

IoT Security: Simulation and Analysis of TCP SYN Flooded DDOS Attack using WireShark

¹Yee Mon Thant, ²Myint Soe Khaing, ³Chaw Su Htwe, ⁴Thazin Tun, ⁵Mie Mie Su Thwin

¹²³⁴Faculty of Computer Science, ⁵Cyber Security Research Lab,

¹²³⁴⁵University of Computer Studies, Yangon.

yeemonthant@ucsy.edu.mm, myintsoekhaing@ucsy.edu.mm, chawsuhtwe@ucsy.edu.mm,
thazintun@ucsy.edu.mm, drmiemiesuthwin@ucsy.edu.mm

ABSTRACT

Nowadays Internet of Things (IoT) technology is significantly entering our daily lives because IoT have widely scope such as security systems, smart industrial environment, vehicles, electronic appliances, wearable devices, healthcare etc. Since these devices are interconnected with each other on the internet to give the various types of services to consumers with various technologies. The emergence of new technology in various fields it also brings up challenges in the area of the forensic investigation. The latest tools and the procedure stream did won't satisfy disseminated and current IoT infrastructure. In recent year, the huge improvement of DDoS assault in IoT network, IoT security has directly gotten to be one of the first concerned points inside the field of network security. SYN flood assault misuses the TCP' three way handshake handle and all victim's assets are depleted and assist connection requests cannot be considered, so this can be denying the legitimate gets to. The outcomes produced are utilized as evidences to demonstrate that a machine is victimized and is confronting a DDOS attack. In this paper, we have done network analysis for detecting SYN flooded attack on IoT Smart Environment using WireShark.

Keywords: Internet of Things (IoT); Network Forensics; IoT Forensics; Distributed Denial of Service (DDoS); SYN Flood attack.

1 Introduction

Internet of things (IoT) is another insurgency of innovation that empowers little devices to go about as smart objects. These devices are associated with one another by various system media types, and the consequence of these interchanges is to come back to the sensors by fitting choice. The objective of IoT is to make lives progressively advantageous and dynamic. IoT devices can trade data between themselves to give a helpful support of the proprietor. In reality, IoT advancement crosses particular industry zones, for example, shrewd city, medical care and shrewd home. The IoT innovation can make more opportunities for cybercrimes to assault these regions, coming about in a coordinate affect on clients. From the forensic point of view, each IoT gadget will give vital artifacts that seem offer assistance within the investigation handle. A few of these artifacts have not been disclosed in open which means the examiners ought to consider of these assets and how they can obtain the artifacts from these gadgets. Despite the fact that IoT has rich wellsprings of proof from this present reality application, it causes a few

difficulties for legal sciences inspector including yet not constrained to the area of information and heterogeneous nature of IoT devices, for example, contrasts in working frameworks and correspondence gauges. The information exchange over the internetwork isn't verified as the conventions utilized were not planned in light of security. At times these assets are inaccessible to authorized clients, as a result of DoS and DDoS attacks. A compromised system or host (likewise called a bot) floods with large number of packets in a brief period, which further causes DoS attack. Different sorts of flooding attacks utilizing conventions, for example, TCP, UDP and so on are well known nowadays.

Dissents of benefit assaults by and expansive take missing the assets and the services of the hub and deny other legitimate access. In SYN flooding assault, an assault hub sends various TCP (Transmission Control Protocol) SYN requests with spoofed source addresses to a hub. Each asks makes the goal center to assign its assets out of the accessibility. The destination sends the acknowledgement to the spoofed address and holds up for the third message from the source, since TCP association is set up after a three way handshake. But, the source address could be a spoofed address and it'll not react with an acknowledgement. Meanwhile, the assailant sends the numerous of SYN demands. All the victim's assets are exhausted and consequently development association requests cannot be considered, denying the legitimate gets to.

The rest of the paper is planned as follows. Section 2 discusses the other research works on analyzing and identification of DDoS attack. Section 3 provides Forensics in IoT Environment and DDoS techniques, Section 4 SYN Flooding Attack Scenario and attacking mechanism. Section 5 presents experimental result for detection of SYN flooded attack. Section 6 concludes the current work.

