An overall study on DDoS Attack & its Protection

BY

PRANABESH MAJUMDER
ID: 193-25-820

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

SHAH MD. TANVIR SIDDIQUEE
Assistant Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JUNE 2021

APPROVAL

This Project titled "**An overall study on DDoS Attack & its Protection**", submitted by Pranabesh Majumder ID No: 193-25-820 to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 03-June-2021.

BOARD OF EXAMINERS

____

Dr. Touhid Bhuiyan **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Md. Ismail Jabiullah **Internal Examiner**
Professor
Department of Computer Science Engineering
Faculty of Science & Information Technology
Daffodil International University

____

Dr. Sheak Rashed Haider Noori **Internal Examiner**
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information T+622echnology
Daffodil International University

Dr. Shamim H Ripon
Professor
Department of Computer Science and Engineering
East West University

External Examiner

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Shah Md. Tanvir Siddiquee, Assistant Professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Tsiddique

Shah Md. Tanvir Siddiquee
Assistant Professor
Department of Computer Science and Engineering
Daffodil International University

Submitted by:

Name: Pranabesh Majumder
ID: 193-25-820
Department of Computer Science Engineering
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Shah Md. Tanvir Siddiquee**, **Assistant Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of network security to carry out this project. His endless patience ,scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Head**,** Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

The project “**An overall study on DDoS Attack & its Protection**” is based on network security as it’s a now-a-days most important issue in the current internet world. The purpose of this project to know about a one kind of networking attack like DDoS and how it acts during an attack and how can we take steps against it for both theoretically and network device appliance level. The overall project is divided into two main modules. First, we have developed an simulation system where we had shown how a DDoS attack is executed over a server and how it behaves during the attack. Here, I uses VMWare Workstation and Kali Linus OS which then we cloned for demonstration of the attack. Second, I’ve developed the proposed solution of my own against DDoS attack and also appended the solution of different network vendor in the world. If anyone take steps against DDoS attack he/she should take measures for both theoretically and appliance level. Because no one knows how can they became attack against their system or network. So, I think if anyone take steps against from both criteria we’ll be kept ourselves safe from such a dangerous attack in the internet world like DDoS.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES **PAGE NO**

CHAPTER 1

Introduction

1.1 **Introduction**

The Internet has revolutionized the computer and communications world like nothing before. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure [1]. Almost all the traditional services such as banking, power, medicine, education and defense are extended to Internet now. The impact of Internet on society can be seen from the fig. 1.1 which shows exponential increase in number of hosts interconnected through Internet [2]. The increasing rate of internet usage rising in such a way that every institution like government, organization and people are very much depends on its without any hesitation.

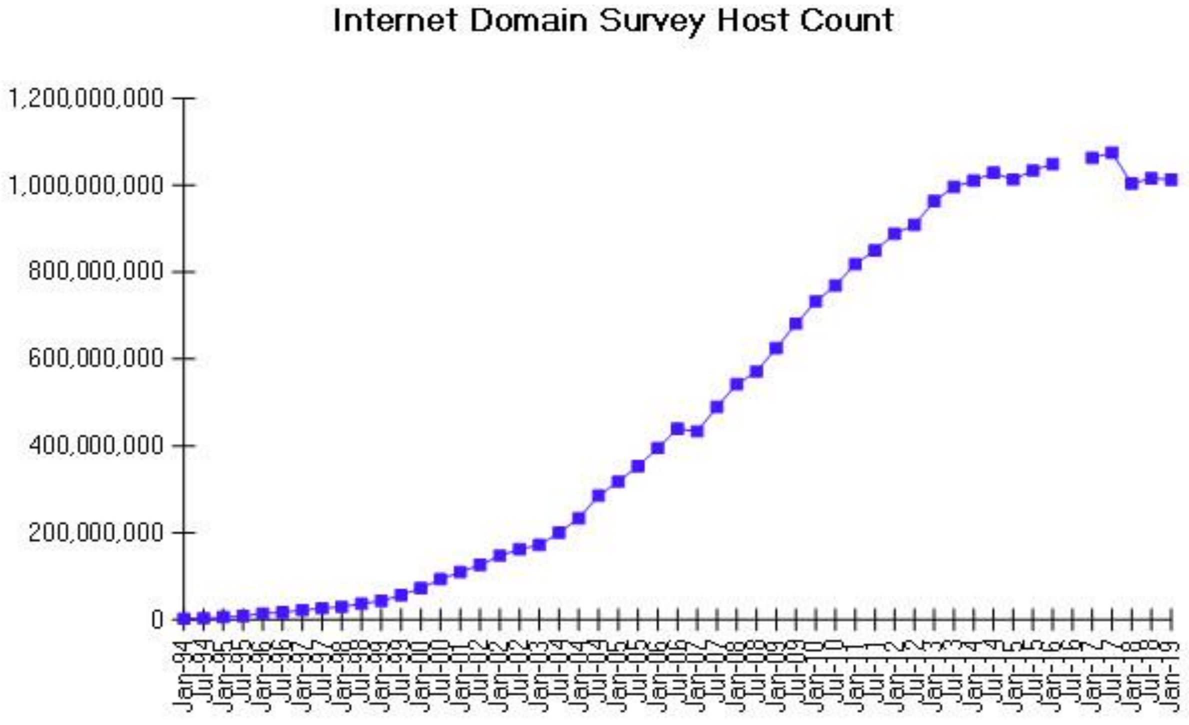


Fig 1.1: Internet Domain Survey Host Count [2].

As a consequence, when the number of host has increased and then the number of attacks also rising at the same time. As a result, most of the attacks and vulnerabilities are not recorded every year. Now-a-days, DDoS attack is the most familiar and extreme threat to our internet world. In a DDoS attack, an attacker mainly target a specific website/network and he/she intentionally sends a huge amount of malicious traffic that causes the website/network unavailable/unresponsive for a period of time and it's intends user then unable to access the resources of that website which may consume enough bandwidth at the same time. DDoS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user [3].

A DDoS attacker uses many machines or tools to launch a coordinated DOS attack against one or more targets [4]. It can be executed by using many compromised computers by sending a huge amount of traffic to consume the maximum resources of the victim. As a result, they continuously uses maximum bandwidth of the website and jamming the network so that user can't access the resources which affected the normal internet traffic also. The number of DDoS attack has been alarmingly increasing for the last few years [5]. Many of today’s DDoS attacks are carried out by organized criminals targeting financial institutions, e-commerce, gambling sites etc [6].

A classification of a wide range of DDoS attacks found in the wild is presented in [3, 7] that Internet providers and users need to be aware of. Usually, it can be launched in two forms [8]. The first form can use the software vulnerabilities by sending huge traffic which then keep the system down. The second form also consumes high bundle of traffic which make the system slow and it cannot working properly for its users. Here, when an attack happened it can then consumes of any systems resources like the systems network bandwidth, disk space, CPU uses, memory etc.

This paper describes the overview of DDoS attack, DDoS attack history, available DDoS attack tools and its detection method, simulation of a DDoS attack, discuss the possible prevention solution for different vendor like Cisco, Palo Alto, Fortinet, Check Point, Cyberoam etc. Section II describes briefly the overview of DDoS attack where section III presents how DDoS attack happened in a VM and its consequences. Section IV contains available DDoS attack tools and the detection method in the details. Details of available DDoS prevention mechanisms for different vendor like Cisco, Fortinet, Palo Alto is elastrated in section V and protection also. Finally, Section VI concludes the paper and presents further future scope, if any.

1.2 Motivation

During my M.Sc in Daffodil International University I was also a service holder. Sometimes after a long tiring day of office I had to go to the university just to participate in a class test arranged by course teacher. It was very hard for me. But last few semester I was attend the class and exam in a online platform named “BLC”. It’s also difficult for me to attend the class. As I’m responsible for network related jobs in my organization and now-a-days security is the main issue to secure the online world that’s why I think we should alert for such a attack like DDoS and how can we mitigate it from this. Internet is growing day by day and its spreading among every people that consequences the watery supplication of Internet tools and software to use for their own purposes.

Hackers are the main threat to delivery hacking tools to exploit the vulnerability of Internet Objects. They are extending to deploy the protocol of “Anonymous” which is being the greatest threat to this modern World. So, I need to think like hackers to split their thoughts and to make the possible solution of DDoS Attack.

1.3 Scope of the Work

Many Organizations now a day are moving their business to the Internet or Virtual World. Every businessman / businesswoman is targeting to establish their whole system to the Internet. By the grace of Internet blessings of Facebook, twitter, Google, Linked-In etcetera are enhancing in such a way that the social media and workers are not going too and far for collecting any information because of Internet Things. So, scopes of this work are elaborating undoubtedly.

Scope of the work:

a. Government Information Security

b. Social Media

c. Business administration

d. Commercial Area

e. Corporate section

f. Developing System

g. System Administration

h. Maintenance of Products Details

i. Security of Information such as:

1) Agencies

2) Administration

3) Bureau

4) Investigation

j. Unavoidable Exploitation

These are the arsenal scope to develop the entire security system for preventing or mitigating denial of service attack.

1.4 Objective of the Project

The objectives of this project work is as under:

I. Learn about overall DDoS attack in all perspective like history, tools, types of DDoS.

II. How a DDoS attack will encounter in the system? What's the system condition during DDoS attack by using a simulation?

III. Enhanced network security against DDoS attack

IV. Familiar with different DDoS attack tools and detection method.

V. Detection and protection of DDoS attack from different vendor like Cisco, Fortinet, Palo Alto, Check point & Cyberoam etc.

VI. Up to date about DDoS attack and do work for future scope, if any.

1.5 Expected Outcome

As I’m responsible for network related jobs in my organization so that I’ve to think about the network security also to protect all kinds of network related attack and should ensure the confidentiality and security of my system. Such a project helped a lot about the world’s most dangerous attack like DDoS and how to ensure system & network security and keep the up time of the system in a maximum level. I’ve developed a solution from this attack from different vendors’ perspective also.

1.6 Report Layout

Chapter 1: Introduction

In this chapter I have discussed about the introduction, motivation, scope of the work, objective of the project and expected outcome of the project and report layout.

Chapter 2: Background Study

Here I have discussed about the overall background study of our project. I have also discussed about the history of DDoS, its types and challenges of the project.

Chapter 3: Simulation of a DDoS attack

In this chapter we’ll show how a DDoS attack will encounter a system and what happened of a system when a successfully DDoS attack is triggered.

Chapter 4: DDoS attack Tools & detection method

This chapter contains about what are the different types of DDoS attack tools and how can we detect it during the attack.

Chapter 5: Proposed plan to protect from DDoS attack

Here, I‘ll discuss regarding my own proposed solution against DDoS attack and how we protect out network & system from DDoS attack by using different vendors like Cisco, Fortinet, Palo Alto, Check Point & Cyberoam in a various stage of this attack like before and after of the attack.

Chapter 6: Conclusion

In my last chapter, I’ve discussed about the conclusion which pretty much derive about the project.

CHAPTER 2

Background Study

2.1 Introduction

A DDoS attack is one in which a multitude of compromised computer systems attack a selected target, thereby causing denial of service for legitimate users of the targeted system [9]. As we already know that a DDoS attack can overload any affected systems resources at its high level to keep the system unavailable/unresponsive. The attackers bombard scare resource either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource [10]. The following figure 2.1 represents the DDOS attack scenario which is illustrates below [12]. First of all, an attacker wants to find a vulnerability of a computer system and then making it as the DDoS master. From that master system the attacker again try to contact with other computer systems and continuously trying to make it as a compromised system. After that, the attacker/hacker cumulatively load the strong DDoS attack tools & equipments to attack the system on that compromised computer systems. Finally, the attacker/hacker can instruct to all the compromised computer systems to initiate the flood against a particular target/website/network. Some DDoS attacks utilize Internet worms to automate the process of exploiting and compromising computer systems, as well as launching DDoS attacks [11].

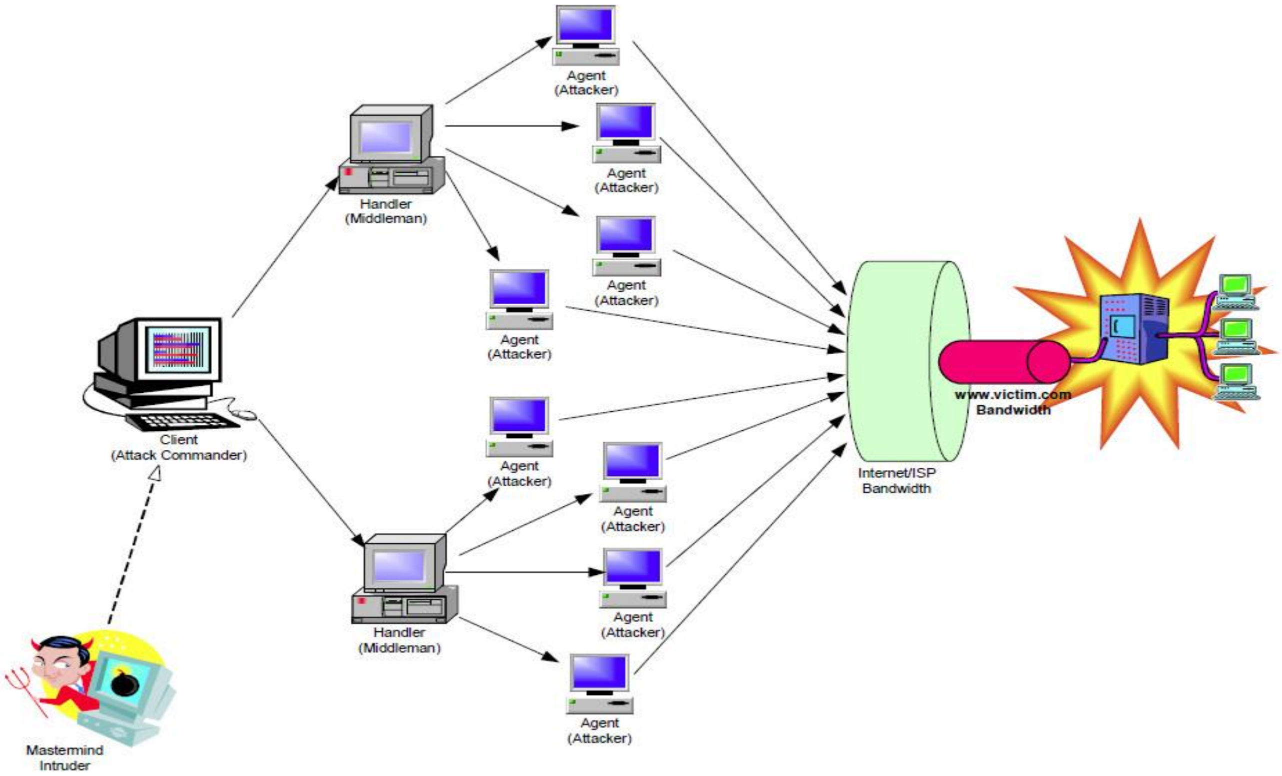


Figure 2.1: A typical DDoS attack

2.2 History of DDoS Attack

Over the last two decades, there is an enormous changes in the IT industry regarding the advancement of various cyber-attacks. The threat of DDoS attack is then increasing and evolving thereafter. DDoS attack is one of the oldest and the dynamically advancing phase of cybercrime. These attacks can helps to hackers' in a high level creativity to create complicated and dynamic threat for who are responsible for cyber security. The first ever DoS attack occurred in 1974, when a 13-year-old boy called David Dennis wrote a programme that remotely locked up multiple terminals in a university computer lab [12]. He successfully managed to shutdown 31 PLATO terminals by writing a programme that sent a problematic command [13]. In the early 2000s, DoS attacks can be done from a single machine to a single target which is executed from a keyboard entries. When it becomes ineffective then such an attack converted from manual to semi-manual.

In 1996, a New York-based Internet Service Provider (ISP) Panix recorded the DDoS attack which is a SYN flood attack. The attacker overloaded the company's server by sending a huge amount of spoofed IP address traffic which then forcedly stop the normal traffic. Panix managed to recover in around 36 hours, but this event was significant for being one of the first major DDoS hacks [13]. After 36 hours Panix was recovered their system successfully and then it was considered as one of the most major DDoS attacks. Several years later, in 1999, a hacker managed to completely disable the University of Minnesota's internal network for more than 48 hours with a massive UDP flood. It was the first large-scale attack through a specialized tool called Trinoo [13].

The Michael "Mafiaboy" Calce considered as the most notorious DDoS attacker. In 2000, he executed a DDoS attacks against world's most top companies like CNN, Yahoo, Amazon, Dell, eBay, and FIFA. The then-teenager used a tool called TFN2 that makes use of previously infected computers to generate a huge amount of fake traffic to a server [13]. The largest DDoS attack is listed below year by year:

i. **The February 2020 attack reported by AWS:** AWS reported a massive DDoS attack in February of 2020. At its peak, this attack saw incoming traffic at a rate of 2.3 terabits per second (Tbps). AWS did not disclose which customer was targeted by the attack [15].

ii. **The February 2018 Github DDoS attack:** In February 2018, GitHub experiencing its largest DDoS attacks which is mainly used by developers' worldwide. This attack reached 1.3 Tbps, sending packets at a rate of 126.9 million per second [14].

iii. **The September 2017 Google services attack:** The biggest DDoS attack happened in September of 2017. Google services was targeted in this attack and reached 2.54 Tbps and sent spoofed packets to 180,000 Google various web servers. Google Cloud disclosed the attack in October 2020 [14].

iv. **The 2016 Dyn attack:** Another massive DDoS attack was directed at Dyn, a major DNS provider, in October of 2016. Many major sites was suffered due to this attack including Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub. This was done by using the malware called Mirai which creates a botnet out of compromised Internet of Things (IoT) devices such as cameras, smart TVs, radios, printers, and even baby monitors. To create the attack traffic, these compromised devices are all programmed to send requests to a single victim [14].

v. **The 2015 Github attack:** GitHub faced a largest DDoS attack ever in its history in 2015. Such a DDoS traffic was created from China and its main target was the two GitHub projects. The attack traffic was created by injecting JavaScript code into the browsers of everyone who visited Baidu, China's most popular search engine [14].

vi. **The 2013 Spamhaus attack:** In 2013, Spamhaus also faced the largest DDoS attack ever in its history. Spamhaus is basically works for spam filtering of emails which make them the easier target of an attacker. The attack drove traffic to Spamhaus at a rate of 300 Gbps [14].

vii. **The 2007 Estonia attack:** In 2007 April, the attacker attacks Estonia's government services like financial institutions, and media outlets. Such an attack was considered as the major DDoS attack in their history so far. This had a crushing effect since Estonia's government was an early adopter of online government and was practically paperless at the time; even national elections were conducted online [14].

