SYN Flooding

Understanding and Mitigating SYN Flooding Attacks

Emmanuel EliasUF Electrical Engineering

EEL4598 - Computer Communications

Gainesville, Florida

[emmanuel.elias@ufl.edu](mailto:emmanuel.elias@ufl.edu)

Garrett Bowman

UF Electrical Engineering

EEL4598 - Computer Communications

Gainesville, Florida

[garrettbowman@ufl.edu](mailto:garretbowman@ufl.edu)

Andoni AlfonsoUF Electrical Engineering

EEL4598 - Computer Communications

Gainesville, Florida

[andonialfonso@ufl.edu](mailto:andonialfonso@ufl.edu)

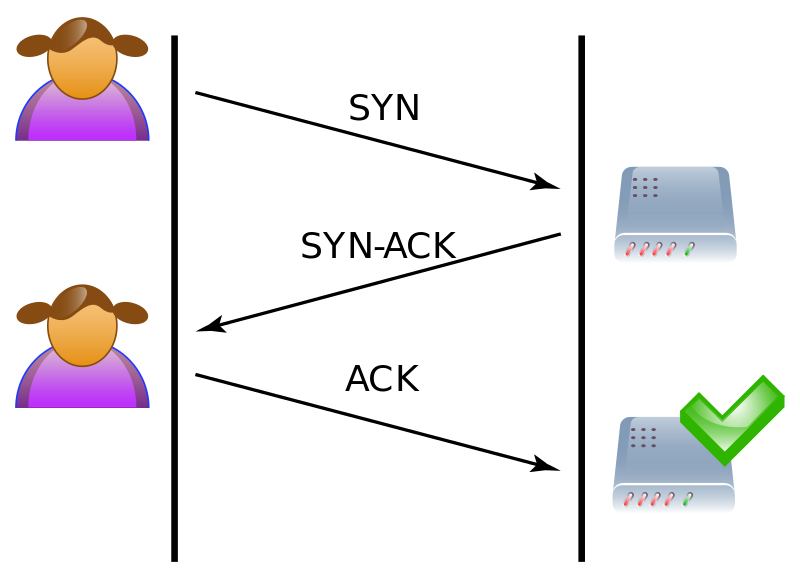
***Abstract*— As we fortify our digital fortresses against cyber threats, a comprehensive understanding of SYN flooding attacks and how to mitigate them is vital to keeping us safe from bad actors.**

***Keywords—SYN Flooding, Cybersecurity, Computer Communications, TCP***

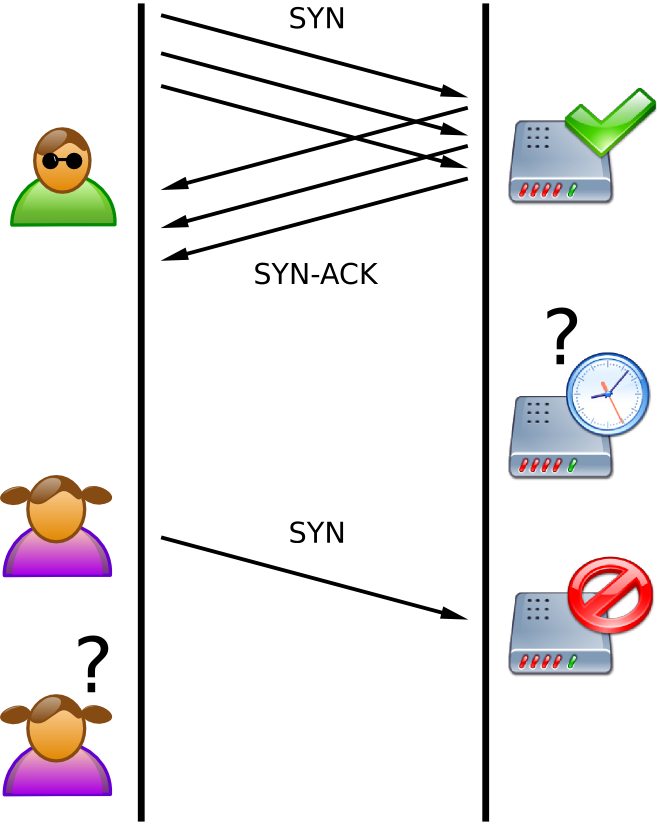
# What is SYN Flooding?