2 Related Work

The DDoS attack hampers the load on processor of Internet services which turns out the huge business loss [6].

- When any attacker launches the DDoS attack, the victim may face following impact on server,
- To make server's process exhaustion;
- To make unavailability of resources of the server to the legitimate users;
- To make server's Bandwidth congestion; and
- Bad QoS of the server From the above highlighted point, the DDoS attack is creating exhaustion of resources for victims and as a result of huge business losses may occur.

Loss of network resources causes economic loss, work delays and a loss of communication between network users. Hardware based checking and filtering mechanism can provide an additional layer of defence against DDoS attack [7]. The TCP/IP protocol should be examined to understand DDoS attacks [8]. To identify the assaults from outside, the authors proposed to have Snort [9] set up on each VM and the observing and cautioning data is coordinated to a fundamental investigation and security framework with its web investigation tool being coordinates to the front-end of Eucalyptus. Gupta et al. The open source cloud stage utilized by the researchers was OpenNebula [10].

[11] gives a point by point investigation on the SYN Flooding assault and analyzes the different parameters which are influenced by the assault. The essential condition for the distinguishing proof of SYN flood assault, which is the proportion of the number of acknowledgements received from the client to the SYN acknowledgements sent from the server is checked.

3 Literature Review

3.1 Internet of Things (IoT)

The Internet of Things (IoT) delineates the framework of physical items "things" that are embedded with sensors, programming, and diverse developments to interface and exchange data with distinctive gadgets and systems over the internet. These gadgets expand from typical family unit articles to present day mechanical gadgets. Inside overabundance of 7 billion associated IoT gadgets nowadays, specialists are expecting that this number ought to create to 10 billion by 2020 and 22 billion by 2025[1]. In the course of later a long time, IoT has gotten one of the foremost critical progresses of the 21st century. Since we are able to relate normal items, kitchen devices, vehicles, indoor regulators, child screens—to the net through embedded gadgets, reliable correspondence is conceivable between individuals, methods, and things. Utilizing ease figuring, the cloud, huge information, investigation, and portable advances, physical things can share and gather information with insignificant human intercession. In this hyper-associated world, advanced frameworks can record, screen, and modify the every cooperation between associated things. The physical world meets the computerized world and they participate.

3.2 IoT Forensics

The IoT Forensics is likewise one of the particular branches in the digital forensics where every one of the stages examined manages the IoT foundation to discover realities about the wrongdoing occurred in the IoT environment. The IoT Forensics is done in the three degrees of crime scene investigation: Cloud level forensics, network level forensics, device level forensics this can be clarified in Figure 1[3].

- Device level Forensics: At this level, a forensic examiner must accumulate data to begin with from the adjacent memory contained within the IoT gadget to be examined. It is critical to utilize the IoT gadget that's missed in analyzing information on the forensic level device.
- Network level forensics: To distinguish diverse sources of assault can be recognized from network activity logs. Along these lines, the log activity network can be basic to choosing the fault or opportunity of the suspect. IoT foundation joins diverse sorts of network, for example, Body Area Networks (BAN), Personal Area Networks (PAN), Home/Hospital Area Networks (HAN), Local Area Networks (LAN) and Wide Area Networks (WAN). Critical evidence got is accumulated from one of these network with the objective that system crime scene examination.
- Cloud level forensics: Cloud forensics is one of the foremost critical pieces of the IoT forensics space. Why? Since most existing IoT gadget have low capacity and computing capacity, data created from IoT gadget and IoT systems are put away and prepared within the cloud. This is often on the grounds that cloud solvents offer a collection of central point counting settlement, gigantic limit, flexibility, and accessibility on request [12].



Figure 1.IoT Forensics

3.3 Network Forensics

Network forensics is the catch, recording, and investigation of system bundles to decide the wellspring of system security attacks. The significant objective of system legal sciences is to gather proof. It attempts to break down system traffic information, which is gathered from various locales and distinctive system gear, for example, firewalls and IDS. Additionally, it screens the system to distinguish attacks and break down the idea of assailants. System crime scene investigation is likewise the way toward identifying interruption designs, concentrating on aggressor action.