Now-a-days, world's internet system is increasing dramatically and growing faster. So we should need for more safety and prepare before the attack to keep protect from this. For just the first half of 2020, there were over 4.83 million DDoS attacks. Such a number already increases for 2019 on a larger scale. We can only expect the trend to continue in 2021 and beyond [15].

2.3 Types of DDoS Attack

Distributed Denial of Service (DDoS) attack is one of the most popular, rising attack method of hackers. There are three common classes of DDoS attack which is appended below:

a) Volumetric-based attack: It uses massive amount of traffic which can inundate the network bandwidth of the target. Example: ICMP flood, NTP/DNS amplification.
b) Protocol/Network attack: Exploits the vulnerability in the network or layer 3 & transport layer 4 protocol in an OSI layer. Example: SYN flood, Ping of death, Smurf attack.
c) Application attack: Such an attack is based on web application and are deliberated as the most modern and major types of attacks. Example: HTTP/SMTP/SIP flood etc.

As we can see in above DDoS attacks has different categories where there is a various attacking method involved for targeted a specific network or systems. Now, we enlisted typical popular types of DDoS attacks which is given below:

i. **SYN flood attack:** This is the most common DDoS attack and by using this attack a hacker basically uses the vulnerability of the TCP three-way handshake process and consume more memory space which is previously allocated by OS. In a normal TCP/IP session there is a three steps needed to establish a successful connection between a host & client and this three steps here called as three-way handshake process. In this process, client first requests the server by sending a SYN. Server receives and acknowledge the client's request by sending a SYN-ACK message. Finally, client responds to the server with an ACK (Acknowledge) message, and then the connection being established between the client and server. In a SYN flood attack, an attacker sends a huge packet to the targeted server where the source address is a spoofed IP address. After that, when the target server trying to process all of these bad request it will then cannot process the actual requests and as a result it will then unresponsive to its known users. Here, attacker motive is to down the target system by sending a huge number of SYN bad IP packets to the target system. As a result the target machines memory which leads the target machine crash, slow response, hang or rebooted the system.

ii. **ICMP (Ping) flood:** ICMP (Ping) flood is also considered as Ping flood. In this attack, the attacker flood the target system by executing a huge number of ping or ICMP request which uses all the bandwidth of the victim and resulting a significant overall system shutdown. It only happened if the hacker has more bandwidth than the target system.

iii. **UDP flood:** A UDP flood is such DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP ‘Destination Unreachable’ packet [16].

iv. **HTTP flood:** This sort of attack is the most common forms of attacks which actually generates huge HTTP requests to the web server which floods the server. HTTP flood is considered as the form of application centric bandwidth attack and here the common HTTP port 80 is being used to initiate the attack.

v. **SIP flood:** Like HTTP attack SIP (Session Initiation Protocol) flood is also an application centric bandwidth attack where the attacker targets the SIP proxy server which is used for making VoIP call.

vi. **Teardrop attack:** This attack utilized vulnerability in the earlier Microsoft Operating Systems and some older versions of Linux whereby improperly framed or overlapping IP fragments were sent to the victim thereby crashing it [17].

vii. **Smurf attack:** Smurf attack is identical to the Brute Force DoS attack where a huge ping requests are sent to the network (normally the Router) in the target network by using bad IP addresses. When the router receives a ping request it will then try to route it or echo it back and as a consequence the server/network is overflowed/flooded with huge number of packets and congestion the traffic also. If there is a large number of nodes, hosts etc. in the network, then it can easily collapse the entire network to process all the ping requests. In this attack, the attacker uses IP protocols and ICMP using a malware program which is called Smurf.

viii. **Permanent Denial of Service:** This type of attack is generally known as "Phlashing". By this attack, it can permanently destroy the hardware of the victim resources.

ix. **Infrastructure attack:** This type of attack can target the infrastructure of internet such as DNS root server and by this attack attacker can potentially bring down the entire internet.

x. **Zero-day DDoS attack:** Zero-day DDoS attack is the name given to new DDoS attack methods that exploit vulnerabilities that have not yet been patched [18].

A specific DDoS attack can hamper any system/network/website by using its feature. So, after the attack we can identify the types of DDoS attack which can severely damage any system/network.

2.4 Challenges

- Time management is one of the key challenges of the project.
- To show a DDoS attack in a live system is quite impossible that's why try to show an attack in a VM and had to work hard on VM to learn new things to implement it.
- Lack of hardware resources like internet speed, memory system of remote PC/VM etc.
- Protection system overview of a live hardware devices.
- It is almost impossible to show the protection for different network vendors in a live network infrastructure.
- To cover all related information regarding DDoS attack.

Evolution of DDoS attack extremely increasing day by day and the prevention of losing information through the internet is needed its solution as soon as possible. It needs a very mandatory step to take a hard hand solution for protecting our valuable information from the thief of Internet Service. There are various types of attackers who are very fugitive to steal the Information and hide away by spoofing their identity. Many steps have been taken as a solution has studied but, in every way, they may not be succeeded at all. So, studies about DDoS attack, type of attackers, their methods, thinking strategies and the possible solutions which can be mitigated most of the prevention against DDoS attack is our fundamental resources to estimate our achievement.

CHAPTER 3

Simulation of a DoS/DDoS Attack

3.1 Introduction:

Now-a-days, the DoS/DDoS attacks are the most ordinarily used network attacks where the attacker getting the victims IP address and intentionally or temporarily unresponsive/unavailable of the victims other network resources, machine, website to its known users by causing the consume more of its bandwidth. The difference between denial of services (DoS) and distributed denial of service (DDoS) attacks is that "an attacker run the DoS attacks from a single source while DDoS attacks are distributed and run from a multiple sources to a single target". By executing a DoS/DDoS attacks, the victims network/resources generally flooded with various types of packets like TCP, SYN flood etc. in a network layer or with requests HTTP, POST etc. in a application layer. During a DoS/DDoS attack the victim couldn't make any communication for its users by using its resources until the attacks stops.

In this chapter, I have showed a simulation of DoS attack by using an open source TCP SYN flood Python script which is run on my computer on the Kali Linux OS in a VM which is also installed on VMWare Workstation, after executing the Dos attack I'll show that my target website unavailable or it takes more times to load. Such a Python script (TCP SYN packet flood), actually floods the target website with SYN packets in the layer 3 and using the TCP protocol & port 443 which keeps the website/network unavailable for long time where it consumes more bandwidth at the same time. My DoS attack is a locally hosted in my PC where the attacker host used as Kali Linux OS in a VM and the targeted website run on the cloned Kali Linux virtual machine which uses same network and subnet as well. The Kali Linux OS initiate the DoS attack by using Python DoS script to flood the targeted website through port 443 and TCP connections also. May be an attacker intends to execute a DoS/DDoS attack against a server as a means of revenge, politics or other purposes but in my simulation I just show a DoS attack against a website inside a virtual machine how it behaves during a DoS attack, the actual condition of a web server and it then takes more times to load. As a proof, here I capture packet for both virtual machine (attacker host) and victim host which shows a SYN packet flood attack from source to destination. In a real world, a website/network keep up itself during a DDoS attack mainly depends on an attacker because an attacker knows how much packet he/she can flooding against a server/network and how long time he/she intends to down the network at the same time. Here, I flood the DoS script against the website for a few minutes and after that the targeted website was down for a few minutes and it then take more times to load as it was. I think we'll understand it in my later part of the report and for the better understanding I will attach a video in PMIS portal to show the full demonstration of the DoS attack. Also, note that, here I demonstrate DoS instead of DDoS because we already know DDoS attack only executed from a multiple source where DoS attack only executed from a single source to a target website/network/server.

3.2 My SYN Flood DoS Simulation:

My DoS attack simulation mainly a TCP SYN packet flood based on Python script where an attacker machine floods the targeted website (hosted in a cloned VM) by using TCP protocol and port 443 after getting the IP address of the target website. Here, I uses the Linux based OS so that to find the IP address I've to type "ifconfig" in the Kali Linux terminal and to find the target website IP address I've to ping the target website full address from my attacking VM. Moreover, to execute the TCP SYN packet flood DoS attack against a website here mainly the TCP SYN absorb the conventional three-way handshake process to down the target website which then force the server to use its maximum resources and bandwidth and which makes the server/website/network temporarily unavailable/unresponsive or take more time to load in its normal condition for its intends users.

How a TCP Three-way handshake process works:

1. Client first requests the server by sending a SYN.

2. Server receives and acknowledge the client's request by sending a SYN-ACK message.

3. Finally, client responds to the server with an ACK (Acknowledge) message, and then the connection being established between the client and server**.**

In a TCP SYN flood DoS attack, the "attacker continuously sends SYN packets to every port of the server, of the targeted network or server" and the targeted server/network then busy to handle the huge amount of such requests.

In my cases, when I continuously executed the TCP SYN DoS flood packet against the targeted website and the target website unable to handle all the packet due to failure of this TCP three-way handshake process and it then take more time to load and I've also found the SYN packet when I've capture the packet by using Wireshark. However, the entire DoS simulation attack was run and contained inside the VMware Workstation on my physical machine so that there was no actual damage happened to the targeted website (https://www.hackertyper.com). My DoS attack is a locally hosted in my PC where the attacker host used as Kali Linux OS in a VM and the targeted website run on the cloned Kali Linux virtual machine which uses same network and subnet as well. The Kali Linux OS initiate the DoS attack by using Python DoS script to flood the targeted website through port 443 and TCP connections also. As I earlier mentioned that, my main goal to demonstrate a DoS attack and how a targeted website behaves when it under attack and what's the actual condition happened during an attack and lastly as a proof I using Wireshark which will help me to capture the packet during such a DoS attack for both attacking VM and cloned VM where the targeted website running.

3.3 How to SYN Flood DoS Attack Simulation Works:

First of all, I’ve install Kali Linux OS in my VMware Workstation to conduct the DoS attack. After that, I've cloned the real Kali Linux virtual machine to create another cloned VM with the same configuration so that my both virtual machine (attacking & cloned) hosted on my PC which uses same subnet and network also where the main Kali Linux virtual machine initiate the DoS attack by using Python script against the target website which is running on the cloned Kali Linux VM. At this stage, I've download and install the latest Python3 inside the attacking VM to execute the DoS attack by using the Kali Linux terminal and then launch the Python script at the same VM. Now, in my attacking virtual machine I've to execute "ifconfig" command to find the IP address of the attacking VM and then pinging the targeted website from the attacking VM by using Kali Linux terminal which is run on the cloned Kali Linux VM. After that, to execute the DoS attack I've to enter the target website IP address, it's port number (here 443) to flood and default packet rate 135 and then hit the "ENTER", which then spontaneously flood the target website with SYN packets by the layer 3 and TCP protocol. In my TCP SYN flood DoS attack simulation, the targeted website successfully unresponsive/unavailable for some time and takes long time to response/load. Due to my computer hardware configuration and internet speed the targeted network in this regard temporarily unavailable and it takes long time to load the website instead to fully shutdown the system after executed the DoS script. In order to make sure my TCP SYN flood DoS attack simulation working properly I've uses Wireshark packet capture log on both virtual machine (attacking & cloned VM). If we analysis the packet we've definitely say that the attack is successfully executed from attacking VM to cloned VM where the targeted website flooded by using the TCP SYN flood packet which is mainly based on Python script.

3.4 SYN Flood DoS Attack Simulation: Step by Step “How To Do”

In this section, I’ll describe how to DoS attack simulation was executed step by step which is appended below:

1. Download and install VMware Workstation 16 Pro from an online source (ex. https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html).

2. Download the Kali Linux OS (.ISO format) from internet by following URL (ex. https://www.kali.org/downloads/).

3. Now, install the Kali Linux OS by escalating the .ISO file or through VMware Workstation settings.

    - ✓ **Mounting .ISO:** Open VMware Player → Click on "Create a New Virtual Machine" → Select "Installer disk image file(.iso)" and locate the Kali Linux .ISO file → Select "Guest operating system" as Linux and Version as Debian 10.x 64-bit → Provide Virtual machine name as "Kali1" and locate the virtual machine → Specify disk capacity → Click "Finish".

    It takes more time to successfully setup the Kali Linux OS on the VMware Workstation.

4. Now, clone the virtual machine from Kali Linux OS.

    - ✓ Right click on the Kali Linux VM →Manage → Click “Clone” →Next → Select “Clone” from "The current state in the virtual machine" → Select “Clone method” as "Create a full clone" → Keep the VM name as same and locate the previous virtual machine location →Click "Finish" and Continue and then click Close.

5. Launch the both original and cloned VM Kali Linux OS by VMware Workstation.

6. Download and install the Python3 version inside VMware Workstation on the VM OS being used to initiate the TCP SYN flood DoS attack.

    - ✓ Click the Kali Linux Terminal → Type “sudo apt-get install python3”

7. Download and copy the .zip folder which holds the TCP SYN Packet Flood Python (.py) DoS script files to the Desktop of the attacking Kali Linux OS VM at (https://github.com/cyweb/hammer).

8. Now, launch the Python DoS script file (which we named DoSGroupA.py) after extracting by using the Kali Linux Terminal:

    - ✓ In Kali Linux Terminal, type “cd Desktop”→“cd DoSGroupA” →“python3 DoSGroupA.py”

9. To find the IP address of the target system pinging the targeted website from the attacking Kali Linux Terminal (“ping Enter URL”)

10. Now, execute the DoS attack following way:

    - ✓ Enter the target's IP address ("-s ip address"), target's port number ("-p 443"), and packet flood rate ("-t 135") (default is 135).

11. Hit ENTER button from keyboard and the script will begin to flood the target's website with TCP SYN flood packets which is based on python script.

12. The targeted website unavailable/unresponsive for sometime and it takes more time to load.

    - ✓ Now, trying to load the targeted website and monitor the capture log file on Wireshark on both attacking VM & cloned VM.

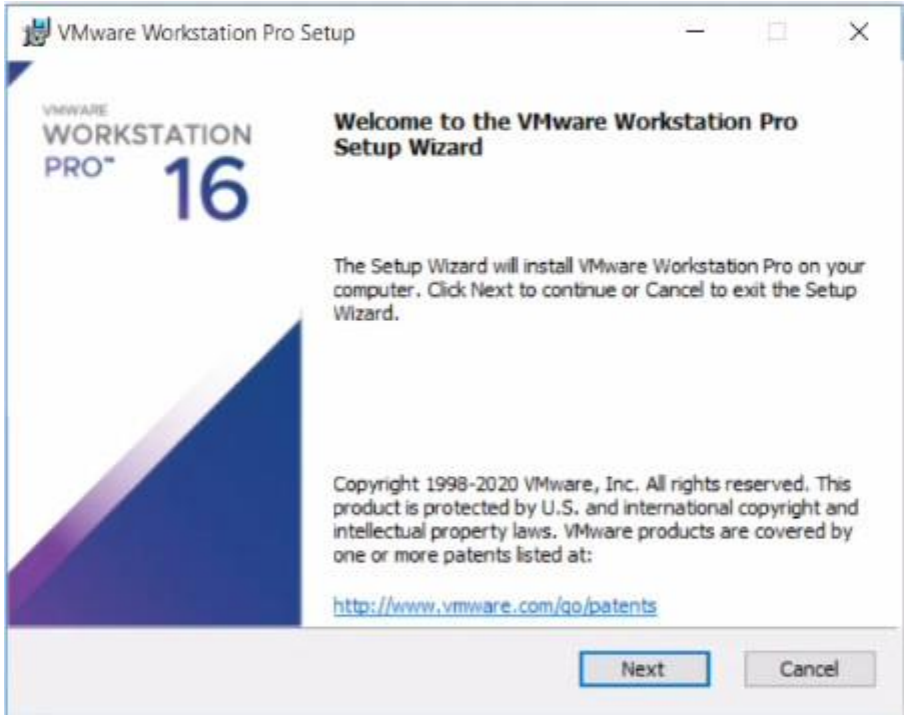
13. By cancelling the attack press Ctrl + C in the Kali Linux Terminal on the attacking VM or close the Terminal to stop the attack.

In my case, it's take more time to load or response due to my computer internet speed and as well as my computer hardware configuration.

In above discussion, I've illustrates the steps of the overall setup procedure and execution of the DoS attack inside the VM.

3.5 SYN Flood DoS Attack Simulation: Evidence, Results, and Verification:

First of all we download both the VMware Workstation 16 pro and Kali Linux .ISO file from the internet and setup them step by step.



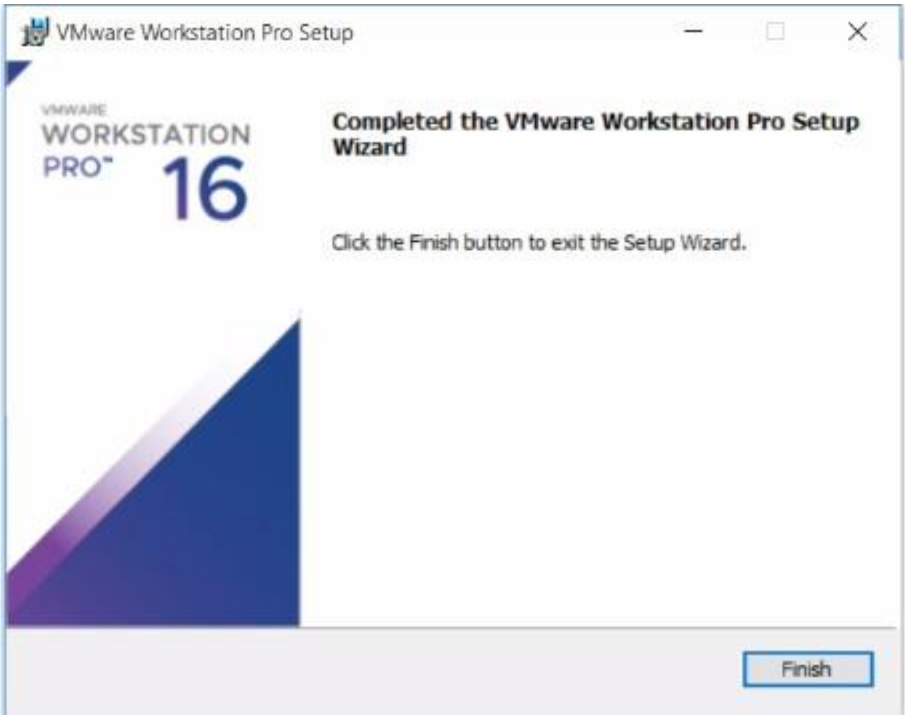
Welcome to the VMware Workstation Pro Setup Wizard

The Setup Wizard will install VMware Workstation Pro on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright 1998-2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at:

http://www.vmware.com/go/patents

Figure 3.5.1: Initial screen of install VMWare Workstation 16 Pro.