1. *Overview of SYN Flooding*

Transmission Control Protocol, or TCP, typically connects to a server by sending a connection request with a synchronize, or SYN, message. After the server acknowledges the request, it sends back a sychronize-acknowledge, or SYN-ACK, message. Finally, an acknowledge, or ACK, message is sent back to acknowledge, finally establishing a connection. This is what is known as a three-way handshake. An SYN flood is a denial of service attack that sends thousands of spoofed requests to connect that are meant to overwhelm the server. As the server tries to send back the numerous amount of SYN-ACK messages, because there is nothing there to receive them, the server could eventually even crash.

[](https://en.wikipedia.org/wiki/SYN_flood)

***Fig. 1.***  *Diagram of a typical three-way handshake connection*

[](https://en.wikipedia.org/wiki/SYN_flood)

***Fig. 2.***  *Diagram of how an SYN flooding attack typically looks*

Fig. 1 shows A demonstration of how a user can connect to a server. First, an SYN message is sent. After the server acknowledges the requests, it returns a SYN-ACK message. Finally, the user responds with an ACK message, establishing a connection.

Fig. 2 is A demonstration of how a SYN flood attack works. First, after the attacker sends a numerous amount of packets, the server tries to respond with several ACK messages. Because the server does not receive the corresponding ACK messages. A typical user will try to establish a connection like normal, but because it is consuming resources to deal with the SYN flood, it is unable to.

1. History of SYN Flooding Attacks

One of the most famous SYN flood attacks, and one of the first DDoS attacks in history, is the Panix incident in September of 1996 [7]. Panix is New York’s oldest commercial Internet provider.

While we do not know how specifically long it took for the attack to be identified, a DDoS attack on this scale can be noticed quite quickly, especially if the intent is to cause mass disruption. The perpetrating hacker had not seemed to be identified, or at the very least, not publicly disclosed. While not officially confirmed, it is speculated that the attack was regarding the recently installed system for email blocking at the time [5].

This attack caused Panix to be shut down for a week, affecting thousands of users and companies to Internet access [8].

Another well-known attack using SYN floods is the WikiLeaks attack from 2010. As WikiLeaks was releasing leaked information regarding US embassy cables, they were hit with a DDoS attack by a group of hacker activists, or hacktivists, that were trying to take them off the Internet. One of their main methods of attack was using SYN floods to slow down the leaks [9].

There are multiple other attacks involving SYN floods, such as the Yahoo! one in 2000, the Boston Bomb Scare in 2007, and the ransomware attack on the University of California, San Francisco a few years ago in 2020.

1. Difficulty and Defense of SYN Flooding

Although there are many reasons that defending against an SYN flood attack can be difficult, some major issues include the large volume of traffic, how fast the attack can occur, and the spoofed IP addresses. Due to the amount of SYN packets that occur, a high volume of traffic is created, causing the network to be overwhelmed. Hackers are able to execute this type of attack quickly, making it harder for any protection in place to respond in a timely manner. With spoofed IP addresses being used, it makes finding the origin of the attack and how to block traffic efficiently difficult.

Some counteractions may include limiting the rate of SYN packets and implementing instructions prevention systems, or IPSs, and firewalls. By limiting the rate of SYN packets, one can prevent an excessive amount of connection requests from a single source. Installing IPSs and firewalls can also help prevent an SYN flood from occurring, by helping filter traffic and being to detect things, such anomalies, such as the sudden appearance of requests.

