



Expertise
and insight
for the future

Naran Upreti

DDoS Attack and Mitigation

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

25 April 2019

Author Title	Naran Upreti DDoS Attack and Mitigation
Number of Pages Date	36 pages + 0 appendices 25 April 2019
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Software and Networking
Instructors	Erik Pätynen, Senior Lecturer
<p>Distributed denial of service (DDoS) attack is a massive threat to the internet which has existed for decades now. Although various detection and defence mechanism have been developed in recent years, the volume of attacks is still rising on the internet. The DDoS attacks affect the service provided by the large companies and organizations on the internet targeting the financial and political entities.</p> <p>The purpose of this project was to understand the realm of the DDoS attacks. The main objective of this project was to study the three types of DDoS attacks which were found to be the most popular and effective DDoS attack in recent years.</p> <p>SYN flood attack, DNS amplification attack and NTP amplification attack are the leading types which are immense in size of the volume of traffic generated and account for more than two thirds of the DDoS attack incidents. In this project, a TCP-SYN flood attack using Hping3 is done in a secure environment to capture and analyze the packets for the testing purpose.</p> <p>The result of the SYN attack using Hping3 tools shows strong evidence that the DDoS attack can target the victim's server with a huge volume of traffic. It was concluded that the immense volume of traffic generated from the attack uses all the resources of the victim's server, and the flow of data between the service provider and the legitimate user is disrupted.</p>	
Keywords	denial of service, distributed denial of service, attack types, network security, vulnerabilities, attack detection and prevention

Contents

List of Abbreviations

1	Introduction	1
2	Motivation of DDoS Attack	2
3	History of DDoS	4
4	Botnets	6
4.1	Typical DDoS attack using botnets	7
4.2	Distributed Reflected Denial of Service attack	8
4.3	Types	9
4.3.1	Mirai	9
5	Perpetrators	12
5.1	Hacktivist	12
5.2	Cybercriminals	13
5.3	Government-sponsored groups	13
6	Types of DDoS attack	14
6.1	TCP SYN flood attack	14
6.1.1	Direct attack	18
6.1.2	IP spoofing attack	18
6.1.3	Distributed direct attack	18
6.2	DNS Amplification attack	19
6.3	NTP Amplification Attack	20
7	Methods of Mitigation	22
7.1	Mitigating TCP SYN Flood DDoS attack	22
7.1.1	End-Host Hardening	22
7.1.2	Network Hardening	24
7.1.3	Agent-based defence	25
7.2	Mitigating DNS amplification attack	25
7.3	Mitigating NTP amplification attack	26

8	Testing SYN flood attack	27
8.1	Hping3	27
8.2	Wireshark	27
8.3	Overview	27
8.4	Result	29
9	Conclusion	33
	References	34
	Appendices	

List of Abbreviations

ACK	Acknowledgement
APS	Availability Protection System
ATM	Automated Teller Machine
BBC	British Broadcasting Corporation
CEO	Chief Executive Officer
CNN	Cable News Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NTP	Network Time Protocol

OSI	Open Systems Interconnection
OVH	On Vous Héberge (French: We Host You)
PLATO	Programmed Logic for Automated Teaching Operations
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SYN	Synchronization
SYN-ACK	Synchronization-Acknowledgement
TCB	Transmission Control Block
TCP	Transmission Control Protocol
RST	Reset
UDP	User Datagram Protocol
US-CERT	United States Computer Emergency Response Team

1 Introduction

Along with the increasing usages and range of internet, web applications, websites, and server, a new type of internet attack have emerged which targets the availability of the internet service, and makes the flow of data between the service provider and legitimate destination. All these types of attacks are categorized as Denial of Service (DoS) attack. When a target is attacked by the collective machines together rising the size of the attack, the attack is acknowledged as the Distributed Denial of Service (DDoS) attack. All types of cyber-attack that make the legitimate end user unable to access the service from the provider is known as the successful DDoS attack. A successful attack can affect a company or a service provider on a large scale with the infrastructure, business, goodwill and its technical tolerance.

The main objective of this thesis was to study the various methods of attacks related to the Distributed Denial of Service. The various technologies related to the attacks and the types of device, software, and protocols combined to create the successful attack are studied and mentioned in this thesis. Along with the types of DDoS attack, a famous and effective one of them, Synchronization (SYN) flood attack was tested in a detailed simulator environment using Hping3 so that any reader could test it in a real environment for the good cause and protection.

The first, second and third section of this thesis cover the introduction of the topic, motivation of the attacker for the attack, and the numerous types of attacks that have occurred throughout the world respectively. The fourth section describes the term botnets, its types and the role in the attack. The fifth section describes the types of attackers on the internet world known as perpetrators and the tools used in attacks which are available online. The sixth section is all about the types of attack, whereas the seventh section consists of the mitigation process of these attacks. An environment is created in the virtual machine to create the SYN flood attack in the eighth section. The conclusion of the thesis is summarized in the ninth section.

2 Motivation of DDoS Attack

The main purpose and the clear motivation of DDoS attacks are difficult to understand. Distributed denial of service attack has become common types of internet attack, exponentially growing in number and volume of its type. The trend is growing towards creating greater impact throughout small time and sources. [1]

As it is already difficult to find the sources of these attack, and almost all the people behind the attack don't identify themselves, it is even harder to find the primary goal and motivation of the attack. Nevertheless, there have been several cases where the attacker leaves the note in the aftermath of the attack to fulfil their purpose [2].

Many people who are against the government also use the DDoS attack against the services provided by the government to release their frustration. In 2018, the DDoS attack was launched against the Finnish online identity verifying service Suomi(dot)fi. The websites of the Finnish National Insurance Institution (Kela) was hit by the attack, and the services were unavailable for the legitimate users. Along with this, the attack followed the website of the Population Register Centre and the police. Online service of several ministry websites like interior ministry, the ministry of education, the ministry of culture, the ministry of social affairs and health were also down following the attacks. As the ministry of defence used the different web structure for the website, the pages of these sites remained unaffected by the attack. Mikko Vuorikoski from Valtori said that in under any circumstances of the attack, all the traffic was programmed to be directed to the static sites for the service of the websites to remain functional. [3]

Due to the raised fuel price and the increasing cost of living in their country, Zimbabweans protest the government. Following the protest, Zimbabwean internet service was shut down by the anonymous group. After taking revenge on the Sudanese government, the anonymous group report to took down more than 72 Zimbabwe government websites. All these websites were DDoS'd by the group. It was done to create international attention towards the Zimbabwean government who were against the citizens oppressing them. A clear motive against that attack was to make the government learn the lesson. [4]

According to the research done by Kaspersky and B2B international in 2016, a company can compromise for up \$52,000 to \$444,000 due to single DDoS attack [5]. A group

named Phantom Squad sent out thousands of emails threatening the companies to pay a ransom. The threat was sent when the market share of bitcoin was on peak. They were demanding 0.2bitcoin for the security of the websites of the respected companies. This was the start of ransom DDoS attacks to make the small business structure compromise for their websites, and make the attacker collect ransom from multiple companies. However, Radware security researcher Daniel Smith told that the attack might not happen as that required vast resources which could not be achieved by the group who send out thousands of extortions letters [6]. Nevertheless, there has been the case when DDoS has been used for a large amount of money against the company. The attack happened until the websites become unusable making the service unavailable which can cause great loss to the company. The result is the company had to pay the ransom to restart their service [7].

A DDoS attack can also be launched for anti-competitive practice within the business. If the competitive websites are taken down by using the DDoS attack, the user or customers can be directed towards themselves launching the attack promoting the negative marketing against the competitor company and causing them a huge amount of loss. Former CEO of Lonestar, Babatunde Osho in January 2019 told that his company lost many of its customers to its competitors due to DDoS attack. According to Osho, the company has suffered substantial business value and loss in profit [8]. He stated that the attack was made between 2015 to early 2017 by Daniel Kaye against his company Lonestar. According to British Broadcasting Corporation (BBC) news, Daniel Kaye was jailed after he caused Liberian phone company to crash by attacking it using DDoS weapon Mirai no. 14 [9].

Primarily, attackers are motivated to DDoS'd the websites when they are against the ideology. Also, the feeling of the competition against the business model of other company and the feeling of releasing boredom by using pre-written scripts made the attack happen. Extorsion, cyber warfare against the company and government are the primitive goal of the attacker to cause DDoS attack.

3 History of DDoS

The first DoS attack occurred in 1974 when a 13-year-old student named David Dennis run the command called “external” on Programmed Logic for Automated Teaching Operations (PLATO), a shared learning computing system without any external devices connected to it causing the terminal to stop working and requiring the system to restart for functionality. The command was originally programmed on PLATO to interact with the external devices connected in the system. [10]

In February 2000, MafiaBoy, a 15-year-old hacker attack the main websites of the internet worlds like Yahoo, Amazon, eBay, Google, CNN, and others by overloading the servers and service with various types of traffic and communication. His main motive was to establish his and his cybergroup name in the market. The loss due to the attack was reported to be over a billion dollar. MafiaBoy was sentenced to jail for eight months by the Canadian Court. [11]

Structured Query Language (SQL) Slammer, a tiny malicious code of only 376 bytes managed to cause havoc in hundreds of thousands of servers in 15 minutes increasing the global traffic by 25% all over the world in mid-2003. The major impact was seen in South Korea where the DDoS attack leaves the country without internet and telephone service for several hours. Along with South Korea, 13,000 Automated Teller Machine (ATM) service of Bank of America was disrupted, and electricity supply for 50 million people in the Northern part of the United State of America was affected as a result of this attack. [11]

The largest DDoS attack occurred in February 2018 when an attacker targeted GitHub, a popular online code management service by amplifying the cache of the database system, and flooding it with the spoofed data request. This attack in GitHub created the incoming traffic in its server with the rate of 1300Gbps with the 126.9 million packet rate per second which is 1:50000 times amplified. A protocol named Memcached was abused, and the simple traffic was amplified in this attack. [10]

Kaspersky Lab, a multinational antivirus provider, and cybersecurity company provide information about the DDoS attacks defeated, its occurrence in various parts of world, types, and effects of the attacks in each quarter of the year. According to the report released by Kaspersky Lab in October 2018, the third quarter of 2018, there were not

many multilevel DDoS attacks on major resources. However, the total number of attacks has been increasing every year as seen in Figure 1 below.