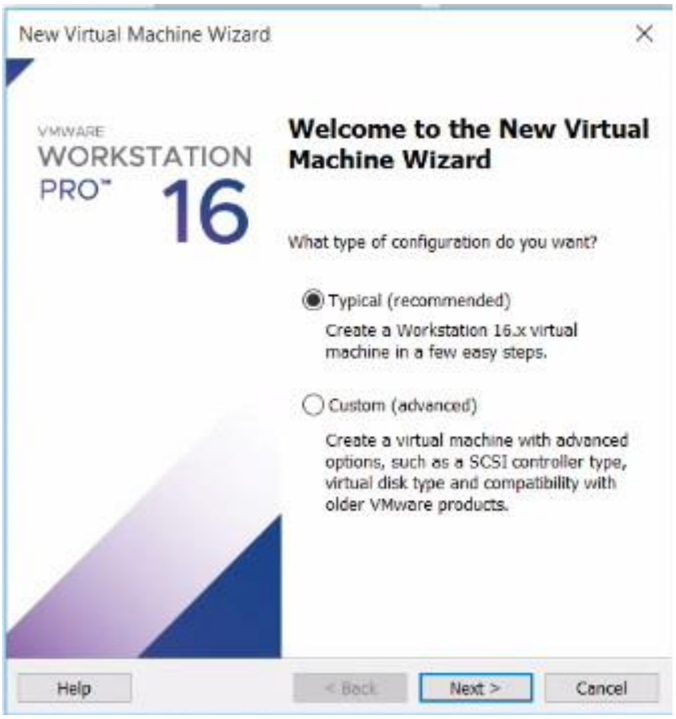


Completed the VMware Workstation Pro Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 3.5.2: Installation completion of VMWare Workstation 16 Pro.

New virtual Machine Kali OS setup by using .ISO file which is appended below:



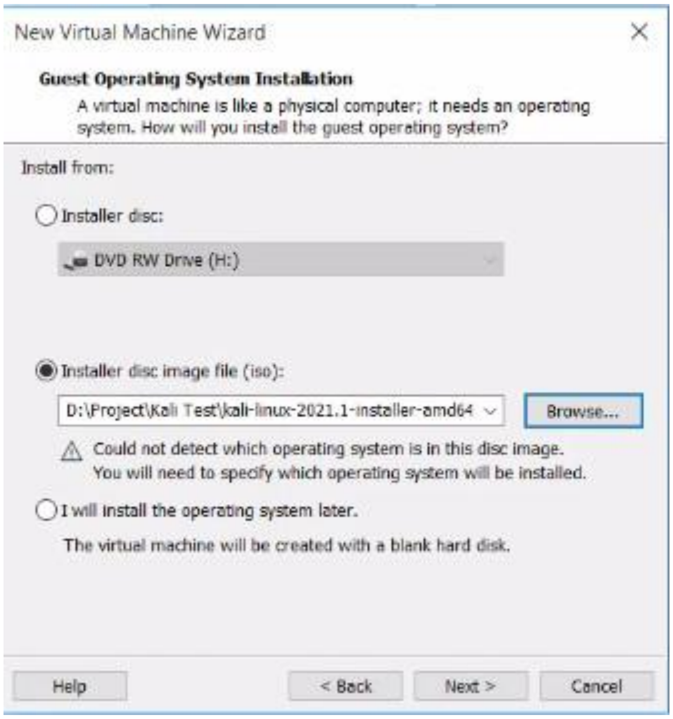
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)
Create a Workstation 16.x virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Figure 3.5.3: Initial screen of installation of Kali Linux OS.



Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

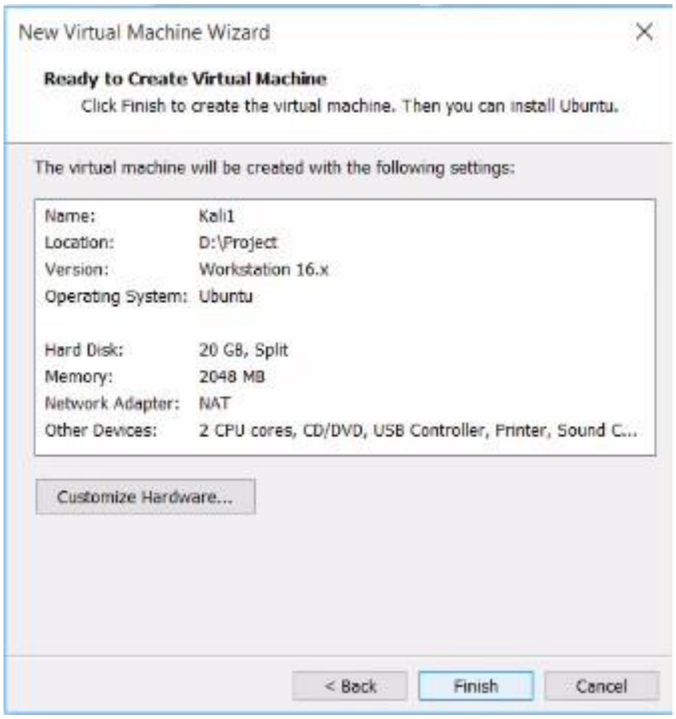
○ Installer disc:
DVD RW Drive (H:)

● Installer disc image file (iso):
D:\Project\Kali Test\kali-linux-2021.1-installer-amd64

Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

○ I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Figure 3.5.4: Locate the Kali Linux OS by mounting .ISO file


New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Ubuntu.

The virtual machine will be created with the following settings:

```
Name:              Kali1
Location:          D:\Project
Version:           Workstation 16.x
Operating System:  Ubuntu

Hard Disk:         20 GB, Split
Memory:            2048 MB
Network Adapter:   NAT
Other Devices:     2 CPU cores, CD/DVD, USB Controller, Printer, Sound C...
```

Figure 3.5.5: Ready to create Virtual Machine.

After creation of Kali Linux by .ISO file now we configure the Kali Linux for its final outlook where we illustrates few screenshots of it which is appended below:

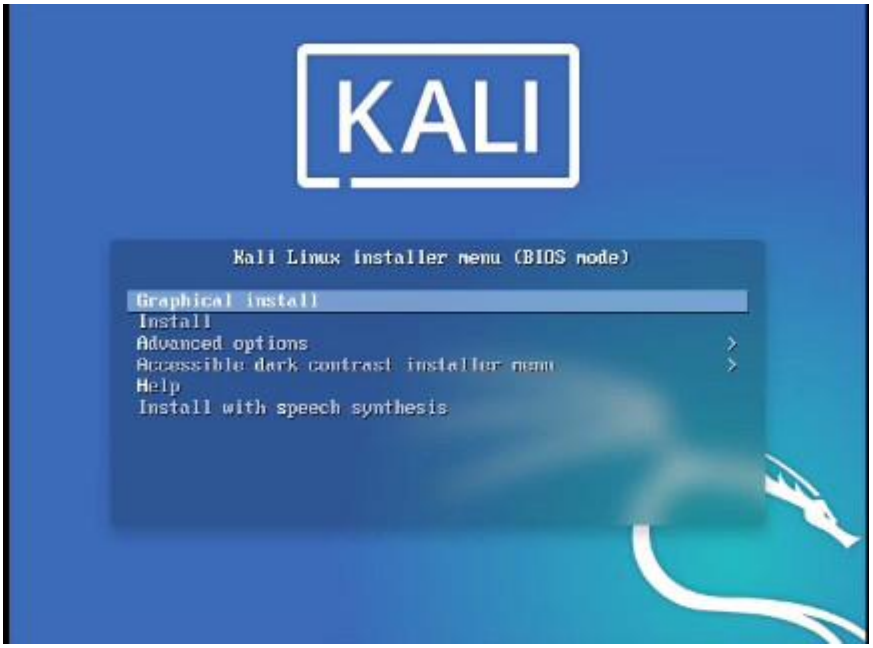
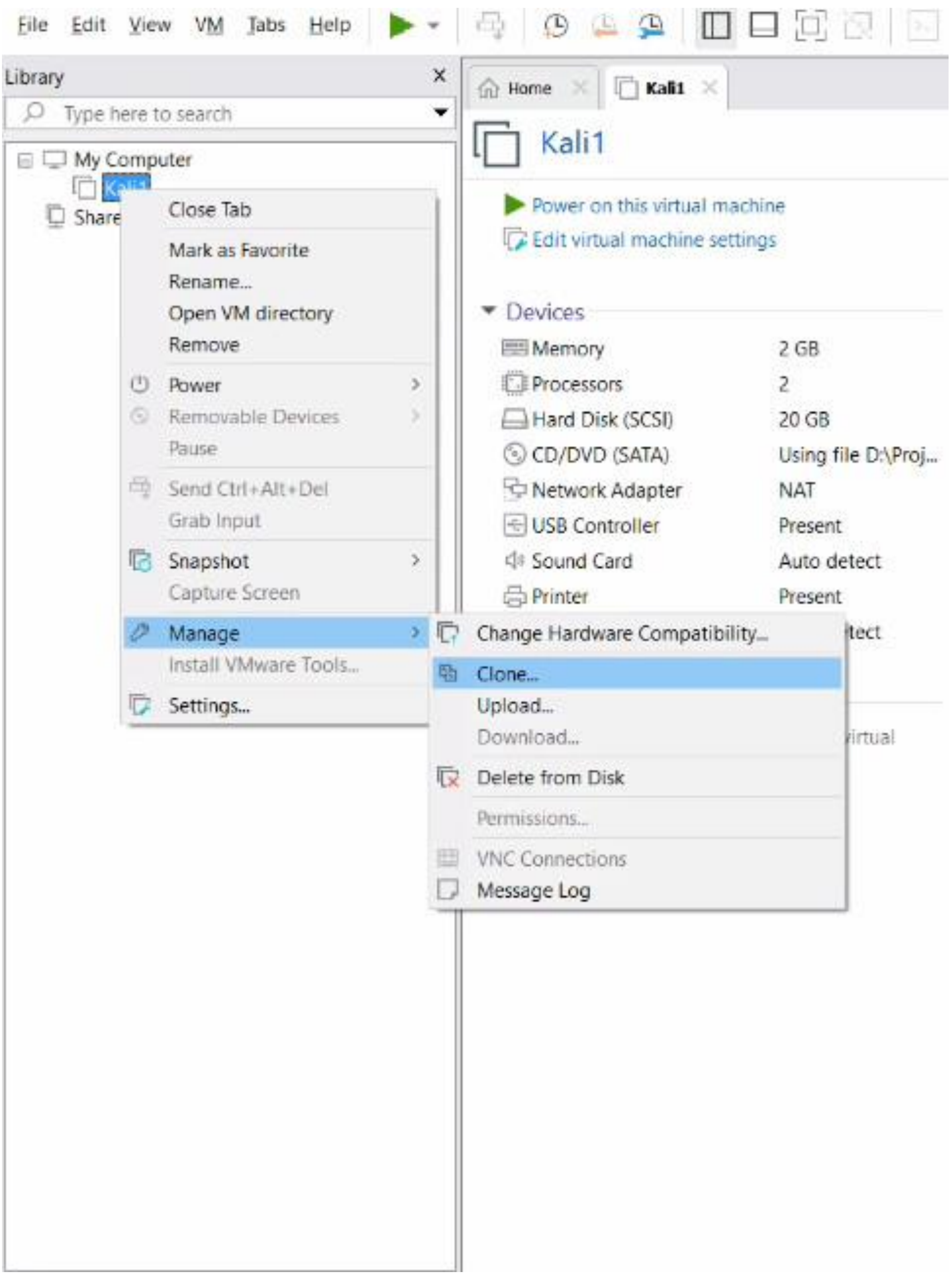

KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Help
Install with speech synthesis

Figure 3.5.6: Graphical Installation process of Kali.

Such a installation process takes more time to setup successfully so have patience.

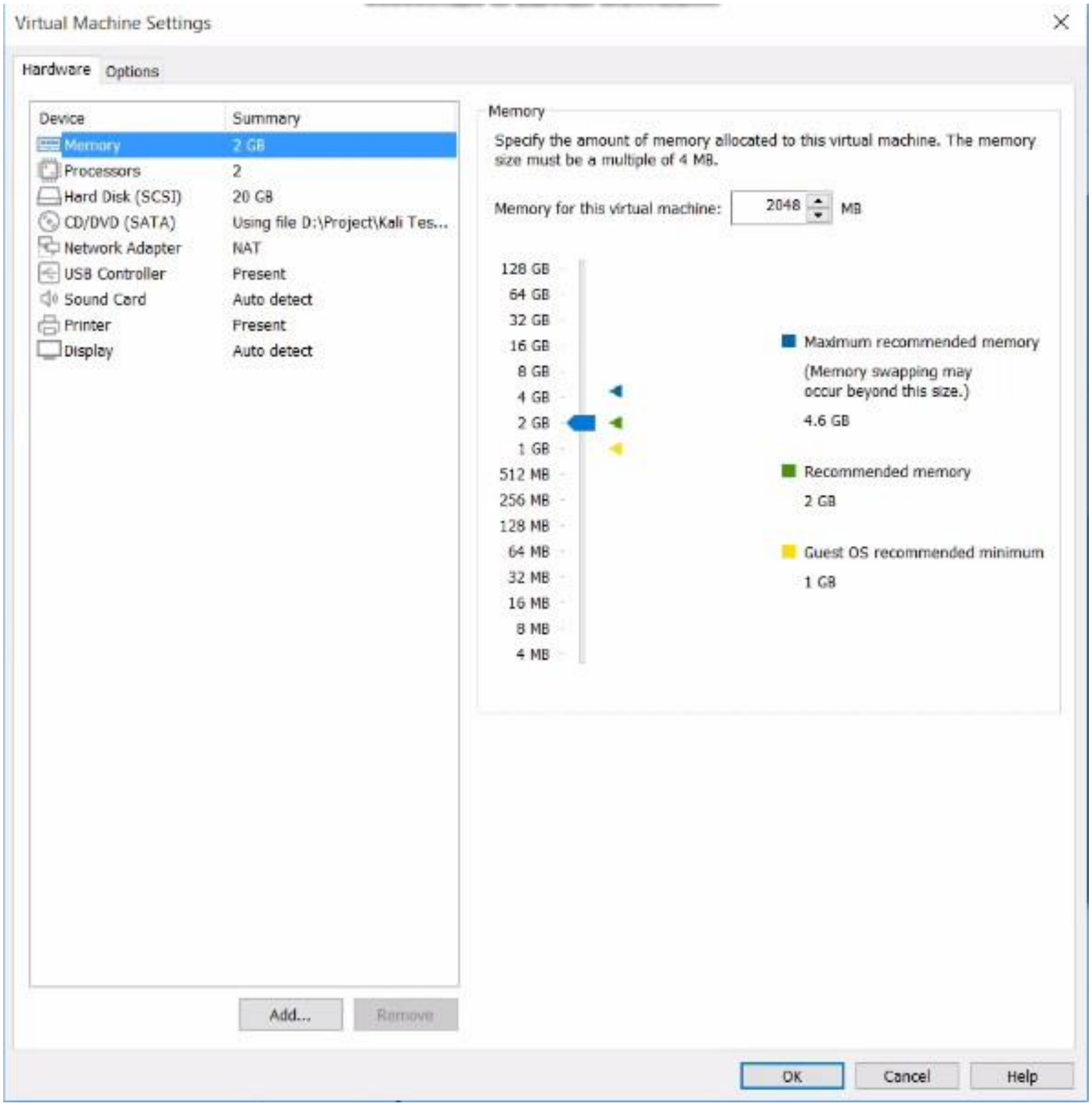
Now, we start the Cloning process by selecting the below option:



Memory 2 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Using file D:\Proj...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present

Figure 3.5.7: Cloning process after Kali installation.

After successfully completion of Cloning of Kali1 OS the below figure illustrates the Clone OS configuration.