# How does the attack work?

## Mechanics of SYN Flooding

A SYN flooding attack works by repeatedly sending SYN packets to a client in an attempt to slow down or shut it down completely. The attack works by exploiting the three way handshake process of a TCP connection. The TCP three way handshake works by the client first sending a SYN packet to a server and then the server will open a connection on a port and then will send a SYN/ACK packet back to the client to establish communication. Finally, the client will respond with an ACK and the handshake will have been completed. A SYN flood will exploit this handshake by continuously sending the SYN packet to a server but then the attacker will fail to send the ACK packet that is supposed to follow after receiving the SYN/ACK packet from the server. This leaves a half open connection on the port of the server [1]. After enough half open, service on the server will begin to slow down and eventually service will be denied.

The attack will occur on OSI Layer 4 which is the transport layer [2]. This is because the transport layer is responsible for network traffic between a client and a server and it will ensure complete data transfers. For the transport layer in a TCP connection to ensure a complete and correct data transfer, a TCP connection uses a three-way handshake process that was described previously, and the exploit occurs here.

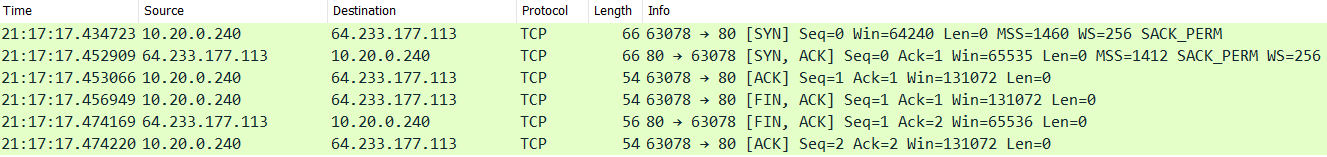
The packets involved in a SYN flooding attack are the SYN, SYN/ACK, and ACK packets. The packet used for the attack is a SYN packet which is short for synchronize, and it is a TCP packet sent to another client or server which requests to establish a connection between them [3]. An ACK packet is sent in response after a SYN packet is received. ACK is short for acknowledgement and shows that the data has been received successfully [4]. If the original client that sent the SYN packet receives an ACK from the server, an ACK is sent by the client.

A SYN flood attack is performed by repeatedly sending SYN packets to clog up the ports of the server so that those ports will be waiting for an ACK packet from the client. The attacker will not send the ACK packet which will make it so that those ports will have a half open connection indefinitely and the server will be forced to waste resources. Enough of these half open connections will make it so that the server does not function as normal [1]. It is also likely that the attack will spoof the IP of the SYN packet so that the server sends a SYN/ACK packet to a random IP address which can help with the attack as well as making it harder for the attacker to be traced back to. This is called a spoofed attack which is opposed to a direct attack which does not use a spoofed IP. A distributed attack uses a botnet to quickly overwhelm the server and also makes it significantly harder to be traced back to the attacker. This type of attack may or may not be using spoofed IPs [1].

This is a very straightforward attack and does not take much time to implement. The most basic version of this attack can be implemented using the hping command on a Linux command line. Adjusting some settings on the command will allow you to exploit that TCP three way handshake [5]. To create a more effective attack that will completely deny service of a victim, it will require the assistance of a botnet. This is because a direct SYN attack is easy to defend against as the victim can simply block the attacker’s IP. If the attacker uses a botnet, blocking the individual IPs of each bot becomes much more difficult and it also becomes much harder to trace back to the attacker [1].

## Location of Attack in Wireshark

To properly show where a SYN flooding attack occurs, it’s necessary to show an example of a TCP three-way handshake. The handshake was captured using wireshark by using the tnc command in Windows PowerShell to establish a TCP connection on port 80 with google.com.