3.3.1 Network Forensics Process Model

- Preparation Stage: The principal objective is to gain the major approval and genuine ensured.
- Detection Stage: Generate an admonition or a ready that shows a security offense.
- Collection Stage: Usable just when the examination is starting throughout the attack.
- Preservation Stage: The most confounded area because the information streams rapidly and is no likelihood to create later hints of something very similar.
- Examination Stage: Original Evidence is kept secure through with registered hashes.
- Analysis Stage: Examines the past stage. All covered up or adjusted information is to be revealed which is finished by the assailant.
- Examination Stage: the Collected proof is broke down to find the wellspring of the blending.
- Investigation Stage: Use data assembled in the investigation stage and spotlight on finding the aggressor.
- Presentation Stage: Final stage for preparing the model. Here the documentation is made and the report is created and it appeared to the higher authority [4].

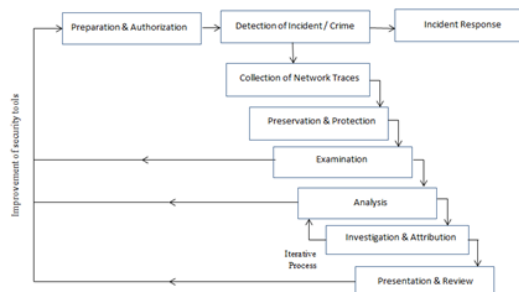


Figure 2. Generic Framework for Network Forensics

3.4 Distributed Denial of Service (DDoS) Attack

DDoS is a sort of DOS attack where different traded off frameworks, which are frequently tainted with a Trojan, are utilized to focus on a solitary framework causing a Denial of Service (DoS) attack. Casualties of a DDoS attack comprise of both the end focused on framework and all frameworks noxiously utilized and constrained by the programmer in the disseminated attack.

In a DDoS attack, the approaching traffic flooding the unfortunate casualty begins from a wide range of sources – conceivably several thousand or more. This successfully makes it difficult to stop the attack basically by hindering a solitary IP address; in addition, it is extremely hard to recognize genuine client traffic from attack traffic when spread crosswise over such a large number of purposes of birthplace. There are numerous types of DDoS assaults. Common assaults incorporate the following:

- Traffic attacks: Traffic flooding assaults send a huge amount of TCP, UDP and ICMP bundles to the target. Legitimate demands get misplaced and these assaults can be joined by malware abuse.
- Bandwidth attacks: This DDoS assault over-burdens the target with enormous amounts of garbage information. This comes about in a loss of network transmission capacity and hardware assets and can lead to a total denial of service.
- Application attacks: Application-layer information messages can exhaust assets within the application layer, taking off the target's system services blocked off [2].

3.5 TCP SYN Flooded Attack

SYN Flooded attacks work by misusing the TCP three way handshake process. In ordinary conditions, TCP established a connection using the following three distinct processes.

- First, the client sends a SYN bundle to the server in arrange to start the connection.
- The server at that point reacts to that starting bundle with a SYN/ACK bundle; in organize to acknowledge the communication.
- Finally, the client returns an ACK bundle to acknowledge the receipt of the bundle from the server. After wrapped up this sequence of process, the TCP association is open and able to send and get the data.

The TCP may be a connection-situated and reliable, in-succession movement transport protocol. It gives a full-duplex stream of data octets and it is the basic convention for the Internet. Most these days administrations on Internet hand-off on TCP. For instance mail (SMTP, port 25), ancient questionable virtual terminal offer assistance (telnet, port 23), report transport protocol (FTP, port 21) and for the most part critical for this circumstance moreover is the hyper content trade protocol (HTTP, 80) too called the worldwide web administrations (WWW). About everything utilizes TCP someway to do their communication over the network in any occasion, the brilliantly ones.

In TCP-SYN flooding assault, the SYN represents the Synchronize banner in TCP headers. The SYN banner gets set when a system at first sends a packet in a TCP association and illustrates that the getting system ought to store the course of action number recollected for this bundle. In this sort of flooding assault, the accentuation is given on the Banners, six one of a kind bits that could be sent to speak to different conditions, for example, starting gathering number (SYN), that the acknowledgment field is legitimate (ACK), reset the association (RST), or near the association (FIN).