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file D:\Project\Kali Tes...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

■ Maximum recommended memory
(Memory swapping may occur beyond this size.)
4.6 GB

■ Recommended memory
2 GB

■ Guest OS recommended minimum
1 GB

Figure. 3.5.8: Clone of Kali1 Configuration

After download we have copy both the Python3 & DoS script into our Kali1 Linux OS Desktop which is appended below:

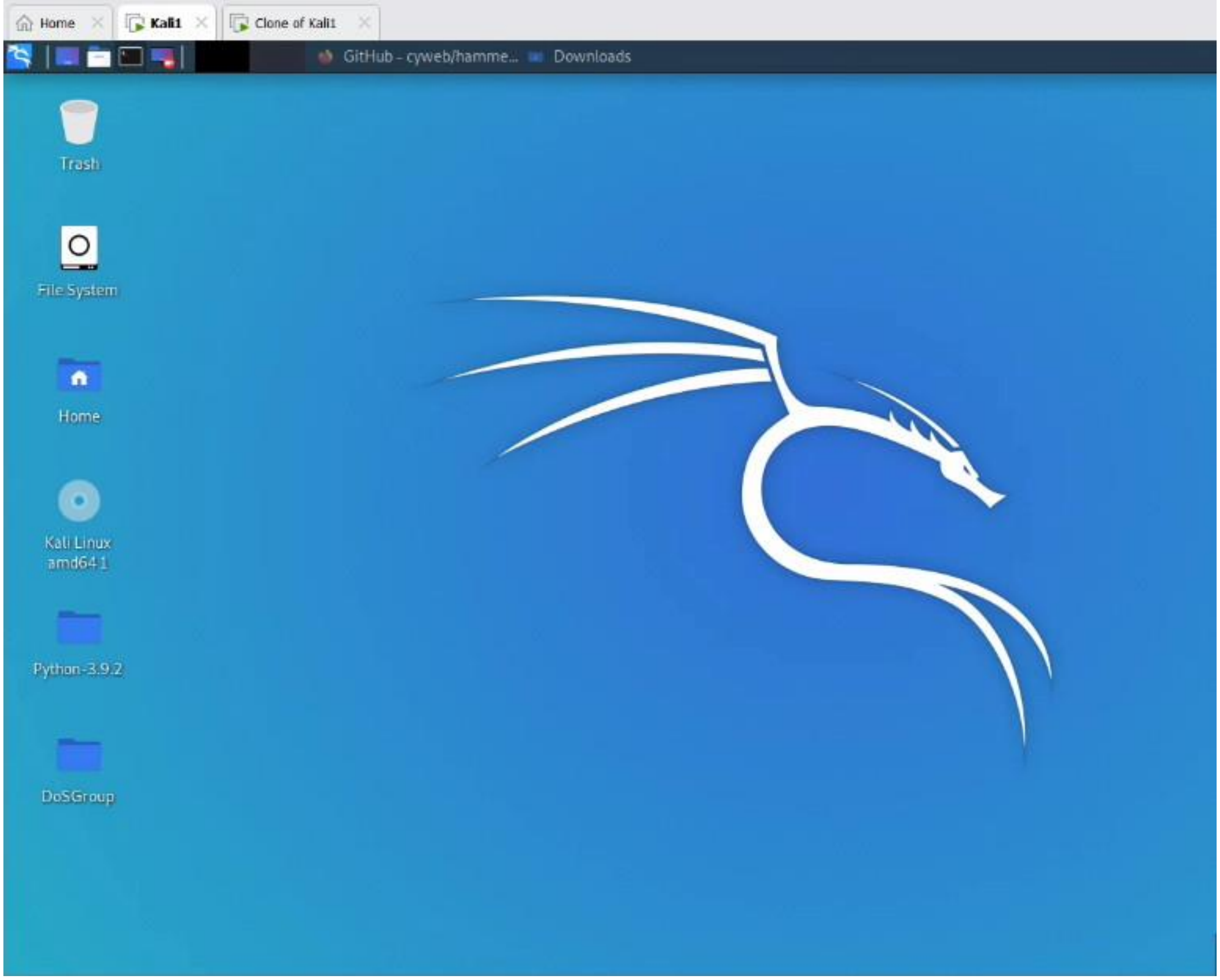
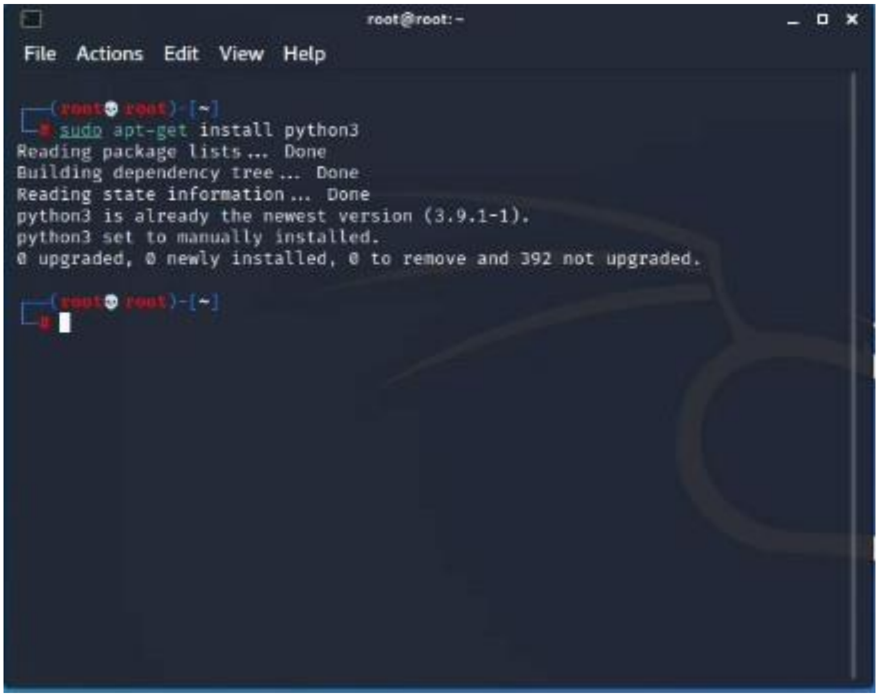


Figure 3.5.9: After download copy both Python3 & DoS script into Kali Linux OS.

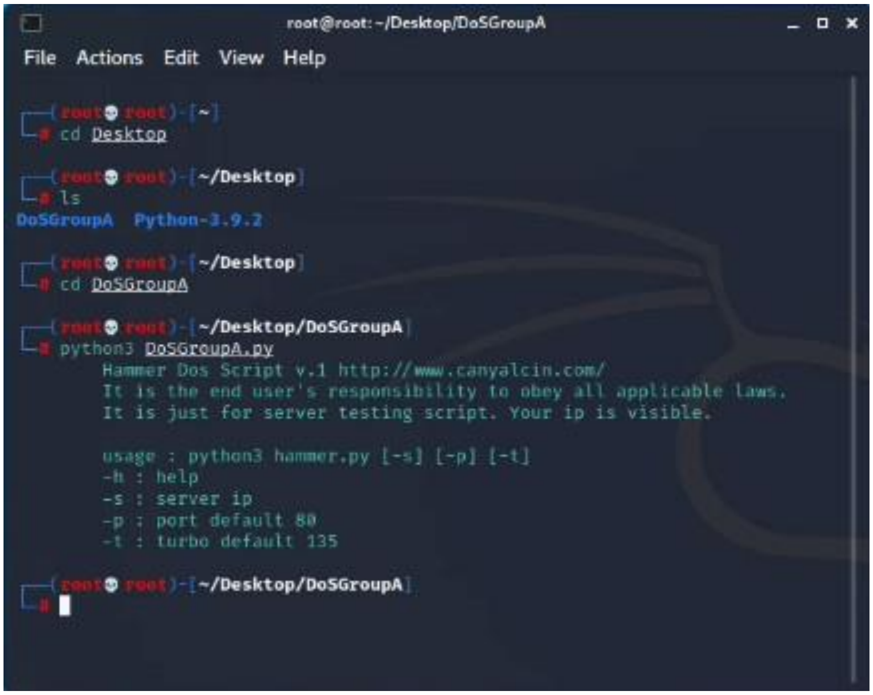
Install the Python3 by opening the Kali Linux terminal which is appended below:



```
┌──(root💀root)-[~]
└─# sudo apt-get install python3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.9.1-1).
python3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 392 not upgraded.

┌──(root💀root)-[~]
└─# 
```

Figure 3.5.10: Install Python3 by using Kali Linux Terminal

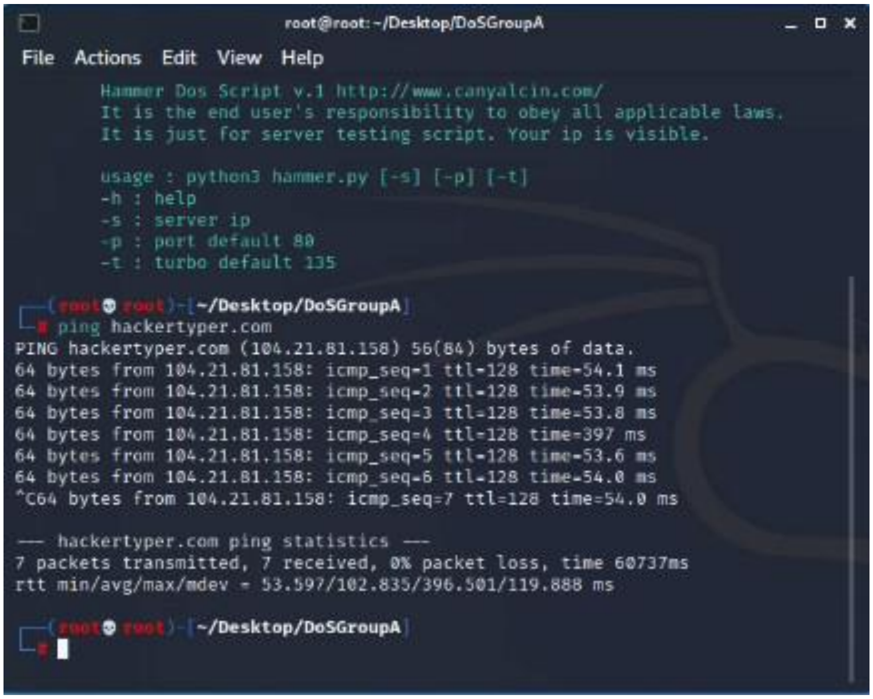
After that, launch the Python DoS Script file (which we named DoSGroupA.py) on the attacking VM.



```
┌──(root💀root)-[~]
└─# cd Desktop

┌──(root💀root)-[~/Desktop]
└─# ls
DoSGroupA  Python-3.9.2

┌──(root💀root)-[~/Desktop]
└─# cd DoSGroupA

┌──(root💀root)-[~/Desktop/DoSGroupA]
└─# python3 DoSGroupA.py
        Hammer Dos Script v.1 http://www.canyalcin.com/
        It is the end user's responsibility to obey all applicable laws.
        It is just for server testing script. Your ip is visible.

        usage : python3 hammer.py [-s] [-p] [-t]
        -h : help
        -s : server ip
        -p : port default 80
        -t : turbo default 135

┌──(root💀root)-[~/Desktop/DoSGroupA]
└─# 
```

Figure 3.5.11: Launch Python DoS script on Kali1 Linux VM.

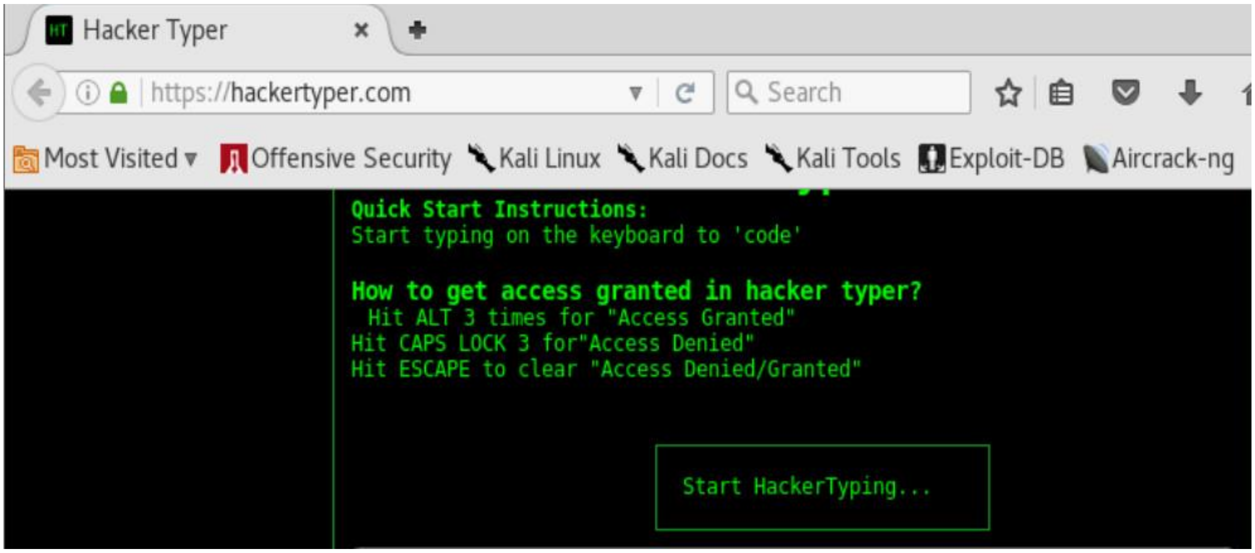
Now, we have to find out the IP address of our target system by pinging the URL i.e ping hackertyper.com on Kali1 Linux OS for hit the DoS attack which is given below:



```
        Hammer Dos Script v.1 http://www.canyalcin.com/
        It is the end user's responsibility to obey all applicable laws.
        It is just for server testing script. Your ip is visible.

        usage : python3 hammer.py [-s] [-p] [-t]
        -h : help
        -s : server ip
        -p : port default 80
        -t : turbo default 135

┌──(root💀 root)-[~/Desktop/DoSGroupA]
└─# ping hackertyper.com
PING hackertyper.com (104.21.81.158) 56(84) bytes of data.
64 bytes from 104.21.81.158: icmp_seq=1 ttl=128 time=54.1 ms
64 bytes from 104.21.81.158: icmp_seq=2 ttl=128 time=53.9 ms
64 bytes from 104.21.81.158: icmp_seq=3 ttl=128 time=53.8 ms
64 bytes from 104.21.81.158: icmp_seq=4 ttl=128 time=397 ms
64 bytes from 104.21.81.158: icmp_seq=5 ttl=128 time=53.6 ms
64 bytes from 104.21.81.158: icmp_seq=6 ttl=128 time=54.0 ms
^C64 bytes from 104.21.81.158: icmp_seq=7 ttl=128 time=54.0 ms

--- hackertyper.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 60737ms
rtt min/avg/max/mdev = 53.597/102.835/396.501/119.888 ms

┌──(root💀 root)-[~/Desktop/DoSGroupA]
└─# 
```

Figure 3.5.12: Finding the IP address of the target website (hackertyper.com).

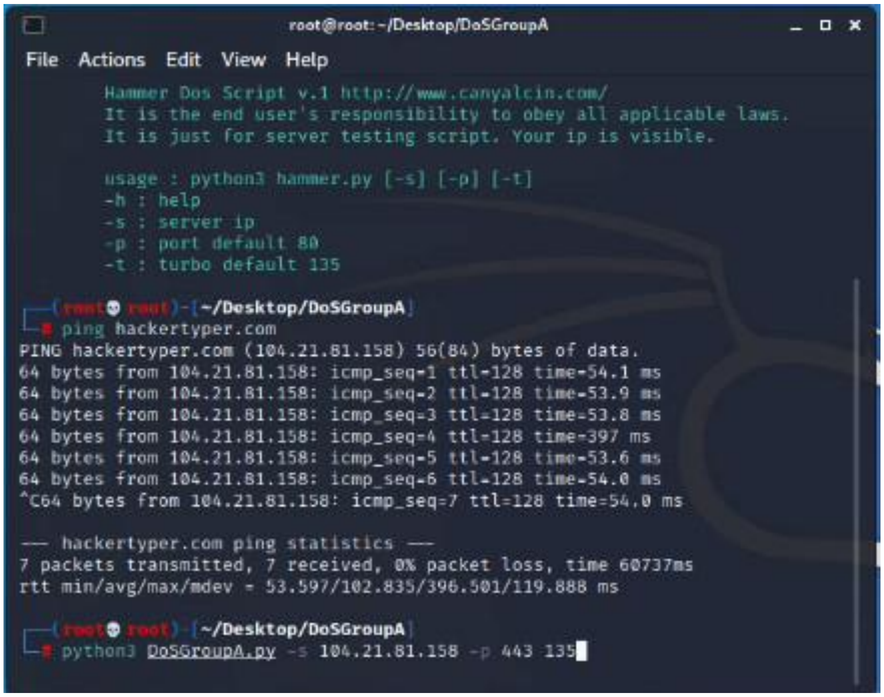
The target website running on the clone Kali1 Linux VM.



```
Quick Start Instructions:
Start typing on the keyboard to 'code'

How to get access granted in hacker typer?
 Hit ALT 3 times for "Access Granted"
Hit CAPS LOCK 3 for"Access Denied"
Hit ESCAPE to clear "Access Denied/Granted"
```

Figure 3.5.13: Target Website (hackertyper.com) running on the cloned VM.

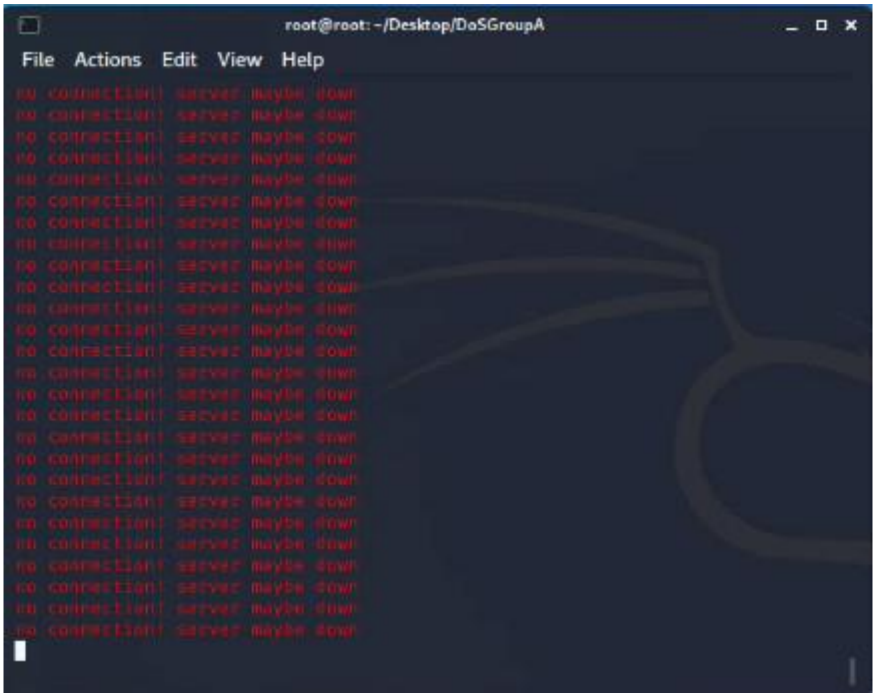
Launch the TCP SYN DoS attack against target website from Kali1 Linux VM.



```
        Hammer Dos Script v.1 http://www.canyalcin.com/
        It is the end user's responsibility to obey all applicable laws.
        It is just for server testing script. Your ip is visible.

        usage : python3 hammer.py [-s] [-p] [-t]
        -h : help
        -s : server ip
        -p : port default 80
        -t : turbo default 135

┌──(root💀root)-[~/Desktop/DoSGroupA]
└─# ping hackertyper.com
PING hackertyper.com (104.21.81.158) 56(84) bytes of data.
64 bytes from 104.21.81.158: icmp_seq=1 ttl=128 time=54.1 ms
64 bytes from 104.21.81.158: icmp_seq=2 ttl=128 time=53.9 ms
64 bytes from 104.21.81.158: icmp_seq=3 ttl=128 time=53.8 ms
64 bytes from 104.21.81.158: icmp_seq=4 ttl=128 time=397 ms
64 bytes from 104.21.81.158: icmp_seq=5 ttl=128 time=53.6 ms
64 bytes from 104.21.81.158: icmp_seq=6 ttl=128 time=54.0 ms
^C64 bytes from 104.21.81.158: icmp_seq=7 ttl=128 time=54.0 ms

--- hackertyper.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 60737ms
rtt min/avg/max/mdev = 53.597/102.835/396.501/119.888 ms

┌──(root💀root)-[~/Desktop/DoSGroupA]
└─# python3 DoSGroupA.py -s 104.21.81.158 -p 443 135
```

Figure 3.5.14: Launch the DoS attack from Kali1 Linux VM.