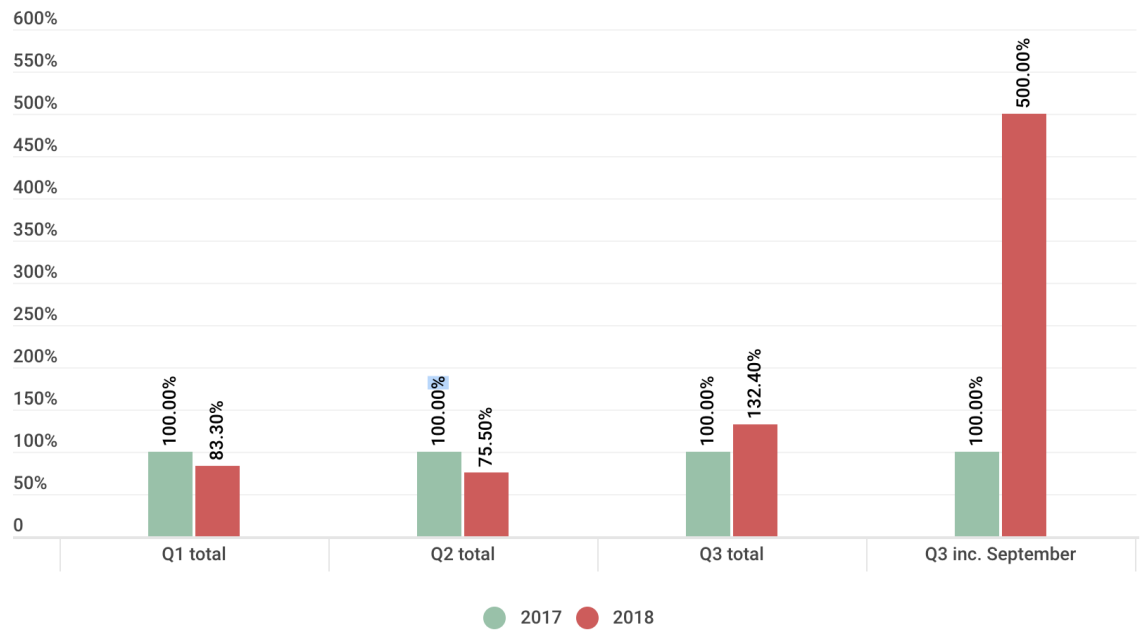


Figure 1. DDoS- attacks defeated by Kaspersky DDoS Protection in 2017–2018 [12]

Figure 1 above compares the number of attacks defeated by Kaspersky Lab in 2017 and 2018 quarterly. In the graph, 100% is the number of attacks that occurred in 2017 which is compared with the increased attacks in 2018. Compared to the quarter third of 2017, the attack has increased in September 2018. However, there was a noticeable drop in the number of attacks in the first and second quarter of 2018. [12]

In recent year, the number of DDoS attacks has increased in number, and its impact significantly. Hactivist and cybercriminals have now fully commercialized the DDoS attack for various reason. As long the internet is growing, an enormous number of Internet of things (IoT) devices are being manufactured, connecting and exchanging data with the internet, the attacker will find a new technique of DDoS attack.

4 Botnets

Botnets play a vital role in creating various types of DDoS attacks. Having basic knowledge of botnets and its working mechanism is crucially important to understand the types of attack. A logical group of computers and devices which are interconnected with each other running one or multiple bots, in a coordinated way for illegal or comprising purpose. An internet bot is programmed to run a pre-written automated script over the internet in an exponential rate which is impossible to perform with human alone. Botnets, derived from robot network, are also called the internet zombies which can be used to perform attacks on the internet, steal the data, send malicious programmes, and allows the attacker to access the information of the devices and its connections.

Botnets have been playing a vital role in DDoS attack since the evolution of this type. Bots allow the hacker or attacker to receive much information from the device and carry out desired actions. The motive of the botnet is to remain undetected, and to make the infected user unaware of the misuse of the device. Botnets used for DDoS can perform silently through the process until it receives a command from the attacker, or the main bot called bot-herder. [13]

Figure 2 below shows how the botnets are used and commanded by the attacker. The attacker controls the C&C server, initiate the attack leading the whole process creating havoc in victim service.

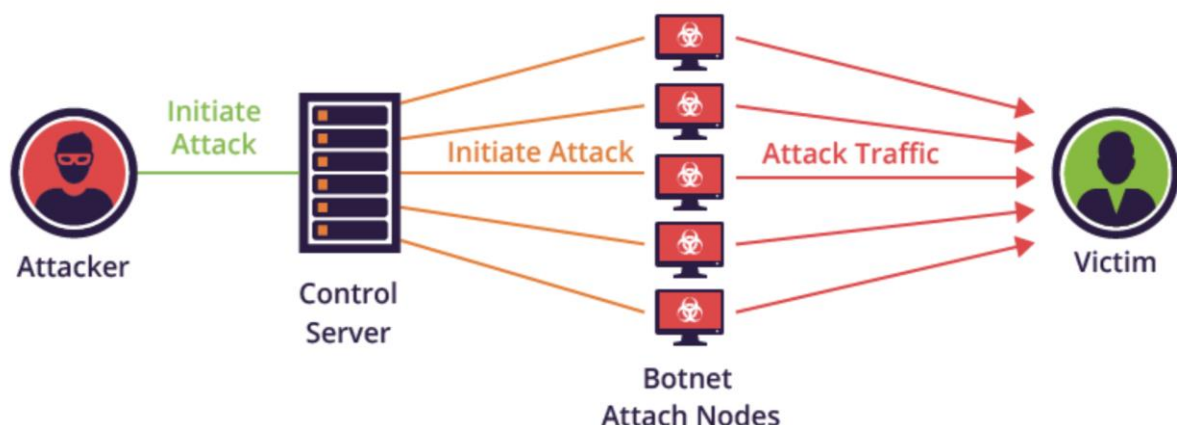


Figure 2. DDoS botnet [14]

Botnets are the most effective way to cause a DDoS attack. The distributed part in DDoS is for these botnets which are derived from multiple computers, and infected devices which makes the traffic produced in the attack to be distributed as from the multiple sources. As the botnets are the real devices or internet of things devices (IoT), having a real Internet Protocol (IP) address, it is almost inevitable to sort out the DDoS attack happening through the botnet's traffic. The attacker or the "bot-herder" send the information to the botnets, which activate the silently running programmes in a device to send the traffic to the predesigned destination address to deny the service of the server. The headquarter or the centre of the botnet is called command and control server (C&C). C&C server is required to relate to other bots for issuing the attack or updating its own attack tool. Cryptography technique is used to transmit a message during this communication to remain undetected. [15]

4.1 Typical DDoS attack using botnets

In a typical DDoS attack, the attacker sends a command to the C&C server, which then commands the hibernated bots to launch an attack to the victim with a large volume of packets flooding the victim with useless traffic, and degrading the performance of the system as shown below.

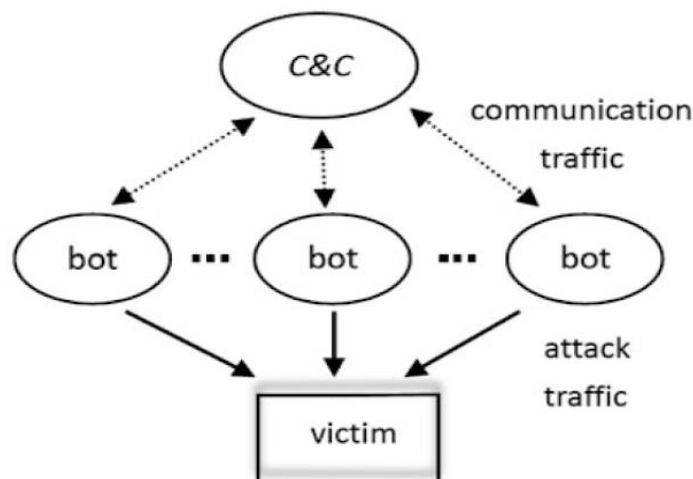


Figure 3. Typical DDoS attack [15]

Figure 3 shows the C&C server communicates with bots through encrypted traffic activating the bots to attack the victim by creating a large amount of traffic directly through the bot address.

4.2 Distributed Reflected Denial of Service attack

Unlike typical DDoS attack, Distributed Reflected Denial of Service attack (DRDoS) network contains reflectors along with C&C servers with bots as shown in Figure 3 below.

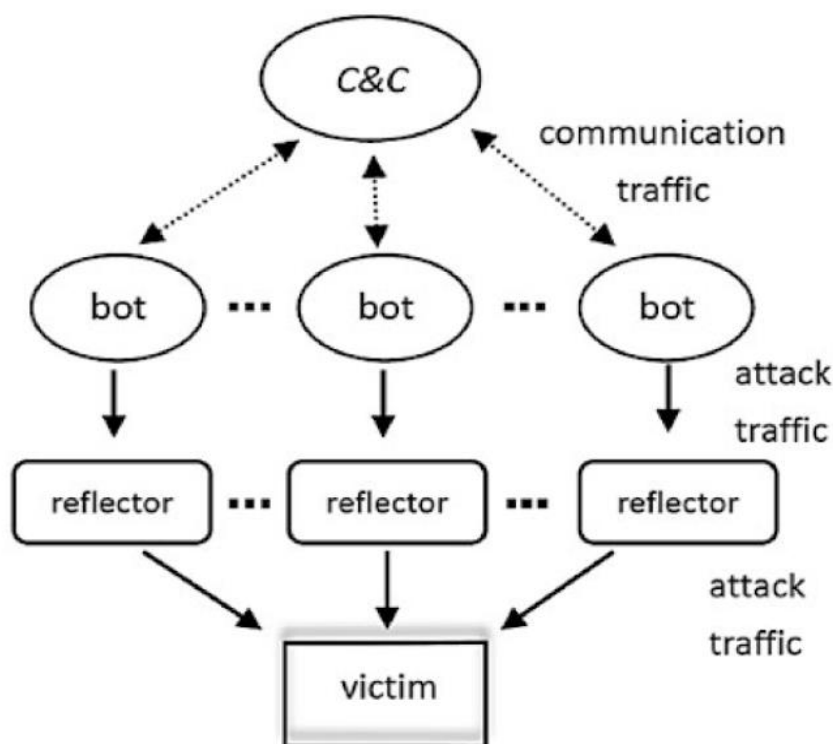


Figure 4. DRDoS attack [15]

Figure 4 shows that the DRDoS attack, the attacker controls the C&C server which controls the bots to launch the attack. Here, the bots send the traffic as the source IP address to the victim's IP address towards the other uninfected devices known as reflectors. The reflectors get the request from the victim IP address as a legitimate source which results in sending a large volume of traffic to the victim from the bots flooding its traffic, and taking down its service completely.

