulate the data into another box and move further down the chain. Now that we are on the network layer, here we are referring to the ip address of the source and destination along with the port of both the host and the server. The data encapsulated here is named Packet. This is where we stick this to the layer 3 header and move further down. Now comes the Data Link layer. Here is where we need to know the source and destination MAC address, we keep further encapsulating the data inside the box. The data encapsulated here is named Frame. Now the data moves down to the ethernet cable which is the physical Layer.

On the other side the same model exists and the data there is being read starting from the physical layer of the server side.

The Server transports the frame to the Layer 2. Which consists of the MAC address. The switches point to the router MAC address which is at Layer 3 and when it gets to the router, the router points to puts it upto the Layer 4 which is the transport layer and than makes sure its either TCP or UCP message and than it further moves up to the Application layer which is layer 1 and finally the server learns about the request and sends the html file on TCP instead of the UDP as the data inside that needs to have integrity and than sends the video or content over UDP. And this process keeps happening as the session layer makes sures the connection is stable after the 3 way handshake. In the above scenario we completely disregarded the number of routers or switches it might have taken for a request to travel from the host to the server.



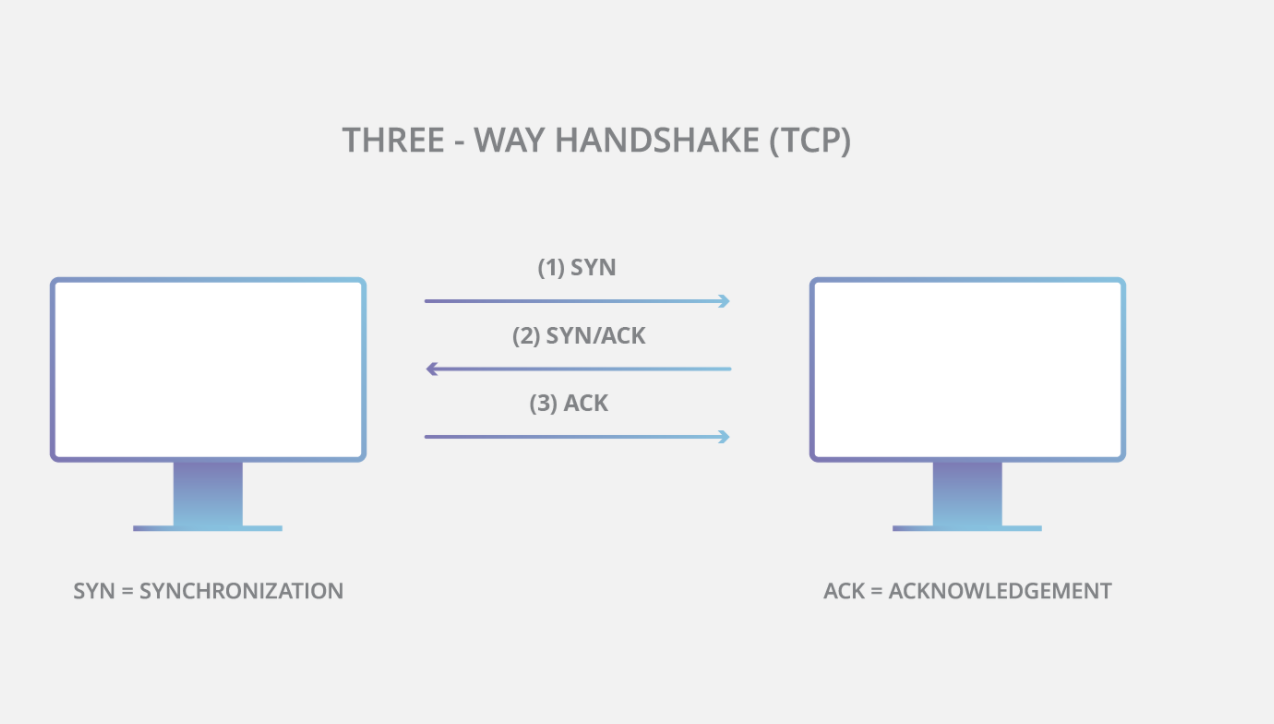
**3-way-Handshake:**

Now that we understand both the models it's very important as a pentester or a network engineer to know how the communication is established, how the transfer of data occurs and how the communication is maintained in a cycle. The job of most pentesters is to test the vulnerability in the network and using those vulnerabilities they try to exploit them using certain tools and methodologies. Some of the attacks that pentesters run on the system are syn floods.

According to a website, “a SYN flood (half-open attack) is a type of [denial-of-service (DDoS) attack](https://www.cloudflare.com/learning/ddos/what-is-a-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” (CloudFlare).