The target website flooded after the TCP SYN DoS attack which is given below:



```
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
```

Figure 3.5.15: Target website down due to TCP SYN DoS attack.

Now, look at the cloned Kali Linux VM:

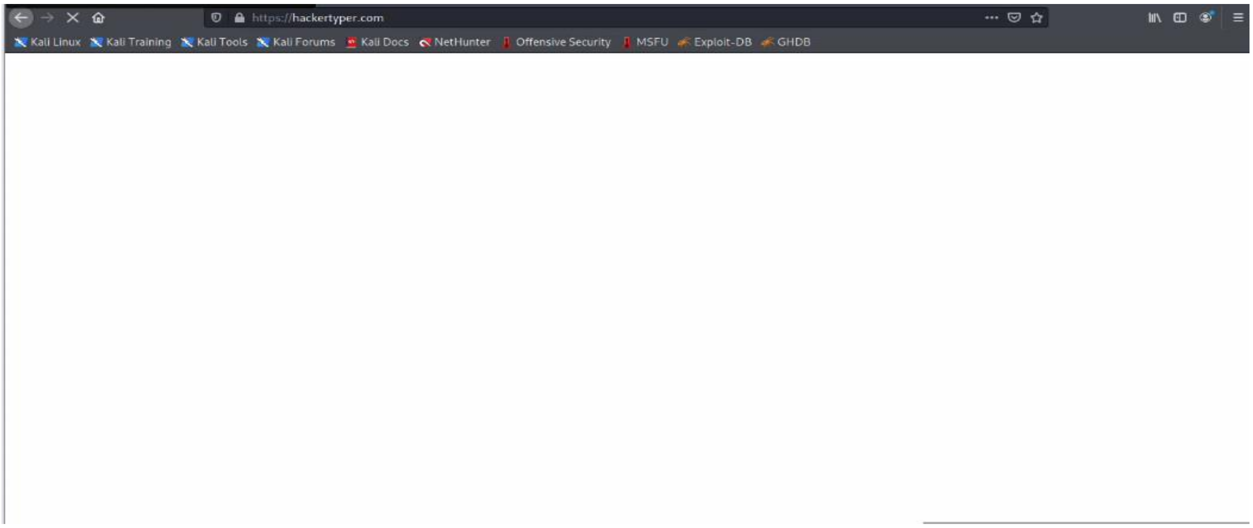
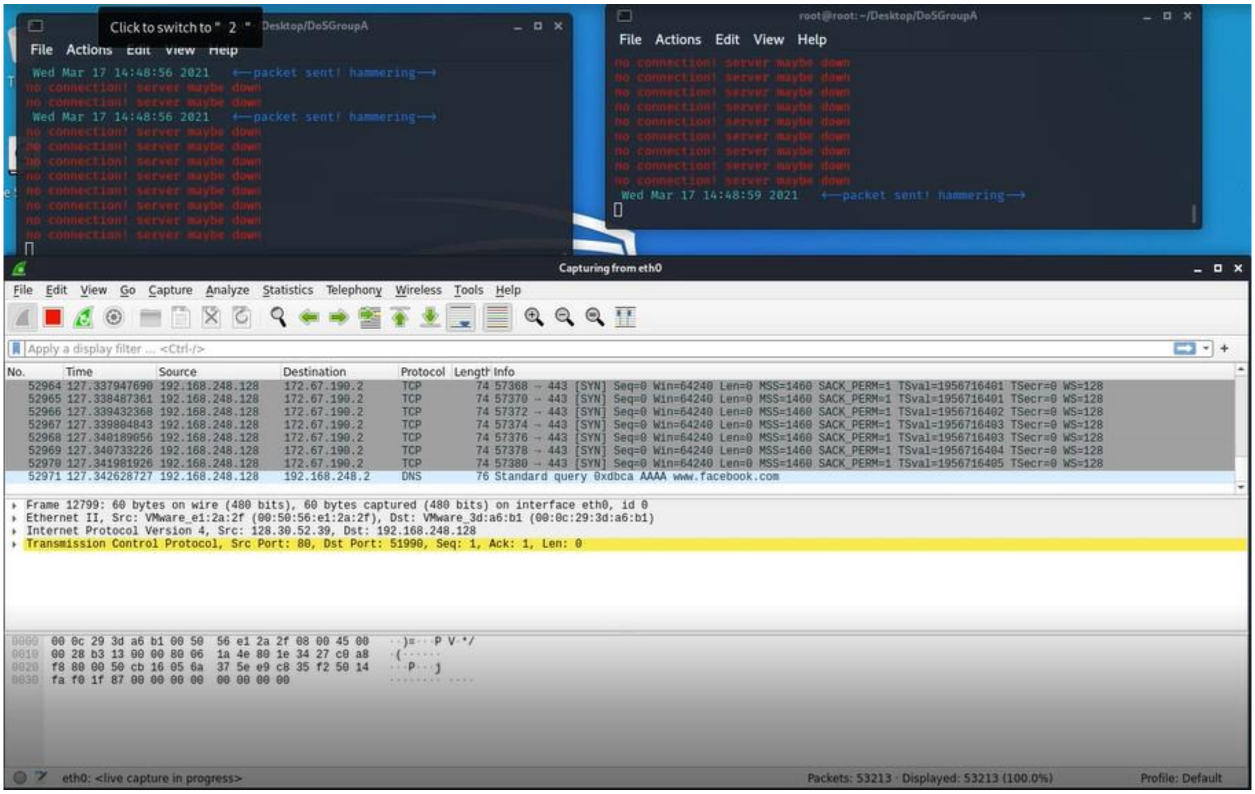


Figure 3.5.16: Target website takes more time to load on clone Kali1 Linux VM.

Now, we have to capture the packet log by using Wireshark for both attacking (Kali Linux VM) and Clone VM which is appended below:



```
 Wed Mar 17 14:48:56 2021   ←—packet sent! hammering—→
no connection! server maybe down
no connection! server maybe down
 Wed Mar 17 14:48:56 2021   ←—packet sent! hammering—→
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
```

```
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
no connection! server maybe down
 Wed Mar 17 14:48:59 2021   ←—packet sent! hammering—→
```

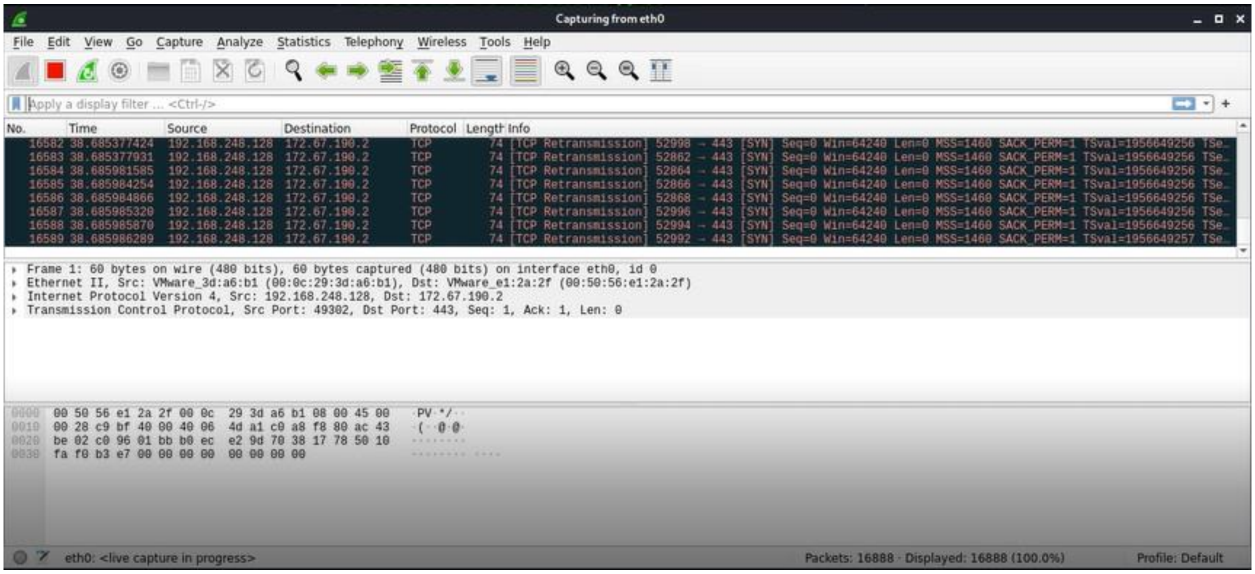
```
No.    Time           Source           Destination     Protocol Length Info
 52964 127.337947690 192.168.248.128  172.67.190.2    TCP        74 57368 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716401 TSecr=0 WS=128
 52965 127.338487361 192.168.248.128  172.67.190.2    TCP        74 57370 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716401 TSecr=0 WS=128
 52966 127.339432368 192.168.248.128  172.67.190.2    TCP        74 57372 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716402 TSecr=0 WS=128
 52967 127.339804843 192.168.248.128  172.67.190.2    TCP        74 57374 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716403 TSecr=0 WS=128
 52968 127.340189056 192.168.248.128  172.67.190.2    TCP        74 57376 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716403 TSecr=0 WS=128
 52969 127.340733226 192.168.248.128  172.67.190.2    TCP        74 57378 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716404 TSecr=0 WS=128
 52970 127.341981926 192.168.248.128  172.67.190.2    TCP        74 57380 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956716405 TSecr=0 WS=128
 52971 127.342628727 192.168.248.128  192.168.248.2   DNS        76 Standard query 0xdbca AAAA www.facebook.com
```

```
▸ Frame 12799: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_e1:2a:2f (00:50:56:e1:2a:2f), Dst: VMware_3d:a6:b1 (00:0c:29:3d:a6:b1)
▸ Internet Protocol Version 4, Src: 128.30.52.39, Dst: 192.168.248.128
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 51990, Seq: 1, Ack: 1, Len: 0
```

```
0000  00 0c 29 3d a6 b1 00 50  56 e1 2a 2f 08 00 45 00   ··)=···P V·*/
0010  00 28 b3 13 00 00 80 06  1a 4e 80 1e 34 27 c0 a8   ·(······
0020  f8 80 00 50 cb 16 05 6a  37 5e e9 c8 35 f2 50 14   ···P···j
0030  fa f0 1f 87 00 00 00 00  00 00 00 00               ········ ····
```

eth0: <live capture in progress>   Packets: 53213 · Displayed: 53213 (100.0%)   Profile: Default

Figure 3.5.17: Wireshark packet capture log found on the Kali Linux VM.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source           Destination    Protocol Length Info
16582 38.685377424  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52998 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16583 38.685377931  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52862 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16584 38.685981585  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52864 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16585 38.685984254  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52866 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16586 38.685984866  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52868 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16587 38.685985320  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52996 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16588 38.685985870  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52994 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649256 TSe…
16589 38.685986289  192.168.248.128  172.67.190.2   TCP      74 [TCP Retransmission] 52992 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1956649257 TSe…

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_3d:a6:b1 (00:0c:29:3d:a6:b1), Dst: VMware_e1:2a:2f (00:50:56:e1:2a:2f)
▸ Internet Protocol Version 4, Src: 192.168.248.128, Dst: 172.67.190.2
▸ Transmission Control Protocol, Src Port: 49302, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000  00 50 56 e1 2a 2f 00 0c  29 3d a6 b1 08 00 45 00   ·PV·*/··
0010  00 28 c9 bf 40 00 40 06  4d a1 c0 a8 f8 80 ac 43   ·(··@·@·
0020  be 02 c0 96 01 bb b0 ec  e2 9d 70 38 17 78 50 10   ········
0030  fa f0 b3 e7 00 00 00 00  00 00 00 00               ········ ····