4.3 Types

As the security of the IoT devices has been developing and enhancing with the year, attackers have found their way out to surpass the security, and take control of the devices in various ways. Many botnets have been used in recent years to create and manage DDoS attack on a large scale. Some of them are Chalubo, Flusihoc, Nitol and Mirai.

Chalubo is a new botnet which was detected in late 2018 which used to compromise the poorly secured IoT devices. Chalubo focuses on targeting internet facing secure shell (SSH) servers in Linux based systems. Flusihoc is a versatile type of malware written in C++ which can make various types of DDoS attack as directed by C&C server. This botnet can create 9 types of DDoS attack which are Synchronization (SYN) Flood, User Datagram Protocol (UDP) Flood, Internet Control Message Protocol (ICMP) Flood, Transmission Control Protocol (TCP) Flood, Hypertext Transfer Protocol (HTTP) Flood, DNS Flood, CON Flood, CC Flood1 and CC Flood2 [16]. Nitol is the botnet mostly operated in China, which usually send the device performance data from the victim to the attacker by connecting malware to the botnet's C&C server through the TCP socket.

4.3.1 Mirai

Mirai is a malware which is capable of self-propagation that turns Linux running internet connected devices into bots to create large scale DDoS attacks. This botnet takes control of home routers and IP cameras to send traffic in an enormous amount to the victim. Mirai was named after the anime series Mirai Nikki. It was discovered by the white-hat security research group "MalwareMustDie!" in August 2016. Mirai came to limelight after it was used to attack KerbsOnSecurity.com, a popular security journalist blog, with the range of 620 Gbit/s. Mirai was also used to create a DDoS attack on another online service of On Vous Héberge (French: We Host You, OVH) server and Oracle Dyn. Ovh reported that the attack exceeds the largest public attack rate of 1Tbps. [17]

Mirai is based on the two-key module, replication module, and attack module. In the case of a replication module, Mirai malware takes control of insecurely connected numerous IoT devices. As Figure 5 below illustrates, the replication module report to the command and control centre to infect it with the updated Mirai Payload. [18]

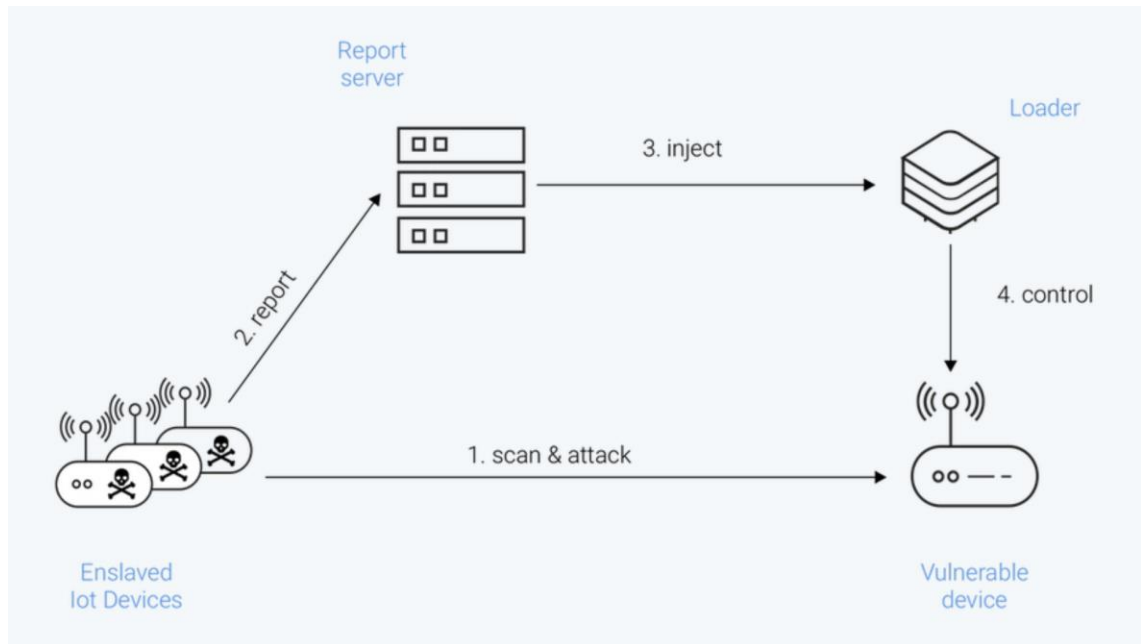


Figure 5. Replication Module of Mirai [18]

In this type of module, 64 most commonly used passwords by IoT devices are combinedly used. Elie, Elie reported that although the attack was not of high infrastructure, it took control of more than 600,000 devices by exploiting the default root password to log in. [18]

A DDoS attack is also made by utilizing an attack module of the malware. HTTP, UDP, and TCP flooding process used on DDoS attacks is implemented with the technique codes. Various types of the attack were made successful using this module such as application layer attack, volumetric attack, TCP attack. The process of the attack module can be observed in Figure 6 below. [18]

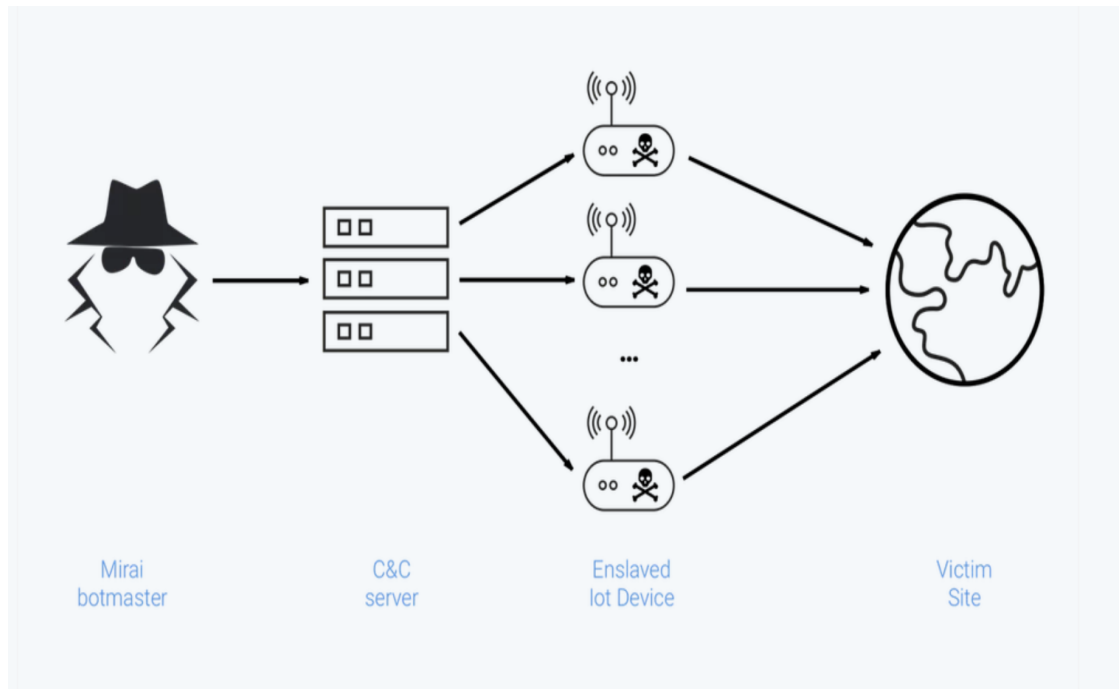


Figure 6. Attack Module of Mirai [18]

Figure 6 illustrates the attack module of Mirai botnet. The victims server is targeted with huge amount of traffic by collaborating C&C server and enslaved IoT devices.

5 Perpetrators

A person or group of people who perform harmful or illegal activities are called perpetrators. In general term, they are also known as hackers. Over the year, the profile of perpetrators and their motives have changed and evolved. In order to defend different types of attacks on the internet, it is very important to understand the changing profile and motives of those hackers. The more the cyber threat and security professionals understand the criminal terminology, and method of the attacks by the hackers, the service provided on, and through the internet is less vulnerable. Understanding these aspects also provides assistance in upgrading the infrastructure and security to the service providers.

Perpetrators or hackers can be classified based on their skills, working mechanism and types of attacks they perform. There are various types of hackers emerging in society. The classification of hackers can be seen from Figure 7 below.

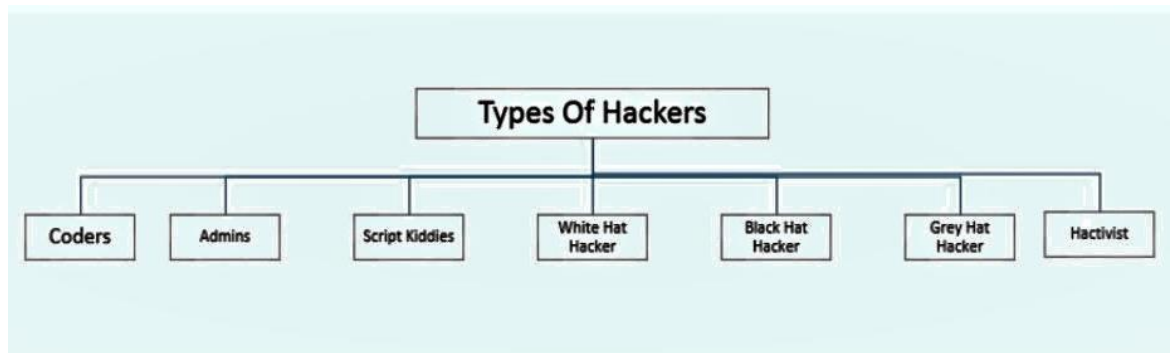


Figure 7. Classification of hackers [19]

The three main groups of perpetrators are the hacktivist, cybercriminals and the hackers who are hired to perform attacks known as a nation state attacks.