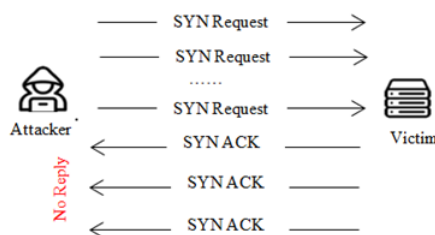


Figure 3. TCP-SYN Flood: Direct attack

During the TCP-SYN flooding assault [5], the assaulting system sends a TCP-SYN ask with a spoofed source IP address to victim. These SYN request allow off an impression of being genuine. The spoofed area implies to a client system that doesn't exist. From this time forward, the final ACK message will never be sent to

the sad casualty server system. This comes about into expanded number of half-open connections at the victim side. A excess line is utilized to store these half-open associations. These half-open associations tie the resources of the server. Hence, no unused associations (real) can be made, bringing almost DoS or DDoS. The victim server can't respond to the demands for Domain Name System (DNS) organization beginning from legitimate users(this assault is present in Fig. 4).Generally within the writing, there are three sorts of TCP-SYN flooding assaults, which are going out in these days Internet network: Direct Attack, Spoofing Attack, and Distributed Direct Attack (see Fig. 3-5).

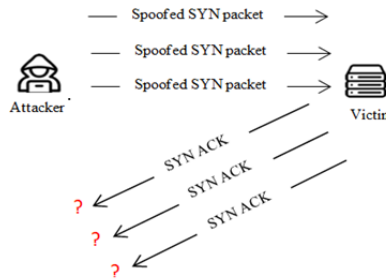


Figure 4. TCP-SYN Flood: Spoofing attack

On the off chance that aggressors rapidly send SYN parcels without spoofing their IP source address, this can be designated as a direct assault (Fig. 3). This strategy for the assault is greatly basic to perform in light of the fact that it doesn't incorporate specifically infusing or spoofing bundles underneath the client level of the attacker's working framework. It can be performed by basically utilizing numerous TCP connect () calls, for occurrence. To be successful, be that as it may, aggressors must anticipate their working system from responding to the SYN-ACKS in any way, since any ACKs, RSTs, or ICMP messages will permit the listener to move the TCB out of SYN-RECEIVED. When recognized, this sort of assault is anything but difficult to safeguard against, in light of the fact that a fundamental firewall rule to square bundles with the attacker's source IP address is all that's required. This defense behavior can be mechanized, and such capacities are accessible in off-the-shelf responsive firewalls.

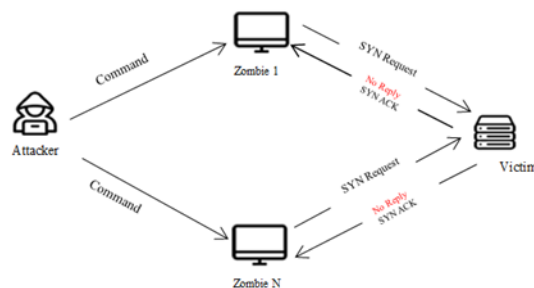


Figure 5. TCP-SYN Flood: Distributed direct attack

Moreover, TCP-SYN spoofing assaults utilize IP address spoofing, which may be seen as more mind-complex than the strategy utilized in a direct assault, in that instead of fair controlling local firewall rules, the assailant moreover ought to have the alternative to shape and imbue unrefined IP bundles with legitimate IP and TCP headers. In addition, the IP address spoofing strategies can be classified into different sorts as per what spoofed source addresses are utilized within the assaulting bundles.

4 Proposed Methodology

4.1 SYN Flooding Attack Scenario

The attacker needs to overpower the target's resources. By flooding a target with SYN packets and not responding (ACK), so he can easily overwhelm the target's resources. In this case, the target struggles to handle traffic which will expand CPU utilization and memory utilization at last prompting the weariness of its resources (CPU and RAM).