eth0: <live capture in progress>          Packets: 16888 · Displayed: 16888 (100.0%)          Profile: Default
```

Figure 3.5.18: Wireshark packet capture log found on the clone VM.

3.6 Findings & Result:

My DoS attack is a locally hosted in my PC where the attacker host used as Kali Linux OS in a VM and the targeted website run on the cloned Kali Linux virtual machine which uses same network and subnet as well. The Kali Linux OS initiate the DoS attack by using Python DoS script to flood the targeted website through the port 443 and TCP connections and it was then takes long time to load or unavailable/unresponsive for sometime. In this case, the targeted network/website wasn't fully unavailable due to my computer hardware and internet speed. But I was showed the actual affect after such a DoS attack. After running the script, the targeted website will remain in a continuous loading state and after some time it was loaded. As we can see if we should down the target website successfully we have to manage powerful computer and more internet speed to flood the target system. . However, the entire DoS simulation attack was run and contained inside the VMware Workstation on my physical machine so that there was no actual damage happened to the targeted website (https://www.hackertyper.com).

Lastly, by this chapter, my main goal is to show how a website affected seriously during a DoS/DDoS attack in today's internet era by using TCP SYN packet flood DoS attack Python script and using two Kali Linux VM installed on VMware Workstation against a target website.

CHAPTER 4

DDOS Attack Tools & Detection Method

4.1 Introduction:

As we already know that now-a-days distributed denial-of-service (DDoS) attack is one of the most dangerous and famous network attack which main aims to crash a server for long duration of time and it can be done by an attacker for revenge, intentionally, war, political purposes etc. In this chapter, we'll discuss about the various types of DDoS tools and it's feature and how can we actually detect a DDoS attack in our system or network. I'll try to discuss such a topic in detail. Now-a-days, an attacker try to open a new way for attack and as well as a network administrator or system admin also try to find a way for mitigate the attack by using various detection method, or setup a policy against DDoS attack on the network by using different vendor. So, every vendor always try to invent a policy against DDoS attack where network admin feel relax. Actually, no one can guarantee that he/she can prevent the DDoS attack fully until he/she can take steps against such an attack. Let's see an figure below which illustrates the today's DDoS attack worldwide which is appended below [19]:

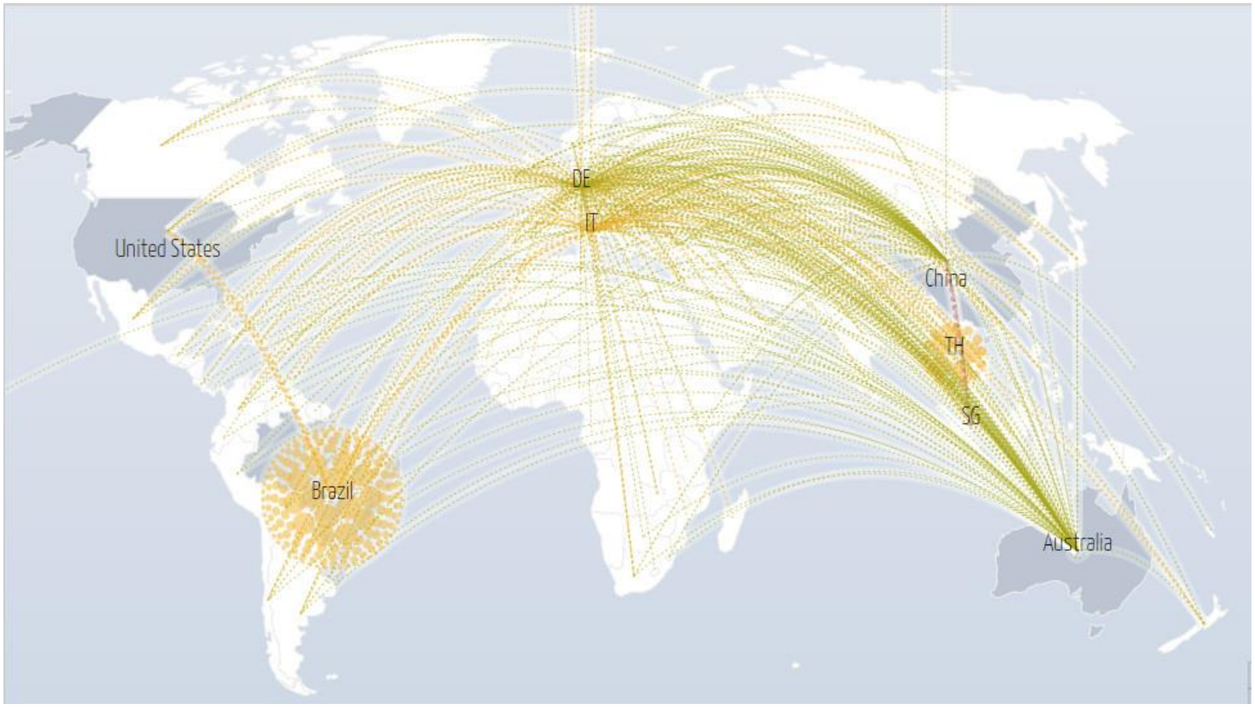


Figure 4.1.1: Today's DDoS attack worldwide.

Here, the orange color illustrates the volumetric attack, green color describes the fragmentation & red color means there was a TCP connection flood happens from a source to other destination.

As the time flows the network security and hacking world is constantly changing so that there are various types of DDoS attack tools need to execute distributed denial-of-service (DDoS) attacks.

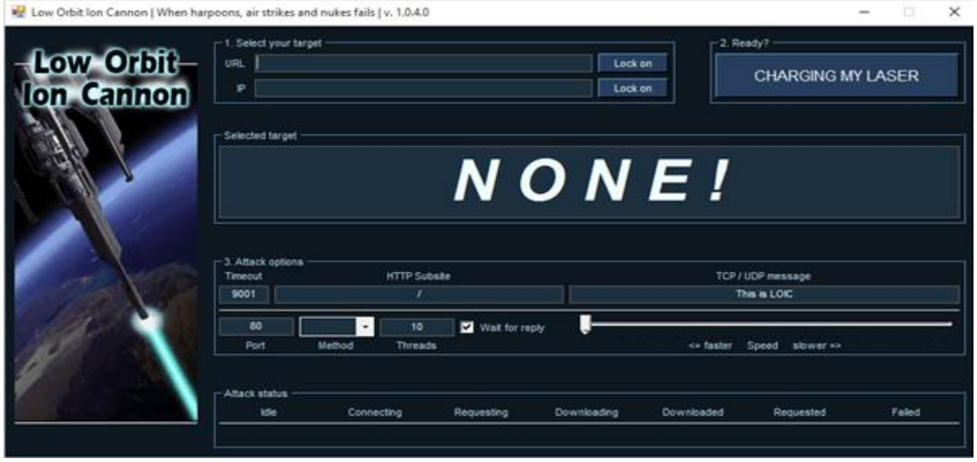
As a result there are some dependencies to use that DDoS attack tools which can vary from OS to OS like Linux, Windows, Solaris etc. There are few DDoS attack tools were made only for testing purpose like LOIC and then it will be modified and used for attacking purpose. Another famous DDoS attack tools named Slowloris was developed by gray hat hackers where they made it only for finding the weakness of any specific software. By releasing such DDoS tools publicly, gray hat hackers force software developers to patch vulnerable software in order to avoid large-scale attacks [20].

4.2 DDoS Attack Tools:

There are numerous distributed denial-of-service (DDoS) attack tools that can executed a DDoS attack over a target website, system or network. Now, we'll discuss such various types DDoS attack tools one by one with their feature which is appended below:

i. **LOIC:** LOIC basically derives as Low Orbit Ion Cannon. It is considered as the nearly famous attacking tools which can be used as free in the internet. Such a tools is written in C# and it can send HTTP, UDP, TCP requests to their server or system. The main feature of LOIC is as under:

- ✓ It's a free open source tools which also helps us to test the performance of the network.
- ✓ It can do the attack based on the URL or IP address of the server [21].
- ✓ Such a tool can effect immediate to the server which can down the server faster than other.
- ✓ It's easy to use.
- ✓ If we get the IP address of the target system/server then rest of the done by this tool.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.4.0

Selected target: NONE!

Timeout: 9001
HTTP Subsite: /
TCP / UDP message: This is LOIC
Port: 80
Threads: 10
☑ Wait for reply

Figure 4.2.1: LOIC DDoS attack tools [21].

ii. **XOIC:** It’s another famous DDoS tools now-a-days. By using this tools attacker can attack the server which has a small website. The feature of XOIC is given below:

- ✓ It provides three modes to attack.
  - ❖ Testing mode.
  - ❖ Normal DoS attack mode.
  - ❖ DoS attack with TCP or HTTP or UDP or ICMP message [21].
- ✓ It’s the best suitable for small website.
- ✓ It’s GUI mood is most user friendly.

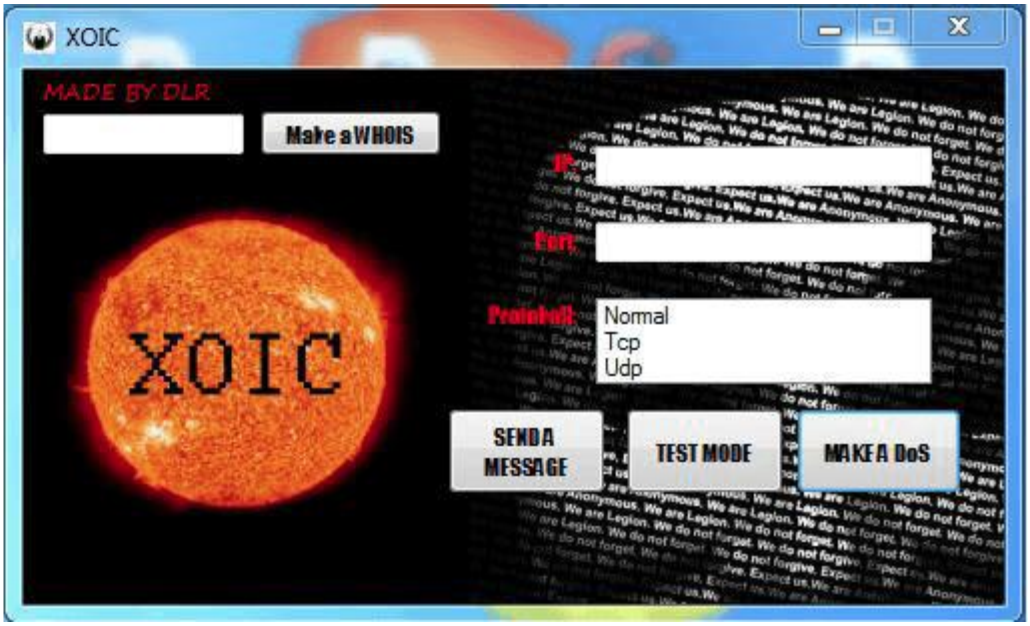
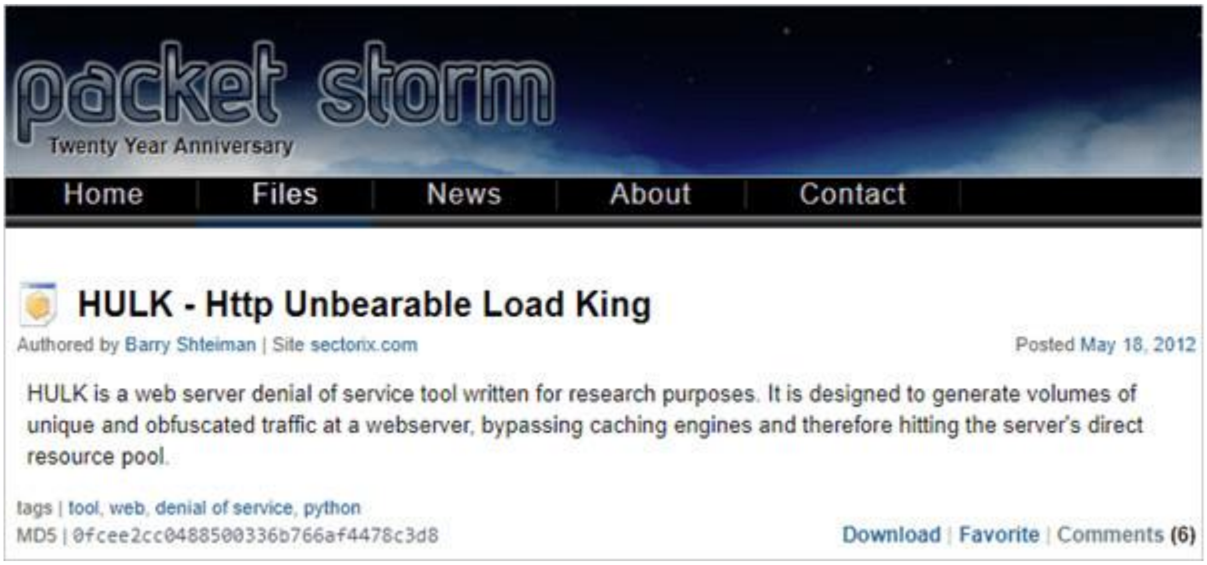


Figure 4.2.2: XOIC DDoS attack tools [21].

iii. **HULK:** HULK represents HTTP Unbearable Load King. It can be used for only DoS attack and it’s made for research purposes. The feature of HULK is appended below:

- ✓ Such a tools can bypass the cache engine so that it can directly hits the server’s resource pool.
- ✓ It can execute a large amount of traffic to a server or system.
- ✓ It can generate random traffic to the server.



HULK - Http Unbearable Load King

Authored by Barry Shteiman | Site sectorix.com

Posted May 18, 2012

HULK is a web server denial of service tool written for research purposes. It is designed to generate volumes of unique and obfuscated traffic at a webserver, bypassing caching engines and therefore hitting the server's direct resource pool.

tags | tool, web, denial of service, python

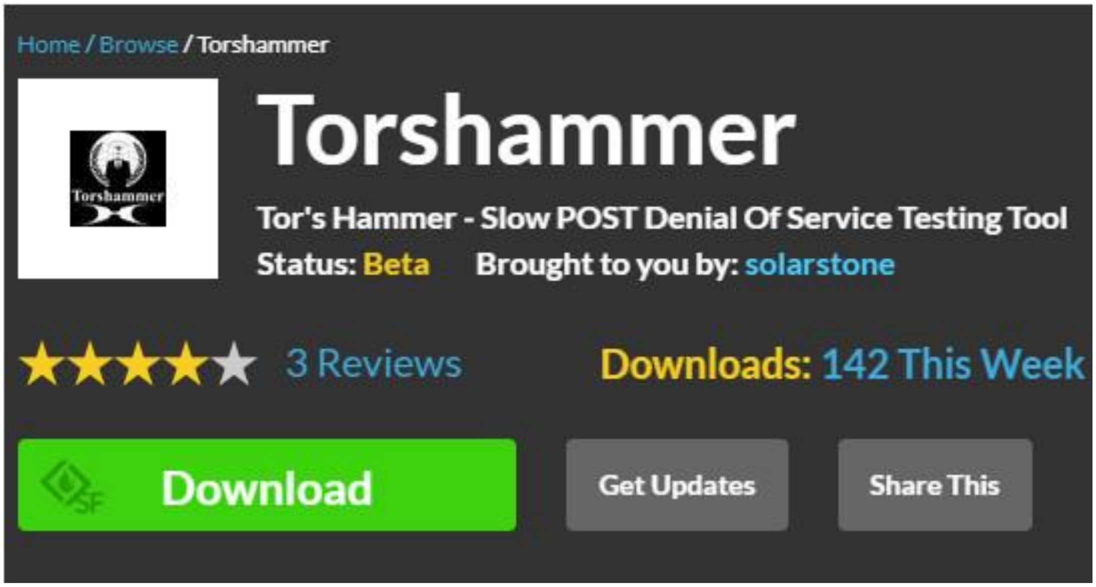
MD5 | 0fcee2cc0488500336b766af4478c3d8

Download | Favorite | Comments (6)

Figure 4.2.3: HULK DDoS attack tools [21].

iv. **Tor's Hammer:** Tor's Hammer is one of the most famous DOS attack tool. The main feature of this attack tools is given below:

- ✓ If we run it through Tor network then we will remain unidentified [21].
- ✓ It is a useful tool that can destroy Apache or IIS servers within a few seconds.
- ✓ In order to run it through Tor, use 127.0.0.1:9050 [21].



Tor's Hammer - Slow POST Denial Of Service Testing Tool

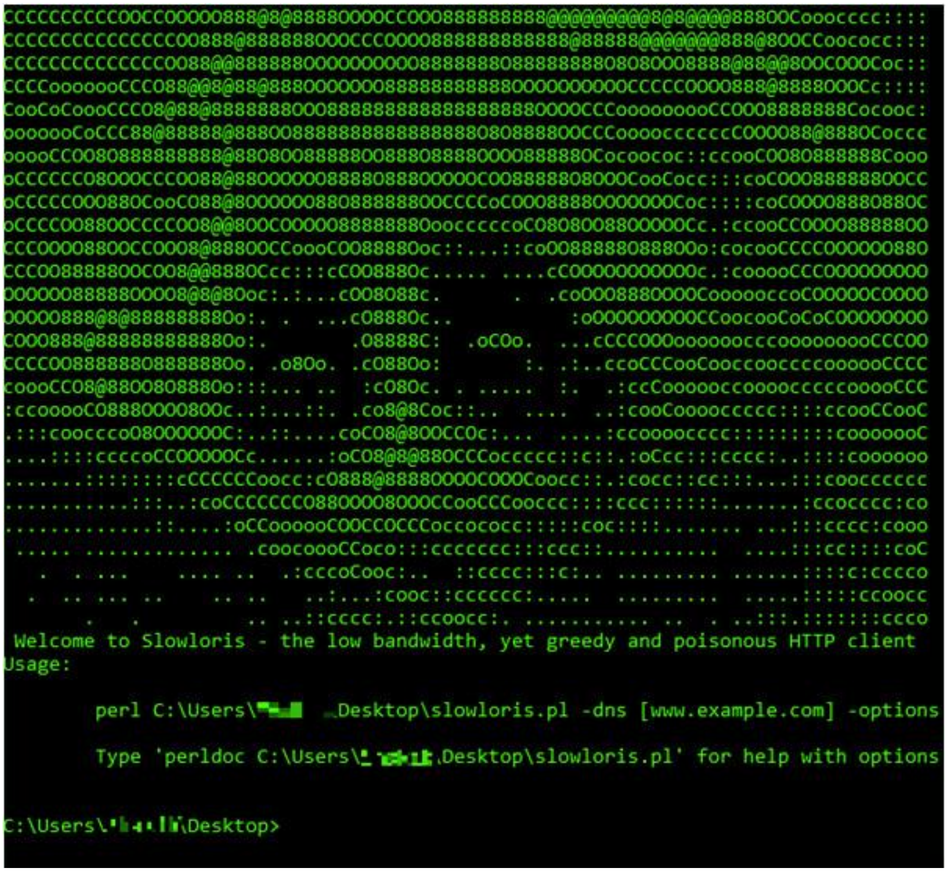
Status: Beta Brought to you by: solarstone

★★★★☆ 3 Reviews Downloads: 142 This Week

Figure 4.2.4: Tor's Hammer DDoS attack tools [21].

v. **Slowloris:** It’s the most famous attack tools in current hacking world. The main feature of Slowloris attack tools is given below:

- ✓ Comparatively it needs less resource for attack.
- ✓ It can generate HTTP traffic at a server.
- ✓ It doesn’t affect other services and ports on the target network [21].
- ✓ As the server keeps the false connection open, this will overflow the connection pool and will deny the request to the true connections [21].



```
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl C:\Users\[redacted]Desktop\slowloris.pl -dns [www.example.com] -options