5.1 Hacktivist

Hacktivism is the perpetrators who are politically motivated to perform attacks on the internet to release or display social, political and religious messages or information to

the public. There are two types of hacktivism called cyberterrorism and freedom of information. Cyberterrorism includes the DDoS attacks created to defame the service provider whereas freedom of information is a type of hacktivism where hacktivists release the information to the public which is supposed to be kept private within the organizations or the government. Hacktivists generally rely on the tools available on the internet to create and perform the attacks which are mostly denial of service attacks. [20]

There are various types of tools available on the internet which can be used freely or at low cost to create a denial of service attack. Some of those also support to hire botnets to create the distributed denial of service attacks. These tools flood the targeted server to create a DDoS attack. Some of the freely available DDoS tools are LOIC (Low Orbit Ion Canon), HULK (HTTP Unbearable Load King), DDOSIM—Layer 7 DDOS Simulator, and PyLoris.

5.2 Cybercriminals

Attackers and group of the attacker on the internet whose motive is to make money using any means necessary are known as cybercriminals. Their main motive is to create a business by trading hacking tools, botnet service, programming code, and the secret information from their victims. These group of attackers have organization, and are often funded by them. They are responsible for causing havoc for various organizations and companies stealing billions of dollars from their victims every year. [20]

5.3 Government-sponsored groups

Attackers who are funded and organised by the government or the state of the nation are known as government-sponsored groups. Unlike other types of perpetrators, they design and program their own hacking tools to find the undiscovered vulnerabilities on the software and service. The attacks caused by these groups are almost impossible to detect as the attack tools and malware used in the attacks are particularly legitimate. Their target before the actual victim is the software company to authorise their illegal attack tools and malware to be authentic. The range of their victims is from average organizations to the government entities. [20]

6 Types of DDoS attack

DDoS types can be classified with the process of attack in which the attackers made the use of service unavailable. However, the study of DDoS cannot be complete without studying the process of how the internet works.

The Internet is a global internetwork of various computers and servers which has its unique Internet Protocol (IP) address. If a computer is connected to the internet through the Internet Service Provider (ISP), a temporary IP address is assigned to the computer during the internet connection within the dial-in session. Likewise, if the computer is connected to the internet using the local area network (LAN), the temporary IP address will be assigned through Dynamic Host Configuration Protocol (DHCP) server or a permanent IP address through LAN. Nevertheless, a computer is always assigned a unique IP address. [21]

Communication process on the internet is based on two end-points. Transmitting of the signal through one computer to another through internet happens using an ethernet cable, fibre optic cable, wireless fidelity (Wi-Fi) or mobile service provider along with the use of operating systems, applications, network hardware, and network card drivers. The signal from one device to another are transmitted through the seven layers of Open Systems Interconnection (OSI) model.

6.1 TCP SYN flood attack

TCP SYN flood attack is caused due to the drawback that comes with the “three-way handshake” of TCP connection sequence. In a TCP connection, an SYN request is sent to the host or server by the requester. The server acknowledges the request by replying with Synchronization-Acknowledgement (SYN-ACK) response to the requester. Then the TCP connection is established by replying the server with an Acknowledgement (ACK) response by the requester. After the TCP connection is established, the communication is open for the server and the client. In SYN flood attack, the requester sends numerous SYN request to the server but later does not respond to the server with ACK confirmation after receiving SYN-ACK request. Also, the attack can be done by sending the request from a spoofed IP address. In both scenarios, the server keeps waiting for

the acknowledgement of “three-way handshake” and its resources is used resulting in the server to deny all the new request of TCP connection. [1]

Imperva, a cyber-security and software company, said that the largest DDoS attack that it mitigated occurred in 10th of January 2019. This attack was so called SYN flood attack in which its client’s server received the request of more than 500 million packets per second. Imperva reported that the requested pace was faster than the processing speed of the server. Flood of normal SYN request and request from the spoofed IP address, and a port was sent to the client. [22]

In 2015, Imperva released a white paper about the top ten types of DDoS attack. According to the paper, a combined SYN flood attack is responsible for more than 70% of total large-scale DDoS attack. As shown in Figure 8 below, TCP SYN flood attack accounts for half of the total DDoS attack.

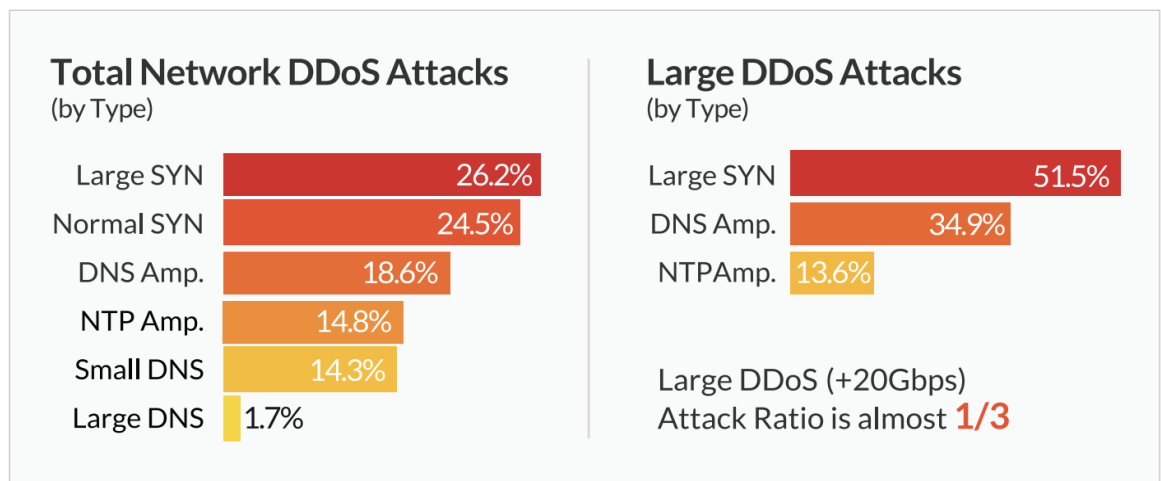


Figure 8. Comparison of types of DDoS attack by Imperva in 2015 [23]

A combined SYN flood attack contains two types of attack differentiated with the size of the requested packet. In a regular SYN flood attack, the server receives the request packet less than 250 bytes. In a large SYN flood attack, the server receives the request packet more than 250 bytes. The latter is the most common type of attack vector comprising more than 26% of the attack type. [23]

The Transmission Control Block (TCB) is a structure of transport protocol data which contains information about the information of the connection. The size memory footprint

of TCB varies from 280 bytes to 1300 bytes. When a TCP SYN request is received by the host or server, the SYN-RECEIVED state is established. This state indicates that the request is not validated for its legitimacy, and the connection is half open. Before the connection is completely established, TCB is allocated after the SYN request is received. When numerous SYN request is received by the host, multiple TCB is allocated with a high amount of data size in the kernel memory of the host or server. A backlog parameter is associated by the operating system as a countermeasure to prevent the kernel memory getting exhausted by the multiple numbers of TCBs. This parameter contains a socket that sets the limit in the number of TCBs created along with the SYN-RECEIVED state. Although the memory resource can be prevented from the attack, the backlog parameter itself accounts for the smaller resource of attack. As a result, the service is denied by the server as there is no room left in the backlog parameter. The main aim of a TCP SYN flood attack is to deplete the backlog parameter by sending the numerous SYN request filling it up completely. The legitimate TCP connection is denied by the host or serve as all the TCBs is stuck in the SYN-RECEIVED state multiple and relatively long time from the request received in the half TCP connection which seems to be reliable. The sequence of TCP SYN flood attack is presented in Figure 9 below. [24]

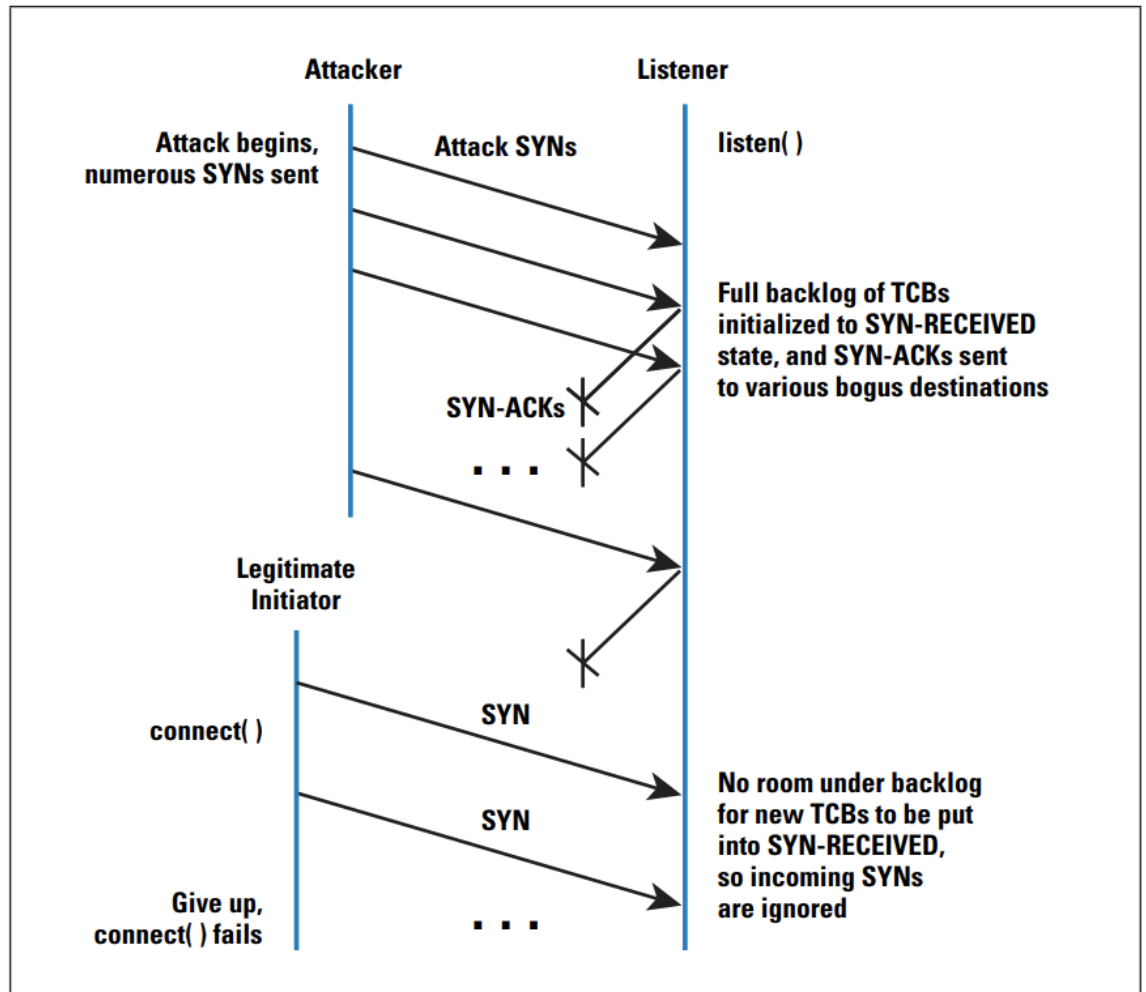


Figure 9. Attack demonstration of TCP SYN flood DDoS attack [24]

The method of TCP SYN flood attack method can be divided into three parts according to the variants of attack. The direct attack, an IP spoofing attack, and the distributed direct attack are the method used for this attack. Figure 10 below simplified the method of these attack.