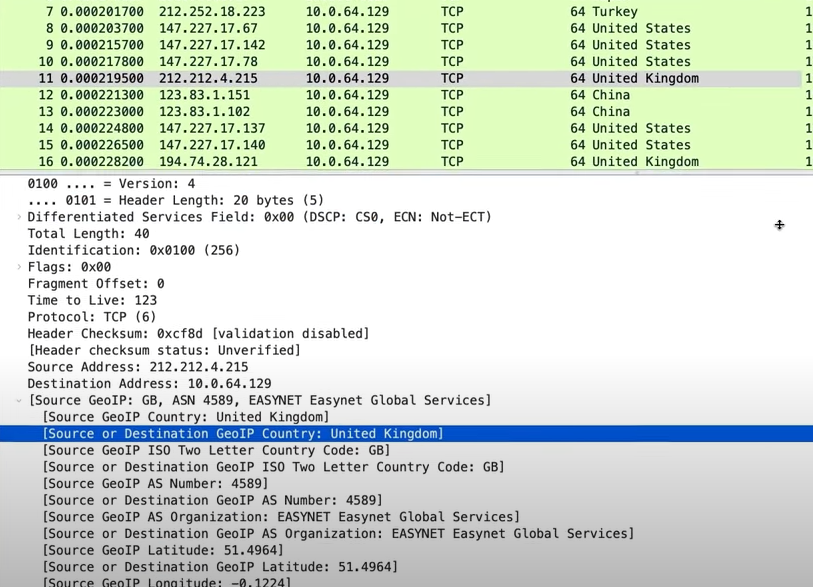
*Fig.1 Screenshot of TCP three-way handshake in Wireshark*

As shown in Figure 1, the handshake packet destinations are demonstrated. First, a SYN packet is sent to google.com and then google responds with a SYN/ACK packet. Next, the client will send an ACK packet in response to the SYN/ACK packet. This handshake is the location of the SYN flood attack. If the attack were to occur, the client would not send an ACK packet in response to Google's SYN/ACK packet which would cause a half open connection on one of Google’s ports. For a full denial of service, many more SYN packets would need to be sent to exploit the TCP handshake on as many server ports as possible.

# Using Wireshark to identify a SYN Flooding attack

If you notice your network starting to slow down or shut off entirely, you might be experiencing an attack. Using a program such as wireshark in order to distinguish an attack from normal network behavior can help us find a solution as quickly as possible. Wireshark is a widely used open source network protocol analyzer that allows users to capture and analyze network traffic in real-time. It helps diagnose network issues, investigate security incidents, and understand communication patterns within computer networks.

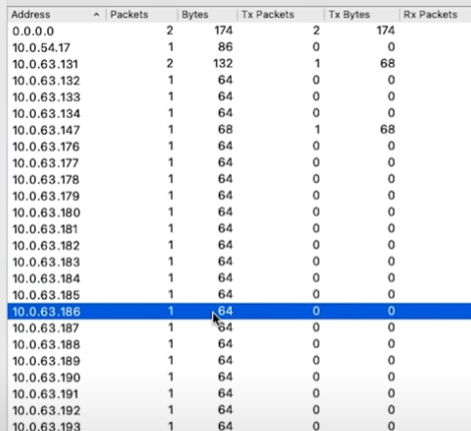
## SYN Flooding Detection using Wireshark

If there's a large number of incoming SYN packets that were not followed by corresponding ACK packets. Attempting to initiate connections without completing the handshake.  
 One way to identify an attack versus normal TCP usage is to look at the source addresses of the TCP packets. In wireshark, it is possible to import databases of known ip addresses and automatically label them based on location. One such database is GeoIP. Typically a business would get traffic from a certain demographic area so we can make assumptions that packets from countries we wouldn't normally do business with, we can mark them as suspicious.  


## Figure : The GeoIP labeling selected address as UK based

It is possible that people located in any country could be connecting to us but if we are getting lots of handshake request packets from out of ordinary locations that could be an indication of an attack occurring.

Another way to possibly identify an attack occurring would be looking at the endpoints menu.

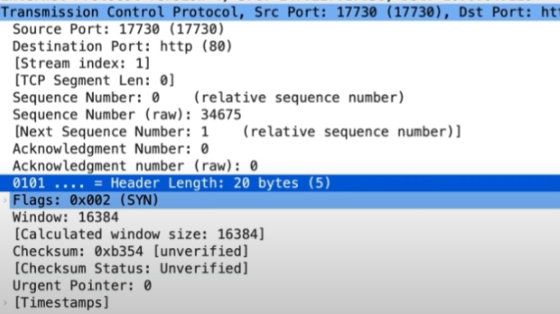


## Figure : Endpoint Menu in Wireshark

We can see that the vast majority of these incoming TCP connections are one single packet. This is most likely because these connections are not genuine and in fact an attempt to bog down our network. A genuine connection would complete the handshake more often than not which requires more than one packet.