        Type 'perldoc C:\Users\[redacted]Desktop\slowloris.pl' for help with options


C:\Users\[redacted]\Desktop>
```

Figure 4.2.5: Slowloris DDoS attack tools [21].

vi. **DDOSIM:** DDOSIM imply for DDoS Simulator. It is used to execute DDOS attacks by simulating numerous compromised hosts. This tool is C++ based and runs on only Linux OS. The feature of this tools is as under:

- ✓ It can attack both a server and a network also.
- ✓ All compromised hosts create a TCP connections for the target system/server.
- ✓ It can do DDoS attack using invalid requests [21].
- ✓ It can make an attack on the application layer [21].

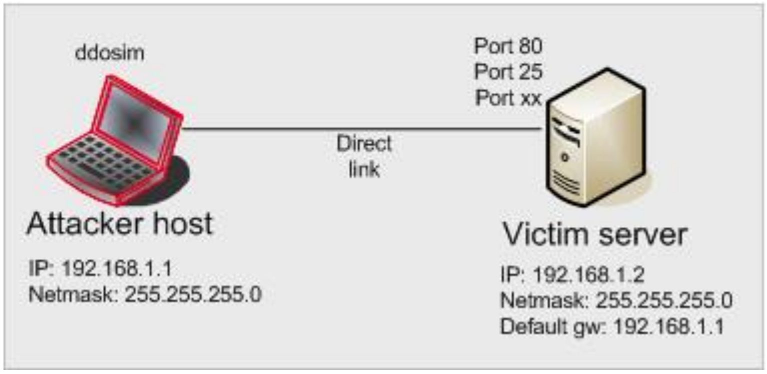


Figure 4.2.6: DDOSIM DDoS attack tools [21].

vii. **RUDY:** RUDY stands for R-U-Dead-Yet. The main feature of RUDY is appended below:

- ✓ This tool comes with a user friendly console menu.
- ✓ We can select the forms from the URL, for the POST-based DDoS attack [21].
- ✓ As it is run at a slow-rate that's why it is time-consuming and detected as abnormal.

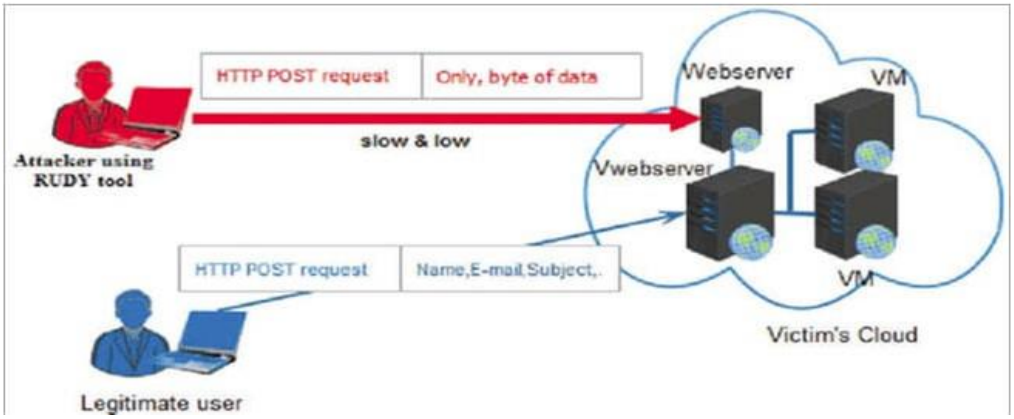


Figure 4.2.7: RUDY DDoS attack tools [21].

The above discussion describes the various types of DDoS attack tools with their feature. But, without such types may be tomorrow there will be another new DDoS attack tools will be evolved so that a network admin must be feeling anxious about how to detect and how he/she can take steps for its prevention. Instead of above mention DDoS attack tools there are some more additional tools which includes **OWASP DOS HTTP POST** where OWASP derived for Open Web Application Security Project and it is made for testing purpose for layer 1 or application layer attack and such a tool can also test the capacity of the server, **GoldenEye-** it is also made for executing security testing purpose and also create for attack on the server and **Hping-** such a tools is also used for testing purpose and it can send ICMP, UDP, SYN packet to the server for attacking purpose and it also made for testing firewall rules.

4.3 DDoS Attack Detection Method:

As we have already discussed that DDoS attack is now common internet attack in the world but an attacker intends to down the particular server or network so it's very much essential to us to identify, detect and take prevention methods against DDoS attack. In this section we'll discuss how can we detect the DDoS attack to take further steps against it. After attacking stage we have to protect ourselves against DDoS attacks so that we need to identify the attack detection. Attack detection is a phase where it can detect an attack once it has executed over any website or network or server. The performance of any attack detection phase is depends on the percentage of attacks it can immediately identify as soon as it can. To protect from DDoS attack we should take proper detection method. DDoS detection is the process of differentiating Distributed Denial of Service (DDoS) attacks from normal network traffic, in order to perform effective attack mitigation [22]. A good detection is depend on how we detect the DDoS attack over a server. So, we can say that "time" is the most important key factor to detect a DDoS attack on the network or server. Now, we try to identify some several ways that can show a continuous DDoS attack is executing in our network/system which is appended below:

a) An IP address makes X requests over Y seconds [23].
b) Your server responds with a 503 due to service outages [23].
c) The attack traffic doesn't follow traffic control protocol.
d) The traffic flow of victim will be abnormal as the victim is unable to respond to all the traffic which is normal.
e) There will be a huge amount of ping loss found on victim network.
f) Attack traffic is created in a random pattern to avoid detection [24]
g) If you use the same connection for internal software, employees notice slowness issues [23].
h) For each kind of attack, we can observe a strong correlation between the attack traffic at target and abnormal behavior at source [24].
i) Log analysis solutions show a huge spike in traffic [23].

But we can’t confident that after find such an indication of DDoS attack that the attack is happening on the server or network also. So, we can maintain the Log monitoring and as well keep an eye on our server or network continuously to detect a DDoS attack. A DDoS attack detection method based on machine learning, which includes two steps: feature extraction and model detection. In the feature extraction stage, the DDoS attack traffic characteristics with a large proportion are extracted by comparing the data packages classified according to rules. In the model detection stage, the extracted features are used as input features of machine learning, and the random forest algorithm is used to train the attack detection model [25]. Now, day by day the attacking method of a DDoS attack is evolving and the detection method also changes a lot. So, experts are trying to find a new or more significant way to detect and the mitigation process against the DDoS attack over a server or network. So, we can say that if we want to mitigate a DDoS attack we have to identify the DDoS attack promptly when the attack begins.

CHAPTER 5

Proposed Solution to Protect From DDoS Attack

5.1 Introduction:

In our above discussion we have discussed about DDoS attack in details. But, now in this chapter I'll discuss about my proposed solution regarding DDoS attack and as well as how can we protect ourselves from DDoS by using different vendor device in our network. Day by day the DDoS attack evolving a lot which may appear in a different way or in a upgraded way so the network admin or a server administrator will take steps against such a dangerous to protect his/her network or server. As a I'm a network engineer for almost 8 years so I had an experience about such DDoS attack many times and that time I was taking few steps in my core network which is in outside facing network to protect from this. After that, I was successful to protect my network from DDoS. In my case, that was ICMP flood attack and I was taking steps in my Core firewall to protect SYN flood, ICMP flood attack which then effective for me from this. In this chapter, here I proposed my few thoughts and share few techniques to protect against DDoS attack and at the same time I'll discuss how can we take few measures against DDoS attack in our network related devices where we'll use different vendors so steps may vary from vendor to vendor. I think such a steps may protect us from DDoS attack for our different server or network at the same time but we should take proper steps before the attack. First of all I'll discuss my proposed solution regarding DDoS attack one by one.

5.2 My Proposed Solution Against DDoS Attack:

In this section I'll discuss about few proposed solution against DDoS attack which is given below:

I. **Determining the DDoS attack initially:** If I've my own servers, then it is my primary responsibility to identify when my servers are under attack. That's because the sooner we'll identify any abnormality for my own website are due to a DDoS attack, the sooner we can stop the DDoS attack. Firstly, we should know our normal traffic activity which can be found from monitoring the traffic. But a DDoS attack will start its activity with a normal spike of traffic so we should understand the traffic volume when maximum user uses our website and alert for sudden spike of huge traffic which can be done by DDoS attack. So, it's better that we have a best DDoS leader who always calm and ready for our complain against DDoS attack that we are under attack.

II. **Prevention against conventional DDoS attack approach:** Attackers often use weak secured networks to execute attacks on victim/target server or website, the network weakness get absorbed and the resources of a sinless network are used by the attacker for his benefits by executing the DDoS attack. The suitable examples of this is the ICMP flood attack. In ICMP flooding attack the attacker sends an simple ICMP echo request with bad source IP address to unprotected networks broadcast address, after that the echo packet request is sent to all the hosts in the network after executing it successfully. After getting the ICMP echo request all hosts in the network respond to that by sending an another echo reply to the source bad IP address in the spoofed ICMP echo request which was the IP address of the target server or website. In this case, we can protect our network by keeping ICMP (ping) requests by default to broadcast IP addresses completely off. By taking easy steps like this can be the best way to preventing a DDoS attack which can then save our valuable server or website or network.

III. **Upgrade the Operating System and weak software:** Attackers mostly employ defective execution of protocols in operating system and different other system and application software to successfully deploy of DoS attacks. We can consider the teardrop attack example, which can use the weakness in the previous version of Microsoft Windows Operating Systems and some earlier versions of Linux which inaccurately overlapping IP packets were sent to the victim which can causes the server unresponsive. Attackers mostly exploit the vulnerabilities in point to point software to misguide the end point hosts and illegally request them to connect to a target computer, then the victim will be flooded with huge amount of connection requests within seconds which causing the DDoS attack at the same time. The above mentioned attacks can be bypass if the OS and software which are causes the DDoS attack are properly updated accordingly.

IV. **Action taken on the Network Border:** If we have taken few steps on our network border then we can mitigate DDoS attack in a partially way especially at the very beginning and this is the simple way we can take. The few of them is given below:

- ✓ We can restrict the rate limit our router to protect our web server from being flooded.
- ✓ We can add filters or may create policy to tell our router/firewall to drop packets from clear sources of attack.
- ✓ We can monitor the traffic or packet capture log by using Wireshark to spot the attacking IP address and source with destination.
- ✓ Drop spoofed or abnormal packets.
- ✓ Set lower SYN, ICMP, TCP and UDP flood drop rate.

By taking above steps we may stop the DDoS attack over our server but we should follow other.

V. **Engaged to ISP against DDoS:** Internet Service Providers (ISP) can play a vital role to ensure the Internet services more safe and can take proper steps against DDoS attacks. If ISPs can successfully establishes entrance filtering at their end routers to completely stop all malicious traffic with spoofed IP addresses. This will undoubtedly effective for segregate and dropping the malicious traffic as close as possible to the source.

VI. **Dropping the malicious traffic as close as possible to the source end:** I think it is the most powerful way to stop the malicious attack which is close to the source. This may protect the target/victim host from going unavailable for the time being but there is a great consequence on the performance of the target/victim host and its network. To handle such a thousands of malicious traffic the routers CPU may busy and loaded which adversely affect the performance for all the hosts in the network.

VII. **Using Maximum Bandwidth:** If we uses the maximum bandwidth for our web server and as well as our network hosts it may sometime protect us from DDoS attack. It might be a simple to prevent but we may pay for a lot about this which won't be effective way for all the company.

VIII. **Manage a DDoS Mitigation Specialist:** It's really very tough to protect from DDoS attack but sometime we need to manage a DDoS specialist which is always ready to protect it and keep calm to handle the horrible situation. Now-a-days, some company provide such a facility to other where there is no expert in their company. So, surely this is not free as this should be paid services only who need.

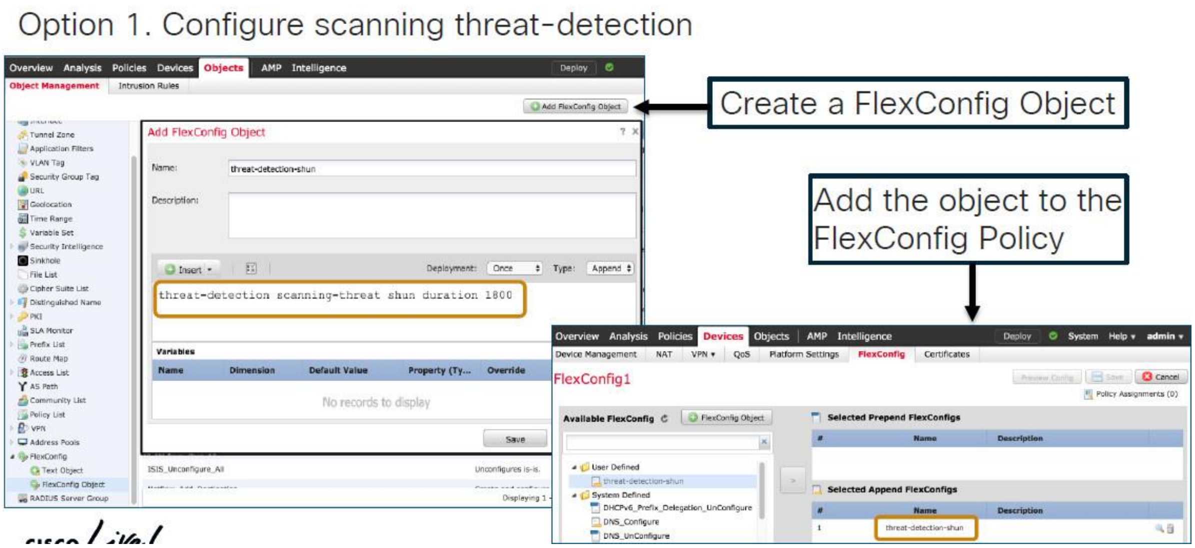
Though any one of the above mentioned proposed solution will never be the adequate steps against DDoS attack alone, a summation of steps from the above mentioned ways should be able to fight against DDoS attacks. On the other hand, if take facility from our different network vendors to protect from DDoS attack, I think this will be the most effective one. Day by day DDoS attack evolving so we should alert for it and should take proper steps against it also. No one can say confidently that he/she can protect his/her server or network from DDoS attack after taking any of the above mentioned steps. So, in this regard I think a combinational steps may protect us from such a dangerous attack like DDoS.

Now, I've move forward to my next steps where I'll illustrates some approaches against DDoS attack for different vendors and it may vary from vendor to vendor. So, the approaches of the different vendor will be different. There are various types of network devices in a network but here I consider only Firewall (NGFW) from different vendor because a firewall is such a kind of device which is positioned in between our inside and outside network. So, if we properly configure our Firewall against DDoS attack then we can easily defend the attack successfully.

5.3 Solution of Network Vendors Against DDoS Attack:

In this section I'll illustrates the configure steps for Firewall from different network vendors against DDoS attack one by one which is appended below:

I. **Cisco:** Cisco is the world's most famous and popular network device manufacturer. It has many devices for several purposes but here I only discuss how can we mitigate DDoS attack by using Cisco FirePower Threat Defense or FTD which is appended below:


Option 1. Configure scanning threat-detection

Create a FlexConfig Object

Add the object to the FlexConfig Policy

Add FlexConfig Object

Name: threat-detection-shun

Deployment: Once Type: Append

```
threat-detection scanning-threat shun duration 1800
```

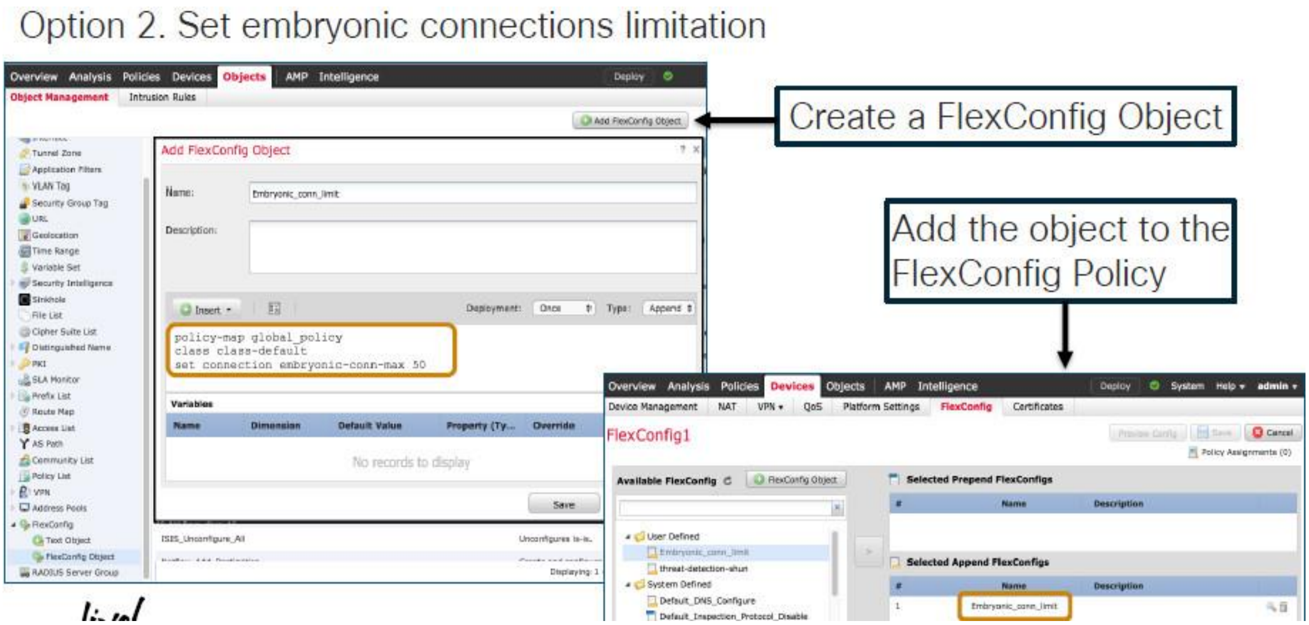
FlexConfig1

Selected Append FlexConfigs

#	Name	Description
1	threat-detection-shun	

Figure 5.3.1: DDoS Mitigation on FirePower Threat Defense, Option-1 [26].

Here, we create an object named FlexConfig and add this object into the FlexConfig policy.


Option 2. Set embryonic connections limitation

Create a FlexConfig Object

Add the object to the FlexConfig Policy

Add FlexConfig Object

Name: Embryonic_conn_limit

Deployment: Once Type: Append