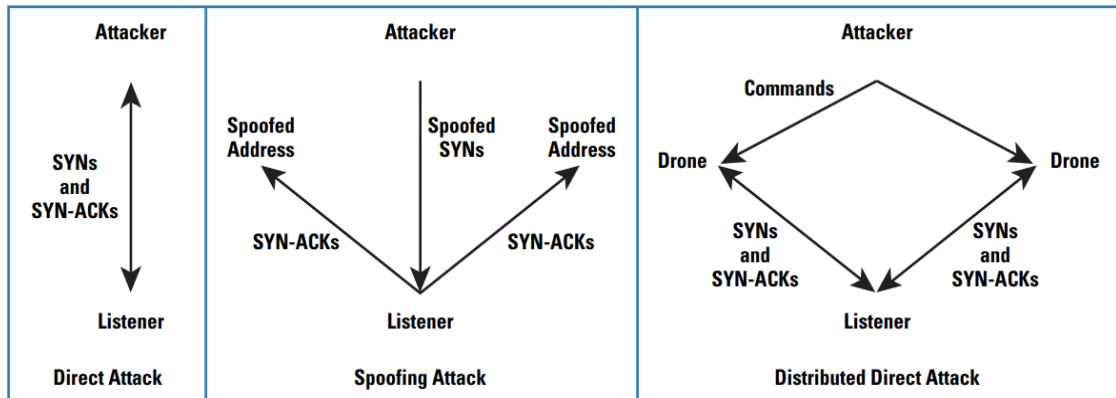


Figure 10. Methods of TCP SYN flood attack [24]

6.1.1 Direct attack

In a direct attack, the attacker sends SYN request to the server or host rapidly from the legitimate IP address or port. The attack is successful if the attacker is able to ignore the SYN-ACK acknowledgement request received from the server or host, and deny sending any request like ACKs or ICMP message back to the host. Firewall rule can be used in this method to deny sending the acknowledgement request or preventing the SYN-ACK request entering the attackers TCP controlling code. [24]

6.1.2 IP spoofing attack

In IP spoofing attack method, the same process is conducted like a direct attack but the SYN request is sent from a spoofed IP address along with valid IP and TCP header in a spoofed and raw IP packets to the server. These spoofed packets can be tracked with the help of an internet service provider (ISP) address[25].

6.1.3 Distributed direct attack

In a distributed direct attack, a botnet is commonly used for an attack. Mirai is one of the famous botnets used for DDoS attack of this type. To make the scenario worst, the attacker might use the spoofed IP address for the botnets even though the source can be traced back with the help of ISP [25]. As shown in Figure 10 above, multiple drones or botnets are used for an effective attack where each of them hosts a spoofed IP address.

Nevertheless, the countermeasure is quite challenging as the botnet's army are centralized and decentralized constantly. [25]

6.2 DNS Amplification attack

A reflection-based DDoS attack is known as a DNS amplification attack. Look up request to the DNS server is spoofed by the attacker so that the DNS server can direct the response to the target network by hiding the attack source. This attack is also known as bandwidth consumption attack where the DNS response message is larger than the DNS query message [26]. This attack results to make the victim's server down. By using multiple types of amplification technique, the attacker can increase the size of UDP packets to make the service down of various internet service by exploiting the drawback of DNS server. [27]

When the DNS amplification attack is made, the attacker spoofed the IP address of the victim, and send the DNS query to an open DNS resolver. Then the DNS resolver sends the DNS response to the victim IP address. This creates an enormous amount of traffic to the victim's side, and the victim's server or network cannot reply to the original user as the victim's network is already flooded with the DNS responses. The amplification factor can amplify up to the factor of 70:1. [27]

According to Rozekrans & de Koning, these types of attacks are more complicated and difficult to trace and track the packet filters and traffic. This result in creating the defence mechanism to be more sophisticated and create the filtering in the name server and open DNS resolver. They have divided the DNS amplification attack into three types as repeating queries, varying queries and a distributed attack based on DNS queries. In a repeating query DNS amplification attack, the same request is queried multiple times. If this attack method is not working or mitigated, then the varying query attack method is utilized where the DNS server receives the queries from varying domain names. If multiple DNS servers are targeted with distributed attack traffic, then the attack is called distributed DNS amplification attack. [28]

6.3 NTP Amplification Attack

Network Time Protocol (NTP) amplification attack is a type of DDoS attack where the attacker misuses the publicly-accessible NTP server functionality by overpopulating the server or targeted network with an exaggerated amount of UDP packet causing the network or server inaccessible to handle the regular traffic from the legitimate user. NTP is used to administer the authentic time data within the network connected devices [29].

All the internet connected devices use Network Time Protocol which also provides the authority to the administrators to query NTP server for counting the traffic. This service called “MONLIST” command can provide up to the 600 last connected customer IP address linked with the NTP server. During the NTP amplification attack, an attacker continuously sends the “MONLIST” command from spoofed IP address of a requesting server to an NTP server. As a result, NTP server response with an amplified amount of traffic aimed towards the target server conclusively leading to the denial of required service to the legitimate user requests. [30]

NTP amplification attack starts with the attacker using the botnets to send the UDP packets to the NTP server from spoofed IP addresses to the actual IP address of the victim. As shown in fig. x, NTP server response with large amount requests for each of the UDP packets that use “MONLIST” command. The target server gets overwhelmed by the large response from the NTP server.

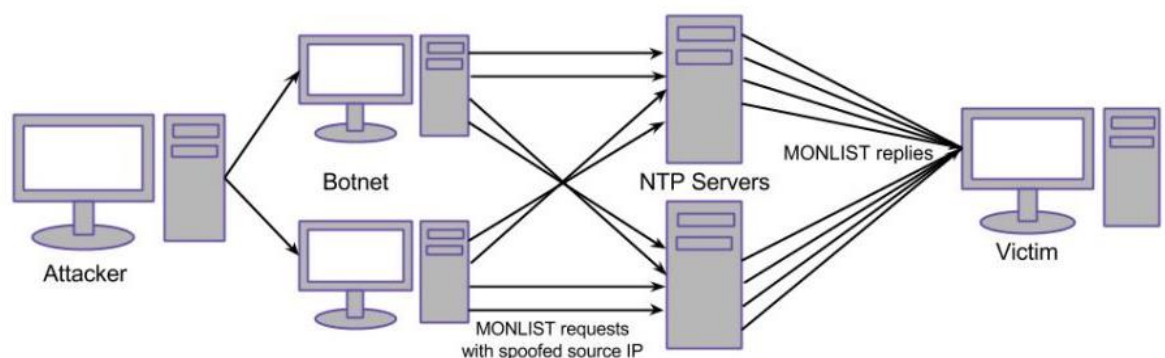


Figure 11. NTP amplification attack [29]

Figure 11 above shows the attack module of NTP amplification. During this type of attack, a real IP address is never used which makes the traceback of attacker almost impossible. However, by the analysis of characteristics of the attack, the types of hosts used to create the attack packets can be observed and analyzed.

7 Methods of Mitigation

7.1 Mitigating TCP SYN Flood DDoS attack

TCP SYN flood attack can be controlled and monitored with various tools and techniques. Initially, it was noted that the TCP SYN was utilizing the common port number even though they were using random spoofed source address. A temporary solution was evolved to deny the incoming packets from such sources but later was not utilized as the attacker were able to change and adapt the port number.

According to the journal published by Wesley for Verizon Federal Network System, two class of process of the mitigating system has evolved according to the implementation of defence mechanism. End-Host countermeasure, where hardening of the end-host TCP is done is the first class of this process. With the end-host hardening, the way of establishing and successful connection of TCP can be controlled by altering the algorithms and data structure along with diverse TCP state machine behaviour of connection. The second class comprises hardening the network itself. In this measure, a middlebox is used to isolate servers on the network to protect it against the spoofed IP address and illegitimate SYNs.

7.1.1 End-Host Hardening

Increasing TCP backlog

By increasing the backlog, overflowing of a host's backlog can be controlled as done in most of the server application. Altering the listen() call of an application, a backlog of an application can request for an upper bound size limit. However, this does not apply to the attacks on the larger scales, and support for base level only as most of the operating system and its application can already support the large scale of the backlogs. Increasing the backlog of the connecting socket does not affect as mitigation technique if the scale of the attack is larger than the ability of the host to support it.

Decreasing SYN-Received Timer

When a TCP connection reaches to the SYN-RECEIVED state, a time limit can be set on its connection to repeat again and again. This can control the attack by not letting the illegitimate source address and its connection request to advanced. However, the legitimate TCP request can be reaped where the aggressive attack can create the time toss in the second and third stage of TCP connection. Although this mitigation technique is reliable, it is not advisable to rely on this technique due to the direct relationship between reduction of SYN-RECEIVED timer created by the administrator and relatively increased in an attack of packet rates sent by the attacker.