Requirement:

- Attacker's Tool: Hping using Kali linux (VM) which is installed on VirtualBox
- Wireshark installed on Victim OS

Description:

- Victim OS's IP is 192.168.43.125
- Victim is connected to network.
- Victim OS is running Wireshark to capture Network traffic.

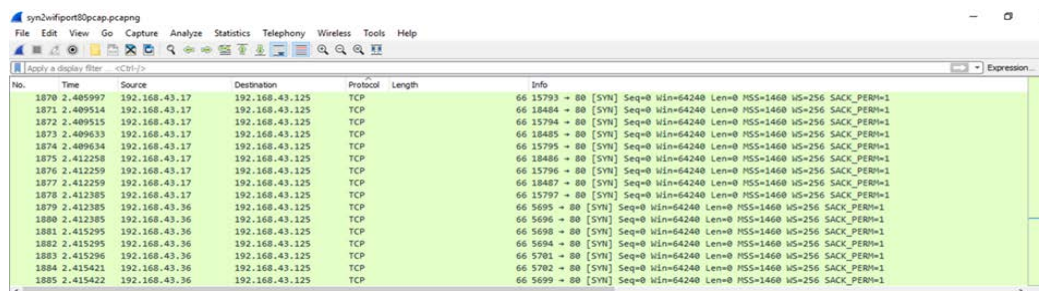
TCP SYN Flood Attack from Attacker's Terminal:

- On attacker's system, open Hping3 terminal
- `hping3 -flood -p 80 192.168.43.125 -S -- rand-source`

On the attacker side, the attacker needs to run an attack command on the Hping terminal. Hping3 is a well-known TCP infiltration testing tool ready to send custom TCP/IP packets and to show target answers. Attacker utilize the attack direction that flood means sent bundle as quicker and quicker and don't show answers, p 80 is target port number 192.168.43.125 is victim's individual ip address with SYN flags just and Rand-Source address mode.

5 Experimental Results

The SYN flooding assault may be a denial-of-service strategy that abuses the plan of the Internet's Transmission Control Protocol (TCP) three-way handshake for building up connections by debilitating a server's distributed state for a tuning in server application's pending connections, anticipating legitimate associations from being built up with the server application.



No.	Time	Source	Destination	Protocol	Length	Info
1870	2.405997	192.168.43.17	192.168.43.125	TCP	66	15793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1871	2.409514	192.168.43.17	192.168.43.125	TCP	66	18484 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1872	2.409515	192.168.43.17	192.168.43.125	TCP	66	15794 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1873	2.409633	192.168.43.17	192.168.43.125	TCP	66	18485 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1874	2.409634	192.168.43.17	192.168.43.125	TCP	66	15795 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1875	2.412258	192.168.43.17	192.168.43.125	TCP	66	18486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1876	2.412259	192.168.43.17	192.168.43.125	TCP	66	15796 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1877	2.412259	192.168.43.17	192.168.43.125	TCP	66	18487 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1878	2.412385	192.168.43.17	192.168.43.125	TCP	66	15797 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1879	2.412385	192.168.43.36	192.168.43.125	TCP	66	5695 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1880	2.412385	192.168.43.36	192.168.43.125	TCP	66	5696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1881	2.415295	192.168.43.36	192.168.43.125	TCP	66	5698 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1882	2.415295	192.168.43.36	192.168.43.125	TCP	66	5694 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1883	2.415296	192.168.43.36	192.168.43.125	TCP	66	5701 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1884	2.415421	192.168.43.36	192.168.43.125	TCP	66	5702 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1
1885	2.415422	192.168.43.36	192.168.43.125	TCP	66	5699 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM=1

Figure 6. Captured the Network Traffic of Victim OS with Wireshark

Figure 6 shows the network traffic that captured the pcap file with Wireshark using Wi-Fi network. There is huge no of TCP SYN packets are received in very short time.

Statistics

Measurement	Captured	Displayed	Marked
Packets	10076	10076 (100.0%)	—
Time span, s	23.786	23.786	—
Average pps	423.6	423.6	—
Average packet size, B	66	66	—
Bytes	667057	667057 (100.0%)	0
Average bytes/s	28 k	28 k	—
Average bits/s	224 k	224 k	—

Figure 7. Statistics Data for Captured File

Figure 7 presents number of packets, time span, average pps (packet per second), average packet size, bytes and average bytes/bits of captured traffic file.