The attack is responsible to cause hefty damage to the business or brand by keeping the server busy or causing it to crash, therefore making the server unable to server legitimate client request.. These types of attacks are pretty common and hard to defend against. In order to fully understand how this attack works we need to first understand 3-way-handshake.

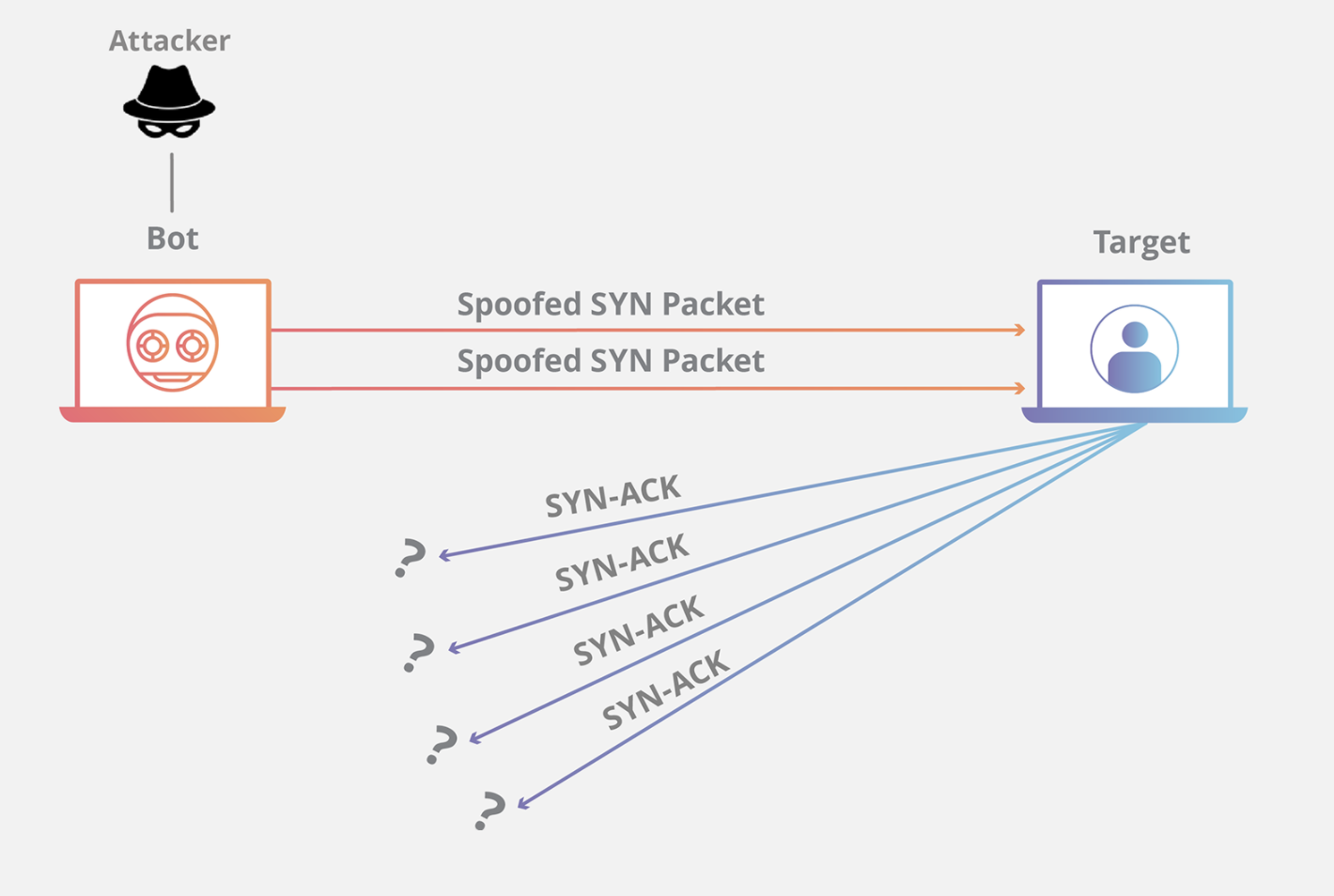
The diagram is provided on the next page.



The 3-way handshake takes place in 3 steps which are as follows:

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.

**Abusing 3-way-Handshake:**



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.

This type of attack may occur as direct attack, spoofed attack or distributed attack which is also known as DDoS attack. Thus this proves that it is very important for a pentester to know this knowledge and the tools required to perform a successful pentesting into the computer network.

**Citation:**

[*https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/*](https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/)