SYN Cache and Cookies

SYN cache and SYN Cookies are the two end-host defence technique where the amount of state reserved in the first state of TCB create by the SYN received state is reduced. In each hash bucket, a limited amount of space is used in every SYN cache using a host to store the subdivision of the abstracts that would shift into TCB that is already allocated. When an ACK is received with a completed handshake, these abstracts are shifted into the full TCB so that the past hash bucket can be destroyed when needed. The value of is calculated with the data provided by the incoming packet, source and destination address, port and the secrets which are randomly chosen. In each bucket, SYN cache entries are link-listed, and the secret is used as an index value. By using this hash secret, the attacker will not be able to attack the specific target. All the possible risk of the attacker attacking the hash bucket is mitigated by using the hash secret, and the legitimate connection does not get nested into the long chain of connection establishing handshake. Along with this, the variety port number is used to calculate the hash secret, every other illegitimate attempt of connection is given the second hash bucket which protects the attack on the specific bucket. [31]

In SYN cookies scenario, to prevent the frequent connection drop, a cookie is created by the server. The technique is such that when the backlog is filled, the server makes the port open for a new connection by dropping the backlog SYN request, after responding to each request of connection with the second stage of three-way handshaking called SYN-ACK request. The server recreates the SYN backlog entry only after receiving the ACK request from the client, which in practice is only possible for the legitimate connection. Although some information about the connection is lost in the process, the service does not get denied for the legitimate connection. [31]

Hybrid approach

This mitigating approach against TCP SYN flood is considered to take advantages of all other types of end-host hardening technique. While using SYN cookies method, some information about the TCP connection is lost, SYN cookie is added as a secondary defence technique after the TCP backlog technique. With this multiple or hybrid approach, SYN cookie is activated only if the threshold is exceeded by the amount of backlog created which prevent the server from the attack and preventing the loss of information in TCP connection caused by SYN cookie method. [24]

7.1.2 Network Hardening

Filtering

Using ingress filtering, the Internet Service Provider can deny to further route the packets which are coming from the source that does not reside to that end site This network-level defence of filtering is applicable for the attack which is coming from the spoofed IP address. As the ingress filtering method is not applied universally, the method is not highly effective. Also, the bots or zombies that attack the server directly and independently with the TCP SYN flood is not affected by this method. However, this can be defended with an adequate adaptation of policies by ISP universally. [24]

Firewalls and Proxies

Firewall and proxy device in between the network can protect the SYN flood attack by spoofing the request in the three-way handshake of TCP connection. Firewall and proxy can spoof the SYN-ACK request to the starter and by spoofing the ACK request to the header. Firewalls and proxies in between the connection divide the connection of attacker and hosts into two connection. Both end devices must create a connection with the intercepted firewall and proxy. Division of the connection by this method works as a defence mechanism for the SYN flood attack. This is a trusted mitigating method because the host server never receives the SYN request from the attacker, and the firewall and proxy receive all the ACK request from the attacker and identity and address of the attacker is modified by this method. [24]

Firewall and proxies spoof the ACK requests sent to the attacker after receiving the SYN-ACK requests. This helps the TCBS to be in SYN-RECEIVED state for a long period, and the backlog space can be maintained. The firewall divides the request either coming from the legitimate source or illegitimate source. If the legitimate ACK is not received from the attacker, then the host device is informed to free the TCB with an interfered TCP-RST segment. However, after the successful TCP connection is established, firewall and proxy device does not intrude in between for the incoming legitimate source of a packet as it does with the method of spoofing SYN-ACK request. [24]

7.1.3 Agent-based defence

Agent-based defence technique comes handy for protection against various types of DDoS attack. Cloudflare, an internet related company that also works on internet security provides a solution for attacks against TCP SYN flood attack. By standing in between the target and the attacker, Cloudflare handles the TCP connection process and intercept in between the three-way handshake process virtually. A connection with a cloud server is established before the connection is made successful between the target server and the attacker.

7.2 Mitigating DNS amplification attack

DNS amplification attack and its impact have been increasing day by day to the internet user and service provider. The removal of amplification and reflection factor in the attack and continuing to provide service to the legitimate user can create a proper defence mechanism. Various types of network devices and security protocols can be considered to mitigate the DNS amplification attack.

The first step to be protected against DNS amplification attack is to configure and manage the DNS server and recursive DNS server within the network properly. The United States Computer Emergency Response Team (US-CERT) advised that for Domain Name System (DNS) servers that are deployed inside an institution or ISP to provide name queries in the interest of a client, the resolver ought to be arranged to just permit queries for the benefit of legitimate and approved customers. US-CERT also suggest blocking all the spoofed IP address request by the ISP all around. [32]

A spoofed IP address or some selective malicious IP address can be blocked by using a firewall within the network. However, this mechanism can also block the traffic request from the legitimate user request. Nowadays, many companies and internet service providers have installed firewall within their system [28]. Also, the network ingress filtering method can be implemented so that the router can check and verify the validity of an IP address. A transmission from a DNS client can be dropped if the same queries come frequently from the same IP address to the continued destination.

7.3 Mitigating NTP amplification attack

After understanding the attack mechanism of NTP amplification attack, it is clearly understood that the removal of the functionality of “MONLIST” command can solve half the problem. Similarly, all the susceptible NTP servers embedded with the version before 4.2.7 can be upgraded to or later version which does not use this command at all. Nevertheless, the server administrator can follow the US-CERT instructions to patch the vulnerability of the command that helps amplified the ratio of attack.

Ingress filtering of traffic in the network is also applicable to mitigate the NTP amplification attack. The filtering of spoofed IP address plays a vital role in decreasing UDP-based amplification attack.

Nowadays, various cybersecurity and software companies provide internet security related to the matter of DDoS attack and security. Imperva Incapsula, Akamai DDoS mitigation, Cloudflare DDoS, Protection, Arbor Networks Availability Protection System (APS) are among the leader of the service provider.

8 Testing SYN flood attack

The demonstration below shows one of the methods to create a TCP SYN flood attack and the readers can understand the process of creating a DDoS attack. The attack method used in this demonstration is hping3 included in Kali Linux environment. Wireshark is used to analyze all the packets and to detect the SYN Flood attack.

8.1 Hping3

Hping3 is one of the TCP penetrating tools which was primarily used as a security tool before but being used for testing of network and host. Hping3 can be utilized, for example, firewall test, traceroute in various protocols, port scanning and packet generator. It is also known as an active network smashing tool. [33]

8.2 Wireshark

Wireshark is a conventional and popular network analyzer which is used all around the world for multiple purposes. It offers the solution to the commercial and non-commercial companies and enterprises to have a deep inspection of the traffic in the network and protocols. The project to develop the program was started by Gerald Combs as Ethereal which was later renamed as Wireshark. Wireshark can be used to capture, analyze and monitor traffic and protocols in the live environment, and the result can also be saved and exported to the various platform. [34]

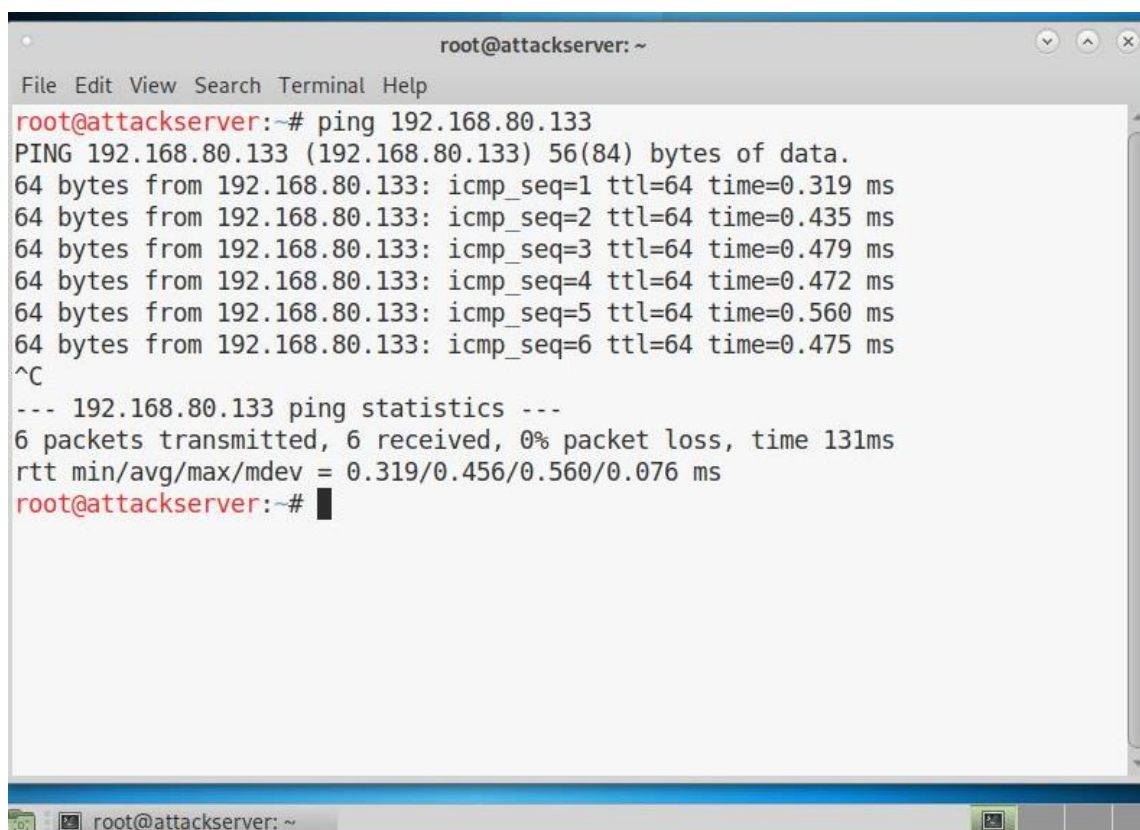
8.3 Overview

Kali Linux was used in this method to create a fake IP address for attacking another host. Debian platform was installed in this host, and all the packets in both machines were captured and analyzed using Wireshark.