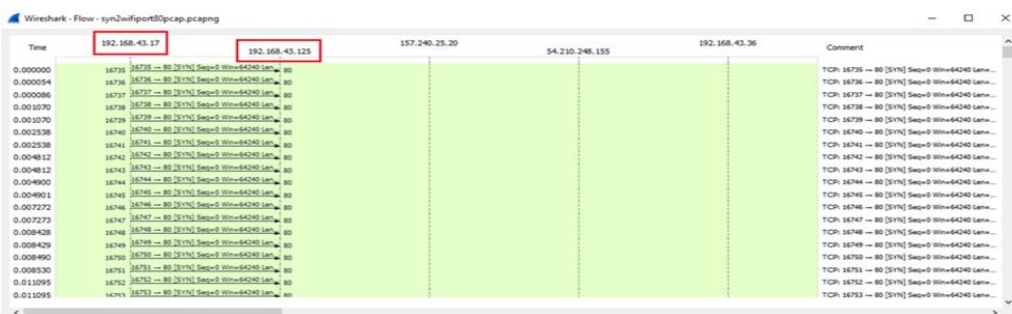
No.	Time	Source	Destination	Protocol	Length	Info
1863	2.402394	192.168.43.17	192.168.43.125	TCP	66	15789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1864	2.402494	192.168.43.17	192.168.43.125	TCP	66	18481 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1865	2.403344	192.168.43.17	192.168.43.125	TCP	66	15790 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1866	2.403513	192.168.43.17	192.168.43.125	TCP	66	18482 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1867	2.403641	192.168.43.17	192.168.43.125	TCP	66	15791 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1868	2.405994	192.168.43.17	192.168.43.125	TCP	66	18483 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1869	2.405996	192.168.43.17	192.168.43.125	TCP	66	15792 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1870	2.405997	192.168.43.17	192.168.43.125	TCP	66	15793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1871	2.405914	192.168.43.17	192.168.43.125	TCP	66	18484 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1872	2.405915	192.168.43.17	192.168.43.125	TCP	66	15794 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1873	2.409633	192.168.43.17	192.168.43.125	TCP	66	18485 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1874	2.409634	192.168.43.17	192.168.43.125	TCP	66	15795 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1875	2.412258	192.168.43.17	192.168.43.125	TCP	66	18486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1876	2.412259	192.168.43.17	192.168.43.125	TCP	66	15796 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1877	2.412259	192.168.43.17	192.168.43.125	TCP	66	18487 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1878	2.412385	192.168.43.17	192.168.43.125	TCP	66	15797 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Figure 8. Detecting TCP SYN Flood Attack (192.168.43.17)

No.	Time	Source	Destination	Protocol	Length	Info
1879	2.412385	192.168.43.36	192.168.43.125	TCP	66	5695 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1880	2.412385	192.168.43.36	192.168.43.125	TCP	66	5696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1881	2.415295	192.168.43.36	192.168.43.125	TCP	66	5698 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1882	2.415295	192.168.43.36	192.168.43.125	TCP	66	5694 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1883	2.415296	192.168.43.36	192.168.43.125	TCP	66	5701 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1884	2.415421	192.168.43.36	192.168.43.125	TCP	66	5702 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1885	2.415422	192.168.43.36	192.168.43.125	TCP	66	5699 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1886	2.415422	192.168.43.36	192.168.43.125	TCP	66	5700 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1889	2.416230	192.168.43.36	192.168.43.125	TCP	66	5697 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1890	2.416230	192.168.43.36	192.168.43.125	TCP	66	5703 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1891	2.416231	192.168.43.36	192.168.43.125	TCP	66	5704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1892	2.416231	192.168.43.36	192.168.43.125	TCP	66	5707 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1893	2.416231	192.168.43.36	192.168.43.125	TCP	66	5705 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1894	2.416232	192.168.43.36	192.168.43.125	TCP	66	5706 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1895	2.416232	192.168.43.36	192.168.43.125	TCP	66	5710 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1896	2.416395	192.168.43.36	192.168.43.125	TCP	66	5712 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Figure 9. Detecting TCP SYN Flood Attack (192.168.43.36)

In Figure 8 and 9, we found that 192.168.43.17 and 192.168.43.36 are sent large amount of SYN request to victim's OS in a few seconds. Most of the traffic which sent SYN request did not respond to SYN-ACK sent back from 192.168.43.125. ACK is not found in captured network traffic. So, there is a high chance of being DDoS SYN flood attack.