## Contents of the Packets

There are things we can look for inside the TCP packets that can alert us of suspicious activity. The TCP section of the packet has many values that can indicate a new or spoofed system.



*Figure : The TCP section of a suspicious packet*

There are a few things to note about the TCP section of this suspicious packet. The most telling sign is a low sequence number. The sequence number is a 4 byte number so it could be up to 2^32 or 4294967296. The number being low means that the operating system is most likely a fresh install or new. This does not by itself prove this is an attack but it is something to note downfor sure.

The other telling sign is the header length being only 20 bytes. This is the minimum size for a TCP header and it is somewhat uncommon for a header to not contain any additional information, unless the attempt of the connection is simply to flood and bog down the network. Genuine connections would most likely have additional information in the header. A genuine user would, when initiating the TCP handshake, add in information as to what services they want to receive from our network which would make the header longer than 20 bytes.

## During and Post Attack Analysis

It is fairly straightforward to identify a SYN Flooding attack while it is occuring using a packet analyzer such as Wireshark, but, because packets are not recorded without a program like Wireshark running, it may be difficult to prove that an attack ever happened once it ends. If packets were recorded constantly, that would be a security risk in of itself.

##### References

1. SYN flood ddos attack | Cloudflare,

<https://www.cloudflare.com/learning/ddos/syn-flood-ddose-attack/> (accessed Aug. 9, 2023)

[2] “What is layer 4 of the OSI model?: Glossary,” A10 Networks, https://www.a10networks.com/glossary/what-is-layer-4-of-the-osi-model/ (accessed Aug. 8, 2023).

[3] “What is syn (synchronize)?,” Computer Hope,

https://www.computerhope.com/jargon/s/syn.htm (accessed Aug. 8, 2023).

[4] R. Awati, “What is ack (acknowledgement) in computer networking? – TechTarget definition,” Networking,

https://www.techtarget.com/searchnetworking/definition/ACK (accessed Aug. 8, 2023).

[5] “Procedure:,” SYN Flood attacks and its Detection. (Procedure) : Virtual Intrusion Detection Lab : Computer Science & Engineering : Amrita Vishwa Vidyapeetham Virtual Lab,

https://vlab.amrita.edu/?sub=7&brch=199&sim=365&cnt=2 (accessed Aug. 8, 2023)

[6] The New York Times, https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html (accessed Aug. 8, 2023).

[7] B. Sehrish, “Lightweight Statistical Approach towards TCP SYN Flood DDoS Attack Detection and Mitigation in SDN Environment,” ProQuest, https://www.proquest.com/docview/2625916480?parentSessionId=yPmO8f18hDOpgyqz75Rtlorw%2BmxkRqGdKf%2B3BDKOuSY%3D&pq-origsite=primo (accessed Aug. 7, 2023).

[8] E. Sullivan, Denial-of-service attack: plan on it, https://go-gale-com.lp.hscl.ufl.edu/ps/retrieve.do?tabID=T003&resultListType=RESULT\_LIST&searchResultsType=SingleTab&retrievalId=520fbf50-331f-4ca3-8fcd-16a615a7f925&hitCount=1&searchType=AdvancedSearchForm&currentPosition=1&docId=GALE%7CA18706982&docType=Column&sort=RELEVANCE&contentSegment=ZONE-MOD1&prodId=AONE&pageNum=1&contentSet=GALE%7CA18706982&searchId=R1&userGroupName=gain40375&inPS=true&aty=ip (accessed Aug. 8, 2023).

[9] C. Arthur, “WikiLeaks under attack: The definitive timeline,” The Guardian, https://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline (accessed Aug. 8, 2023).