The attacking machine Kali Linux and the host machine Debian was installed in the virtual environment, and both machines were set up for demonstration. In most cases, hping3 is preinstalled in Kali Linux. However, in other Linux distribution, it can be installed by using the following command.

```
# sudo apt-get install hping3
```

In the virtual environment created, the real IP address of the attacking machine is 192.168.80.135, and the IP address of the host machine is 192.168.133. At first, a ping test was done to verify the connectivity between the machines. Figure 12 below shows the ping result of the environment which was successful.



```

root@attackserver: ~
File Edit View Search Terminal Help
root@attackserver:~# ping 192.168.80.133
PING 192.168.80.133 (192.168.80.133) 56(84) bytes of data.
64 bytes from 192.168.80.133: icmp_seq=1 ttl=64 time=0.319 ms
64 bytes from 192.168.80.133: icmp_seq=2 ttl=64 time=0.435 ms
64 bytes from 192.168.80.133: icmp_seq=3 ttl=64 time=0.479 ms
64 bytes from 192.168.80.133: icmp_seq=4 ttl=64 time=0.472 ms
64 bytes from 192.168.80.133: icmp_seq=5 ttl=64 time=0.560 ms
64 bytes from 192.168.80.133: icmp_seq=6 ttl=64 time=0.475 ms
^C
--- 192.168.80.133 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 131ms
rtt min/avg/max/mdev = 0.319/0.456/0.560/0.076 ms
root@attackserver:~#

```

Figure 12. A ping test from attack machine to the host machine

By using the hping3 command, 12000 packets were sent to the host machine. Each of the packets was of the size 120 bytes and the TCP window size of 64. While performing the attack, SYN Flag (-S) was enabled and all the traffic was flooded using *-flood* towards the HTTP port, specifically port 80 of the host machine. To trick the host machine, spoofed IP address was generated by using hping3 *--rand-source* utility. All the SYN requests were sent from the fake IP addresses generated to the host machine. The SYN-ACK reply from the host machine to the attack machine was denied by using the same *-rand-source* utility. As a result, the port waiting for the acknowledgement (ACK) reply from the invisible machines with the spoofed IP address was left half open. All this process was executed from the attack machine by using the single command below.

```
# hping3 -c 12000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.80.133
```

The hping3 TCP SYN flood attack done from attack machine to the host machine of the same environment can be seen in Figure 13 below.

Accordingly, Wireshark was used to capture all the packets during the attack. At first, the traffic was filtered and analyzed for TCP SYN packets which were not acknowledged by the attack server in Wireshark by using the filter below.

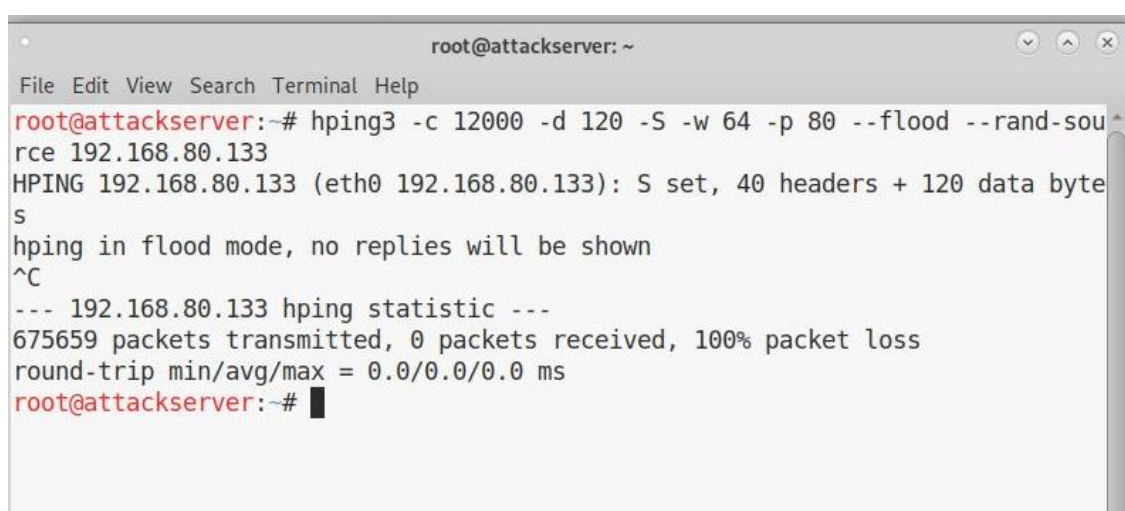
```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

Similarly, the TCP SYN packets with the acknowledgement were also filtered in Wireshark by using the filter below.

```
tcp.flags.syn == 1 and tcp.flags.ack == 1
```

8.4 Result

All the traffic directed towards the IP address of the host machine was analyzed and filtered for the detection of the spike in traffic to the host machine. The process of hping3 attack from the attack machine can be observed from Figure 13 below.