**Figure 10. Analysis of Flow Graph under TCP SYN flood attack (192.168.43.17)**

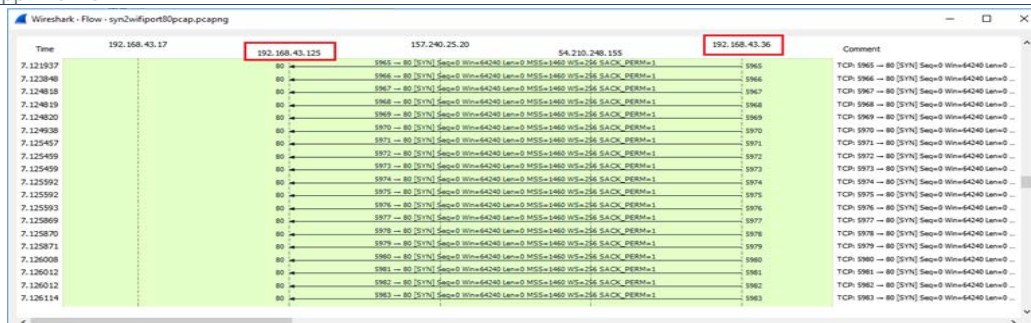


Figure 11. Analysis of Flow Graph under TCP SYN flood attack (192.168.43.36)

In Figure 10 and 11, we continue to analyze SYN flood attack with flow graph for sending from 192.168.43.17 and 192.168.43.36 to the victim IP. Attacker IP sent many SYN request continuously so victim do not have time to reply even SYN/ACK.

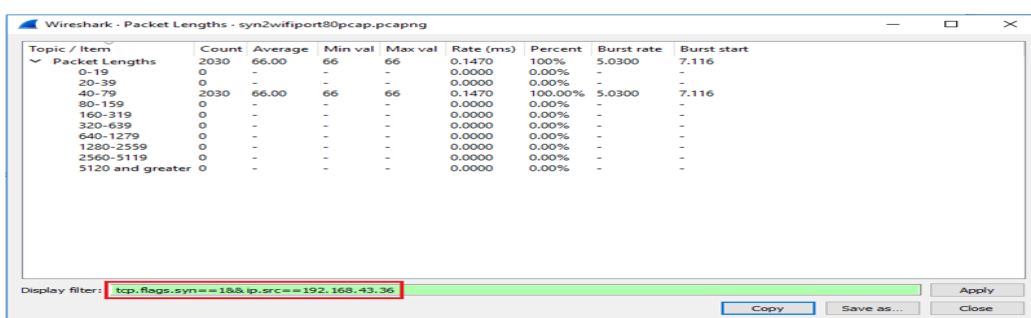


Figure 11. SYN Request Count for 192.168.43.36

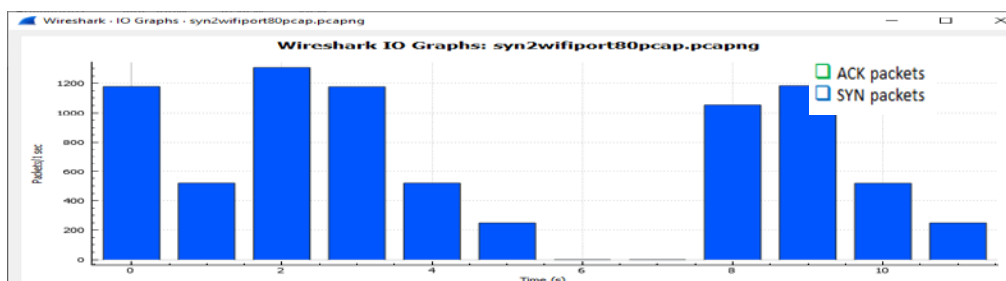


Figure 12. Detecting the ACK packet replied by attacker IP (192.168.43.17)