```
root@attackserver: ~
File Edit View Search Terminal Help
root@attackserver:~# hping3 -c 12000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.80.133
HPING 192.168.80.133 (eth0 192.168.80.133): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.80.133 hping statistic ---
675659 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@attackserver:~#
```

Figure 13. Hping3 attack to the host machine

The hping3 attack was done for few seconds only. However, the number of packets sent to the host machine was around 452020. After filtering for the SYN packets without the acknowledgement using the filter mentioned above, the result can be seen in Figure 14 and 15 below.

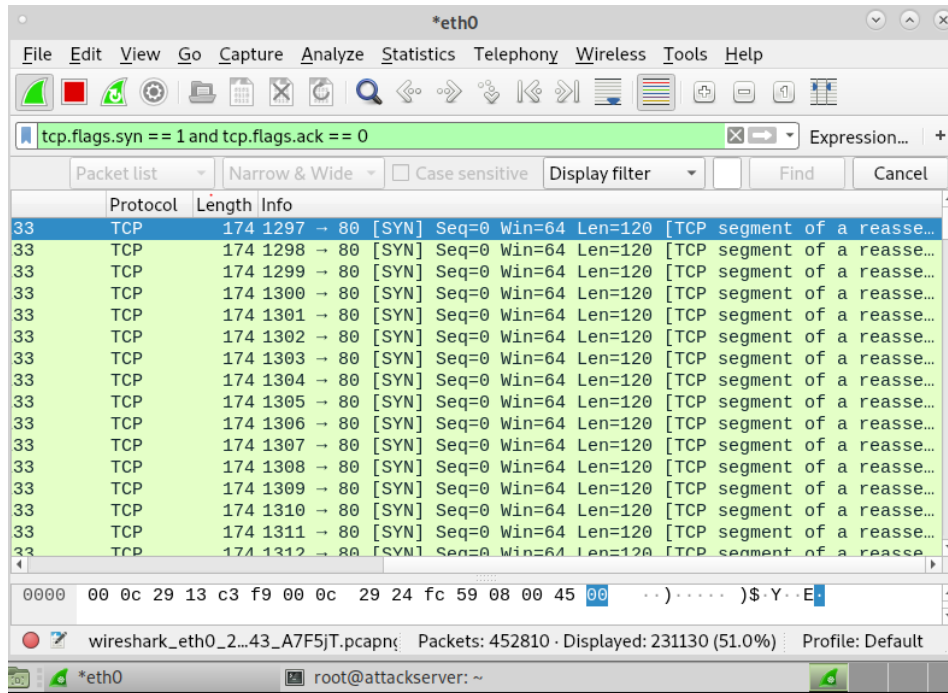


Figure 14. TCP SYN packets filter without acknowledgement (left view)

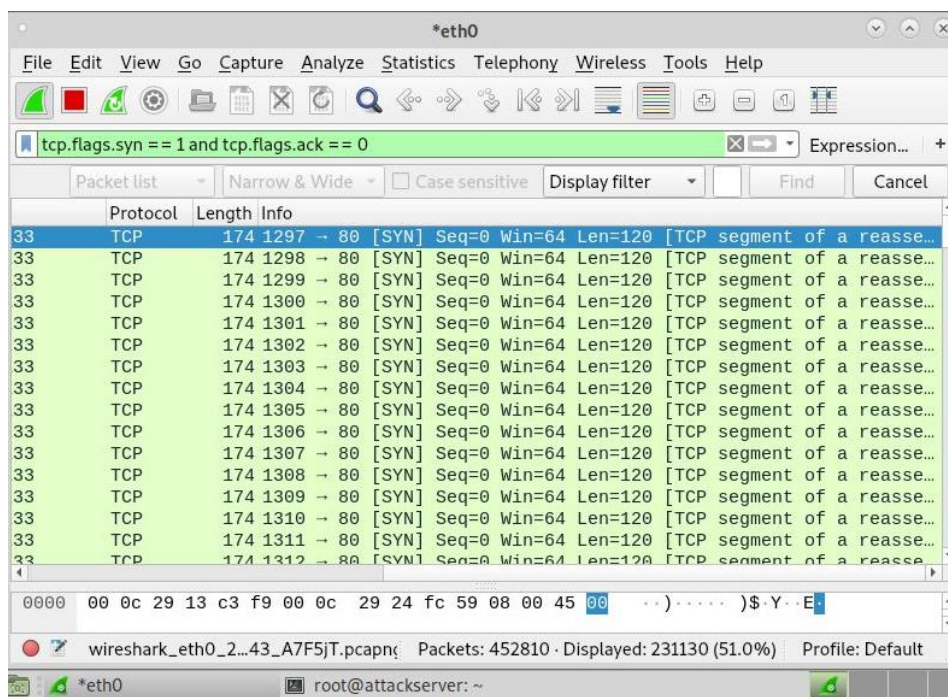


Figure 15. TCP SYN packets filter without acknowledgement (right view)

As seen in Figure 15 above, all the TCP SYN packets were generated from the various spoofed IP address. All the packets of size 120 bytes were sent to the port 80 of the host machine and were of window size 64. As the result can be clearly seen in the Wireshark, the percentage of the filter packets was more than 50. However, after filtering the TCP SYN Packets with the acknowledgement (ACK) filter, the number of filters obtained from Wireshark was comparatively negligible that were received by the attack machine. The filtered packets can be seen from Figure 16 below.

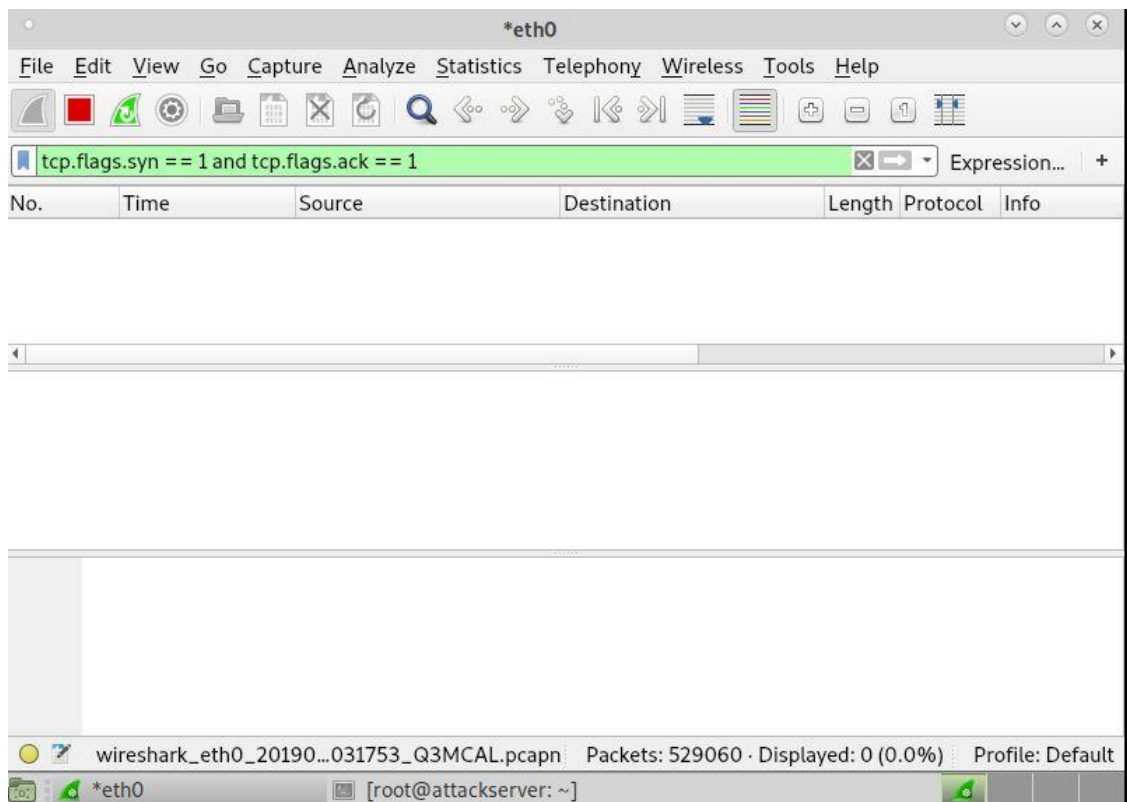


Figure 16. TCP SYN packets filter with acknowledgement

The simple attack from the attack machine using hping3 was able to send thousands of packets to the host machine disguising the host machine with the spoofed IP address. After the TCP SYN request, the host machine replied with SYN-ACK reply to the attack machine but remained unsuccessful due to the numerous spoofed IP address of the origin of TCP SYN packets. With the increasing size and number of packets to the host machine, the backlog of TCB which was initialized to SYN-RECEIVED state and kept

waiting for the successful three-way handshake. This made the backlog of TCB backlog completely full, and the host machine could no longer receive the SYN request from another attacker nor from the legitimate user. As the resource of the host machine was completely utilized and it could no longer provide the service, the result was TCP SYN flood DDoS attack.

9 Conclusion

The main goal of this project was to study the detailed methodologies and mitigation method of different types of Distributed Denial of Service attack so that any reader could understand the requirements of the attack, and create and evaluate an attack in a secure environment for the better understanding of the topic. The objective of this project was also to create a DDoS attack in a secure environment to capture and analyze the packets for the testing purpose.

After the study of all the technologies, requirements, environment, types and ways of mitigation related to various types of attack, an environment was set up for the possible scenario of the SYN flood attack using Hping3 tool that could be possible in the real world. After setting up the environment with two computers, one as an attacker and another as a victim, the test attack was made and tested successfully as per it was created.

As it was illegal to create a DDoS attack in the real environment, the best choice was to create a virtual environment within a closed network with the machines connected from inside. The main limitation in the project was to create an attack with the single machine as the configuration of the device used in this project was not up to par due to which no botnets were used in the attack. However, the methods and technologies used and discussed in this project are useful to understand the DDoS attack of large size. The main goal was achieved through the project.

References

- 1 DDoS Attacks [Internet]. Incapsula.com. [cited 12 January 2019]. Available from: <https://www.incapsula.com/ddos/ddos-attacks.html>
- 2 SAGER C. Why Do People Perform DDoS Attacks? [Internet]. BrainStuff. 2014 [cited 8 January 2019]. Available from: <https://www.brainstuff-show.com/blogs/why-do-people-perform-ddos-attacks.htm>
- 3 Yle Uutiset. Cyber attack shuts down many government websites in Finland. [Internet]. 2018 [cited 8 January 2019];. Available from: https://yle.fi/uu-tiset/osasto/news/cyber_attack_shuts_down_many_government_websites_in_finland/10350316
- 4 Bulawayo24. Anonymous kickstarts DDoS protest against Zimbabwe's government. [Internet]. 2019 [cited 22 January 2019];. Available from: <https://bulawayo24.com/index-id-news-sc-national-byo-154141.html>
- 5 What is a DDoS Attack? - DDoS Meaning [Internet]. Kaspersky.com. 2019 [cited 2 March 2019]. Available from: <https://www.kaspersky.com/enterprise-security/resources/case-studies>
- 6 Cimpanu C. BleepingComputer [Internet]. BleepingComputer. 2017 [cited 15 January 2019]. Available from: <https://www.bleepingcomputer.com/>
- 7 Chan J. The Motivation and Goals Behind DDoS | DOSarrest Internet Security| DDoS Protection [Internet]. Dosarrest.com. 2010 [cited 15 April 2019]. Available from: <https://www.dosarrest.com/ddos-blog/the-motivation-and-goals-behind-ddos/>
- 8 Yates D. We Lost Tens of Millions. Daily Observer newspaper [Internet]. 2019 [cited 28 January 2019];. Available from: <https://www.liberianobserver.com/news/we-lost-tens-of-millions/>
- 9 Casciani D. Briton who knocked Liberia offline with cyber attack jailed. BBB news [Internet]. 2019 [cited 1 February 2019];. Available from: <https://www.bbc.com/news/uk-46840461>
- 10 Lemos R. How DDoS Attacks Techniques Have Evolved Over Past 20 Years [Internet]. eWEEK. 2018 [cited 15 February 2019]. Available from: <https://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years>
- 11 Bene N. A Brief History of DDoS Attacks. [Internet]. Eugene Kaspersky. 2016 [cited 14 January 2019]. Available from: <https://eugene.kaspersky.com/2016/12/06/a-brief-history-of-ddos-attacks/>

- 12 Kupreev O, Badovskaya E, Gutnikov A. DDoS Attacks in Q3 2018 [Internet]. Securelist.com. 2018 [cited 12 April 2019]. Available from: <https://securelist.com/ddos-report-in-q3-2018/88617/>
- 13 Roach J. What is a Botnet? Networks Gone Bad [Internet]. Cloudwards. 2018 [cited 20 January 2019]. Available from: <https://www.cloudwards.net/what-is-a-botnet/>
- 14 Shoemaker A. How to Identify a Mirai-Style DDoS Attack [Internet]. Application Security. 2017 [cited 6 January 2019]. Available from: <https://www.incap-sula.com/blog/how-to-identify-a-mirai-style-ddos-attack.html>
- 15 Yu S. Distributed Denial of Service Attack and Defense. 1st ed. New York, NY: Springer New York; 2014.
- 16 Nelson T. The Flusihoc Dynasty, A Long Standing DDoS Botnet | NETSCOUT [Internet]. NETSCOUT. 2017 [cited 27 January 2019]. Available from: <https://asert.arbornetworks.com/the-flusihoc-dynasty-a-long-standing-ddos-botnet/>
- 17 OVH Innovation for Freedom [Internet]. OVH News. [cited 17 February 2019]. Available from: <https://www.ovh.com/world/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac>
- 18 Bursztein E. Inside Mirai the infamous IoT Botnet: A Retrospective Analysis [Internet]. NETWORK SECURITY. 2017 [cited 12 February 2019]. Available from: <https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/#toc-1>
- 19 Nayan K. Hacking into Hackers' Head: A step towards creating CyberSecurity awareness. 1st ed. Kamal Nayan; PublishDrive edition; 2018.
- 20 Nachreiner C. Profiling modern hackers: Hacktivists, criminals, and cyber spies. Help Net Security [Internet]. 2013 [cited 22 April 2019];. Available from: <https://www.helpnetsecurity.com/2013/05/30/profiling-modern-hackers-hacktivists-criminals-and-cyber-spies/>
- 21 Shuler R. How Does the Internet Work? [Internet]. Pomeroy IT Solutions; [cited 17 January 2019]. Available from: <https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm>
- 22 Vijayan J. Massive DDoS Attack Generates 500 Million Packets per Second. Informatio Week IT Network [Internet]. 2019 [cited 26 February 2019];. Available from: <https://www.darkreading.com/attacks-breaches/massive-ddos-attack-generates-500-million-packets-per-second/d/d-id/1333766>

- 23 The Top 10 DDoS Attack Trends [Internet]. Imperva; 2015 [cited 5 January 2019]. Available from: https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf
- 24 Eddy W. Defenses Against TCP SYN Flooding Attacks. Cisco release [Internet]. 2006 [cited 19 January 2019];9(4). Available from: <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-34/syn-flooding-attacks.html>
- 25 SYN Flood DDoS Attack | Cloudflare [Internet]. Cloudflare. 2019 [cited 26 January 2019]. Available from: <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>
- 26 Lopez J, Hämmerli B. Critical Information Infrastructures Security. Malaga, Spain: Springer; 2007.
- 27 DNS Amplification [Internet]. Incapsula.com. [cited 15 February 2019]. Available from: <https://www.incapsula.com/ddos/attack-glossary/dns-amplification.html>
- 28 University of Amsterdam System & Network Engineering RP1. Defending against DNS reflection amplification attacks. Netherland; 2013.
- 29 Rudman L, Irwin B. Characterization and Analysis of NTP Amplification Based DDoS Attacks. Department of Computer Science Rhodes University.
- 30 NTP Amplification [Internet]. Incapsula.com. [cited 14 January 2019]. Available from: <https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html>
- 31 FreeBSD Project. Resisting SYN flood DoS attacks with a SYN cach [Internet]. Available from: <http://pdfs.semanticscholar.org/a2a8/67ff144c8f90f0a24f7f7765f18cfe2c6d6f.pdf>
- 32 Kerner S. US-CERT Warns about DNS Amplification Attacks. eSecurity Planet [Internet]. 2019 [cited 21 February 2019];. Available from: <https://www.esecurityplanet.com/network-security/us-cert-warns-about-dns-amplification-attacks.html>
- 33 Sanfilippo S. Hping - Active Network Security Tool [Internet]. Hping.org. 2006 [cited 4 March 2019]. Available from: <http://www.hping.org/>
- 34 Wireshark · Go Deep. [Internet]. Wireshark.org. [cited 20 March 2019]. Available from: <https://www.wireshark.org/>