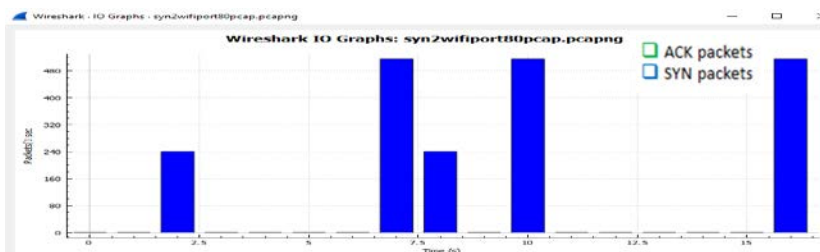


Figure 13. Detecting the ACK packet replied by attacker IP (192.168.43.36)

In Figure 12 and 13 shows the SYN and ACK packet in traffic for this IP. We are not found ACK replied from those IP. So, we decide this event is the TCP SYN flood attack from attacker two IP. The denial of service attack is identified here as SYN Flood attack.

6 Conclusion

Flooding assaults are major threats on TCP/IP protocol in anytime; most extreme assaults are started through TCP and misuse the assets and transmission capacity of the machine. Flooding assaults are DDOS (Distributed Denial of service) assaults and utilize the vulnerability of the network protocols. SYN flood attack abuses the 3-way handshaking of the TCP by sending numerous SYN request with IP spoofing method to victim have and deplete the accumulation line asset of the TCP and deny legitimate client to associate. Capturing the bundle flow is exceptionally critical to identifying the DOS attack. In this paper, we presented to completely appear and depict how perilous a focused on DoS/DDoS attack can be in the present innovative world through running the open source DDoS TCP SYN Packet Flooding and reproducing a DDoS attack, utilizing two Kali Linux virtual machines installed on VirtualBox, against a target network. Moreover, we successfully provide a simple experiment to detect a TCP SYN flooded attack and we can investigate the packet information and attacker IP on a victim site with a few second by using Wireshark. As a future work, we like to examine and provide the results for detecting botnet attacks on the Internet of Things (IoT) Network.

REFERENCES

- [1]. <https://www.oracle.com/>
- [2]. <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>, Last Accessed December 21, 2019.
- [3]. Zawoad, Shams, and Ragib Hasan. "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things." Services Computing (SCC), 2015 IEEE International Conference on. IEEE, 2015.
- [4]. E.S. Pilli, R.C. Joshi, & R. Niyogi. "A Generic Framework for Network Forensics". International Journal of Computer Applications (IJCA) (0975 – 8887) Volume 1 – No. 11, 2013.
- [5]. H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks", in Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM), volume 3, pages 1530-1539, June 23-27 2002
- [6]. Darren Anstee(2016), Denial of service attack data, Arbor Networks Inc
- [7]. Keyur Chauhan, Vivek Prasad, September, 2015, "Distributed Denial of Service (DDoS) Attack Techniques and Prevention on Cloud Environment", International Journal of Innovation and Advancement in Computer Science, Volume 4,210-215.
- [8]. K.Saranya, N.Aparna, June-2016, "Prevention of Vulnerability on DDoS Attack Towards Wireless Networks", International Journal of Merging Technology and Advance Research in Computing, Volume 4, Issue 14, 1-12.
- [9]. Snort.(2016):<https://www.snort.org/>
- [10]. OpenNebula.(2016):<http://opennebula.org/>
- [11]. Ms.K.Geetha , Dr.N.Sreenath "SYN FLOODING ATTACK – IDENTIFICATION AND ANALYSIS" International Conference on Information Communication & Embedded Systems (ICICES 2014)
- [12]. Rizal, R., Riadi, I. and Prayudi, Y., 2018. Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. Int. J. Cyber-Secur. Dig. Forensics (IJCSDF), 7, pp.382-390.