```
policy-map global_policy
class class-default
set connection embryonic-conn-max 50
```

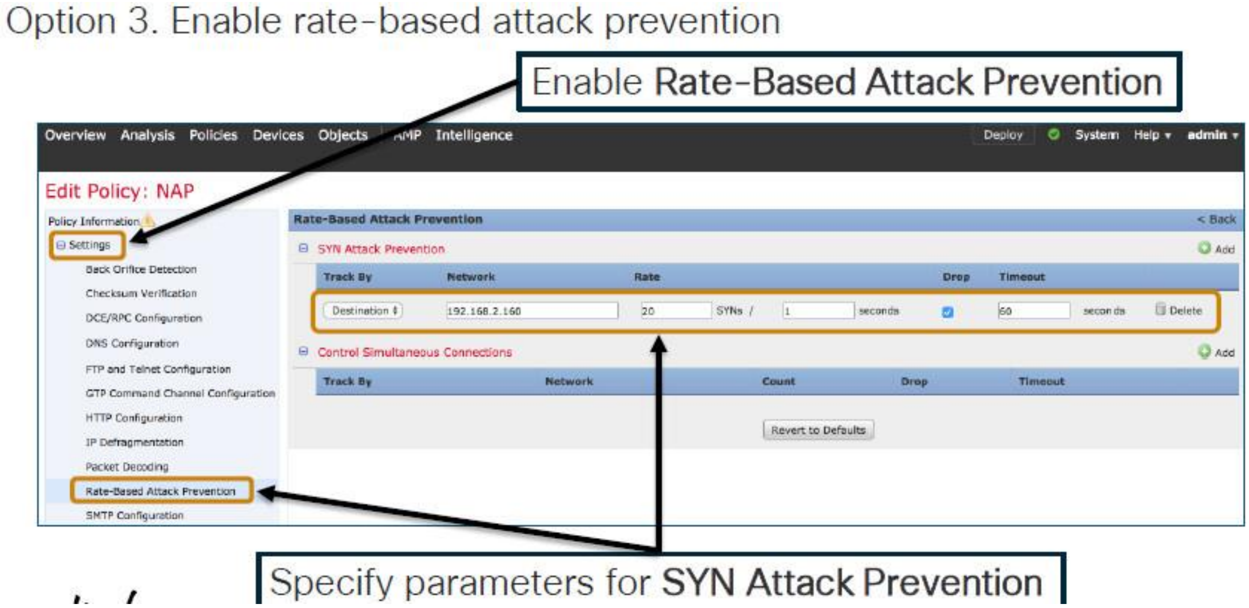
FlexConfig1

Selected Append FlexConfigs

#	Name	Description
1	Embryonic_conn_limit	

Figure 5.3.2: DDoS Mitigation on FirePower Threat Defense, Option-2 [26].

Here, we have set embryonic connection limitation where this embryonic connection is used to prevent the three-way handshake between source and destination. So, if we keep down the number of embryonic connections that can helped us to prevent SYN flooding attacks.



Option 3. Enable rate-based attack prevention

Enable Rate-Based Attack Prevention

Edit Policy: NAP

Rate-Based Attack Prevention

⊟ SYN Attack Prevention

Track By	Network	Rate				Drop	Timeout	
Destination	192.168.2.160	20	SYNs /	1	seconds	☑	60	secon ds

⊟ Control Simultaneous Connections

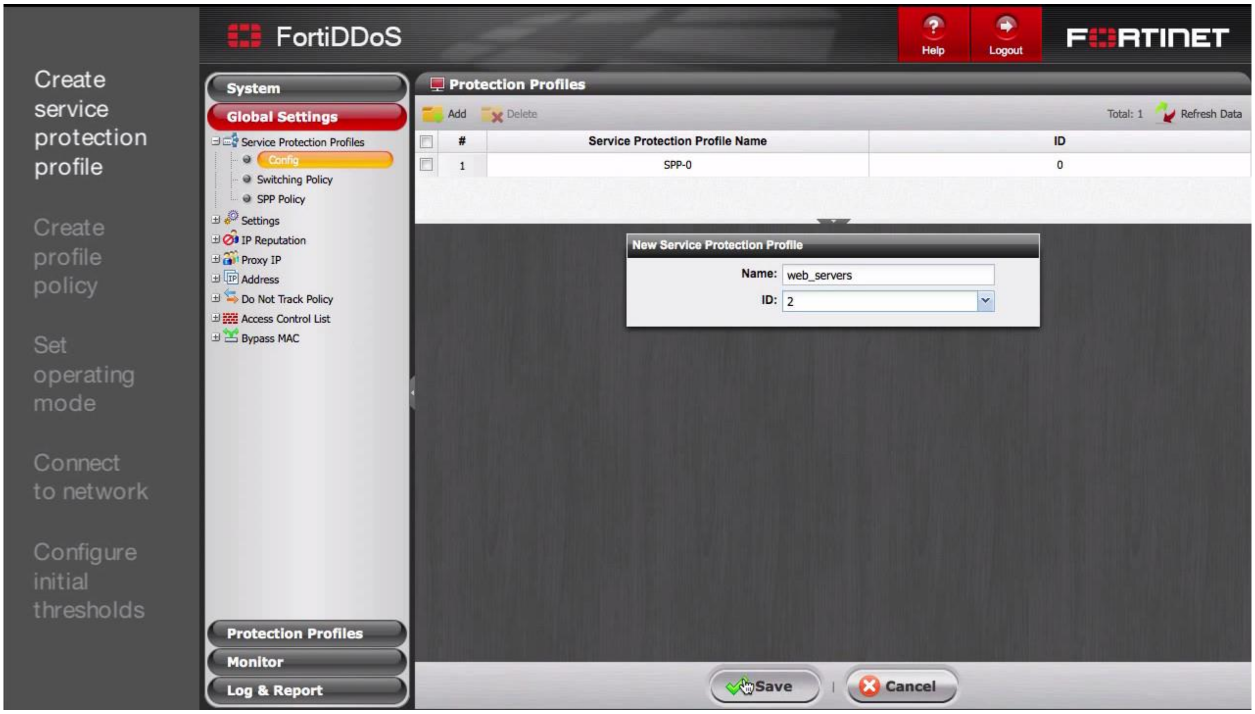
Track By	Network	Count	Drop	Timeout

Specify parameters for SYN Attack Prevention

Figure 5.3.3: DDoS Mitigation on FirePower Threat Defense, Option-3 [26].

Here, we have rate limit the attack where if there is a SYN packet has a 20 rate at per second it will be dropped or has timeout the connection which can prevent the attack successfully.

II. **Foritnet:** Now-a-days Fortinet is one of the most popular networking device manufacturer in the world. They have set their position strongly in the market for their product feature and user acceptance satisfaction. To combat against DDoS attack Fortinet have their own appliance named FortiDDoS. It's now most effective hardware appliance of Fortinet. It must be positioned between the internal network resources like server and outside network or internet. After deploying it first monitor the traffic (for both incoming & outgoing) and record it and after 1 to 7 days later it will prevent the DDoS attack after enabling the prevention method configuration. When it detects any abnormal traffic or legitimate traffic it will then successfully drop that traffic to prevent DDoS attack. To deploy the DDoS prevention configuration we need to configure the basic configuration i.e add admin password, configure management network interfaces, add static routes, set system time and register with Fortinet technical support etc. on our FortDDoS appliance. Now, we firstly Enter the Global Settings and under this settings we'll select the "Service Protection Profile" or SPP and then Click "Config". Now, we will create a new Service Protection Profile as "web_servers" and Save it which is shown in below:



#	Service Protection Profile Name	ID
1	SPP-0	0

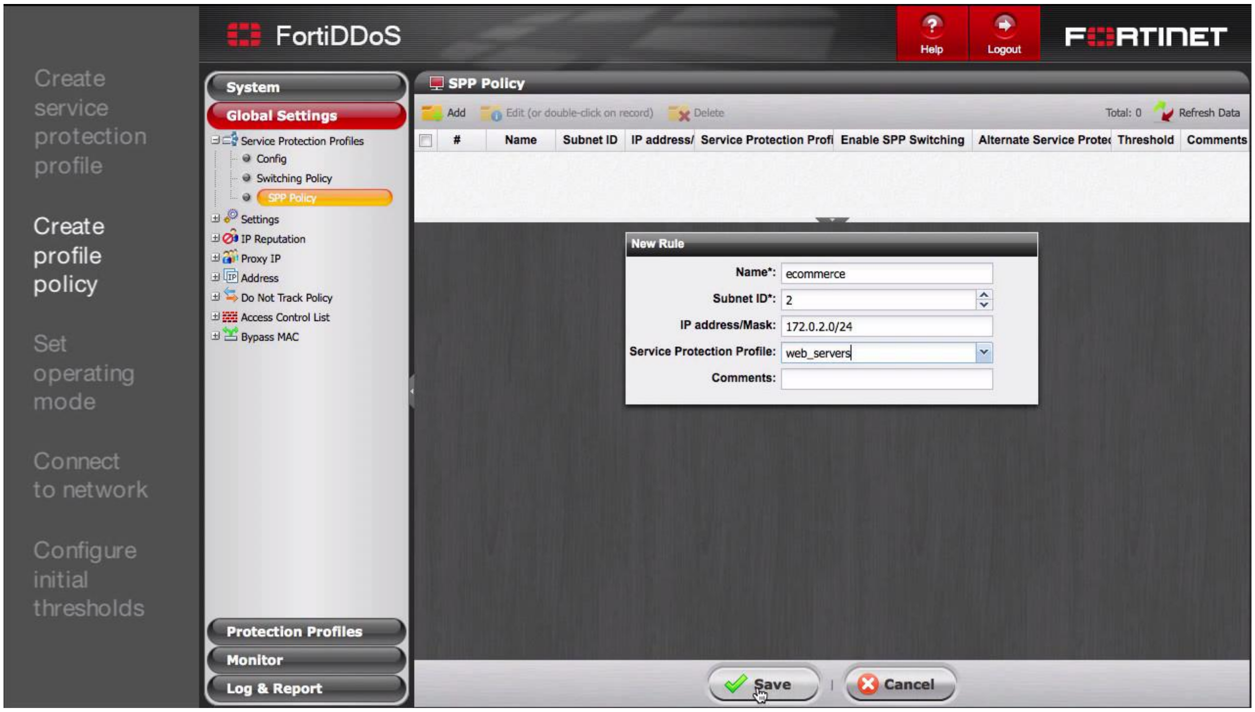
New Service Protection Profile

Name: web_servers

ID: 2

Figure 5.3.4: Create Service Protection Profile (SPP) [27].

At this stage, we need to create a profile policy or “SPP Policy” which consists of a “Profile Name” as ecommerce, a “Subnet ID” as 2, “IP address / Mask” as 172.0.20.0/24 and pre-configured “Service Protection Profile or SPP” as web_servers which is shown in below:



#	Name	Subnet ID	IP address/	Service Protection Profi	Enable SPP Switching	Alternate Service Protec	Threshold	Comments

New Rule

Name*: ecommerce

Subnet ID*: 2

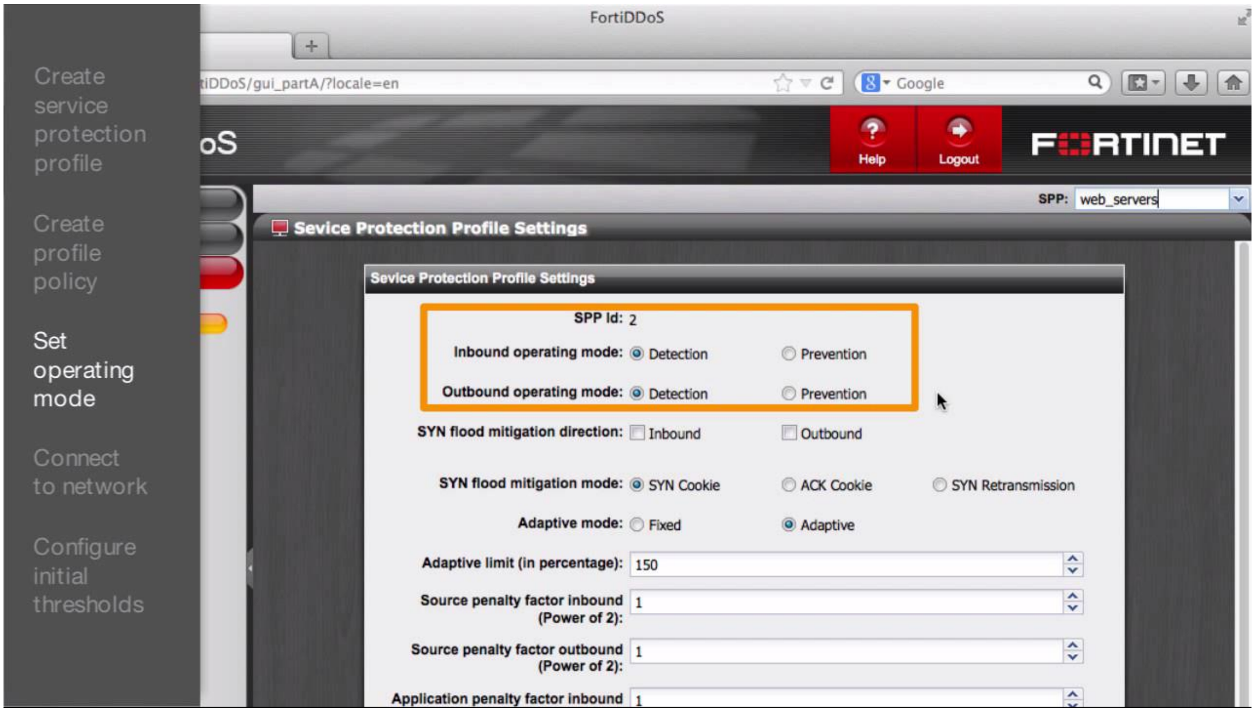
IP address/Mask: 172.0.2.0/24

Service Protection Profile: web_servers

Comments:

Figure 5.3.5: Create Profile Policy or SPP policy [27].

Now, we need to "Set Operating Mode" and by-default it is in "Detection" phase. In this phase the FortiDDoS just tracks and record and examine the incoming traffic towards the network resources. In this stage it doesn't blocked any traffic where it should be keep in detection mode for 2 to 7 days generally. The below figures illustrates the same which is given below:



SPP: web_servers

Sevice Protection Profile Settings

Sevice Protection Profile Settings

SPP Id: 2

Inbound operating mode: ● Detection ○ Prevention

Outbound operating mode: ● Detection ○ Prevention

SYN flood mitigation direction: □ Inbound □ Outbound

SYN flood mitigation mode: ● SYN Cookie ○ ACK Cookie ○ SYN Retransmission

Adaptive mode: ○ Fixed ● Adaptive

Adaptive limit (in percentage): 150

Source penalty factor inbound (Power of 2): 1

Source penalty factor outbound (Power of 2): 1

Application penalty factor inbound 1

Figure 5.3.6: Set Operating Mode as Detection in SPP settings [27].

After define the Service Protection Profile and Policy now we need to connect our FortiDDoS with our network. Here, under the Shared Interfaces there is 2 pair of RJ-45 Ethernet port (1 to 4) and SFP Port (1 to 4) which connects Fiber optic network. If we use Ethernet port 1 & 2 which is used as LAN 1(port 1) and WAN 1(port 2) and if we use port 3 & 4 which is also used as LAN 2(port 3) and WAN 2(port 4). So if we use port 1 for LAN we must use port 2 for WAN which is given below:

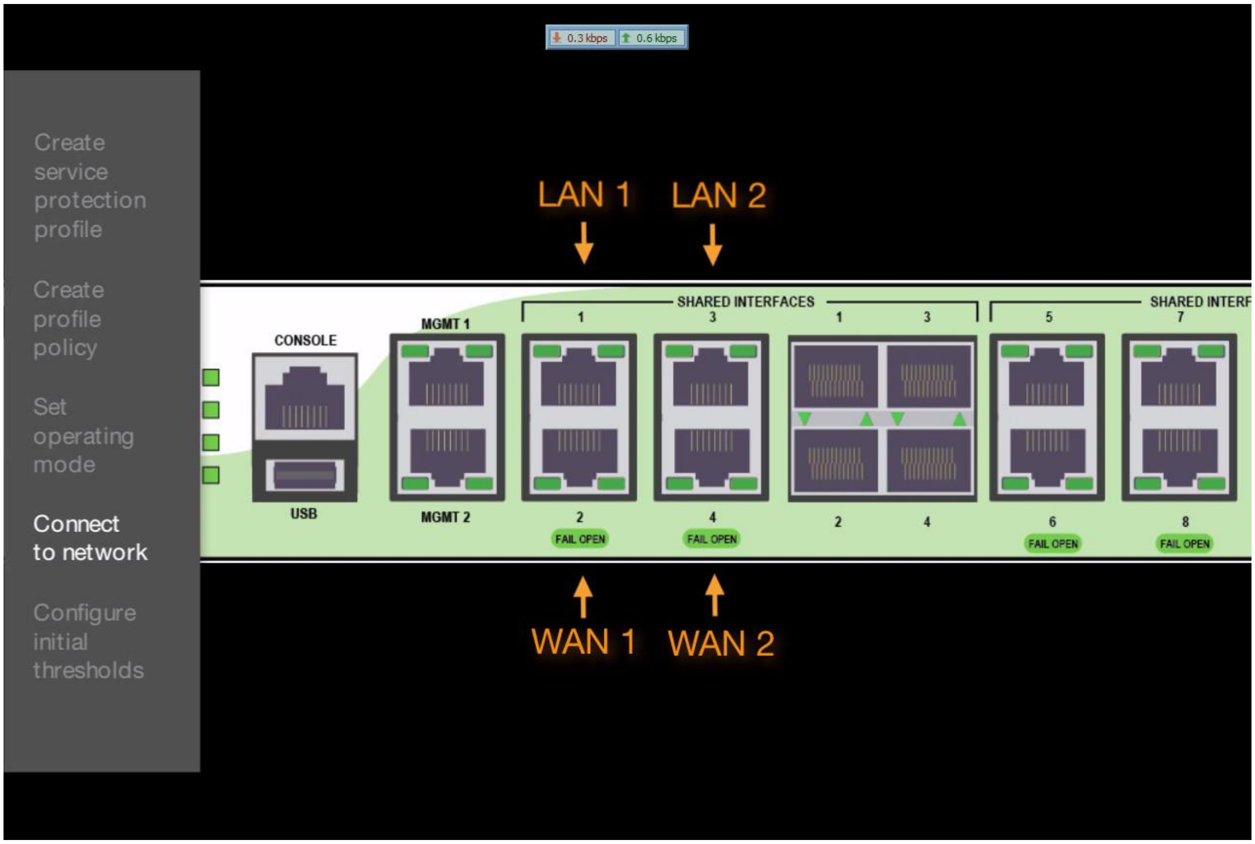
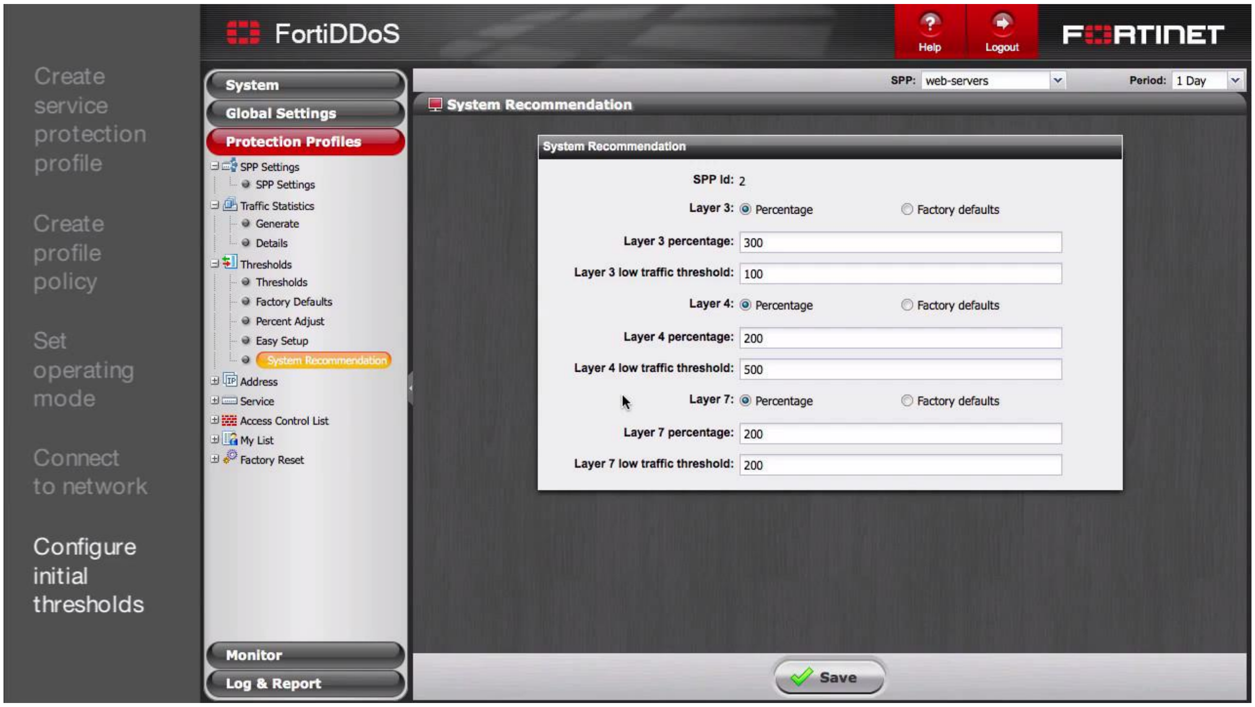


Figure 5.3.7: Connect FortiDDoS to the Network [27].

When the FortiDDoS passed the learning period then we can set the custom threshold to get best result. We can set the maximum value parameters to protect DDoS attack in a wider range.



Create service protection profile

Create profile policy

Set operating mode

Connect to network

Configure initial thresholds

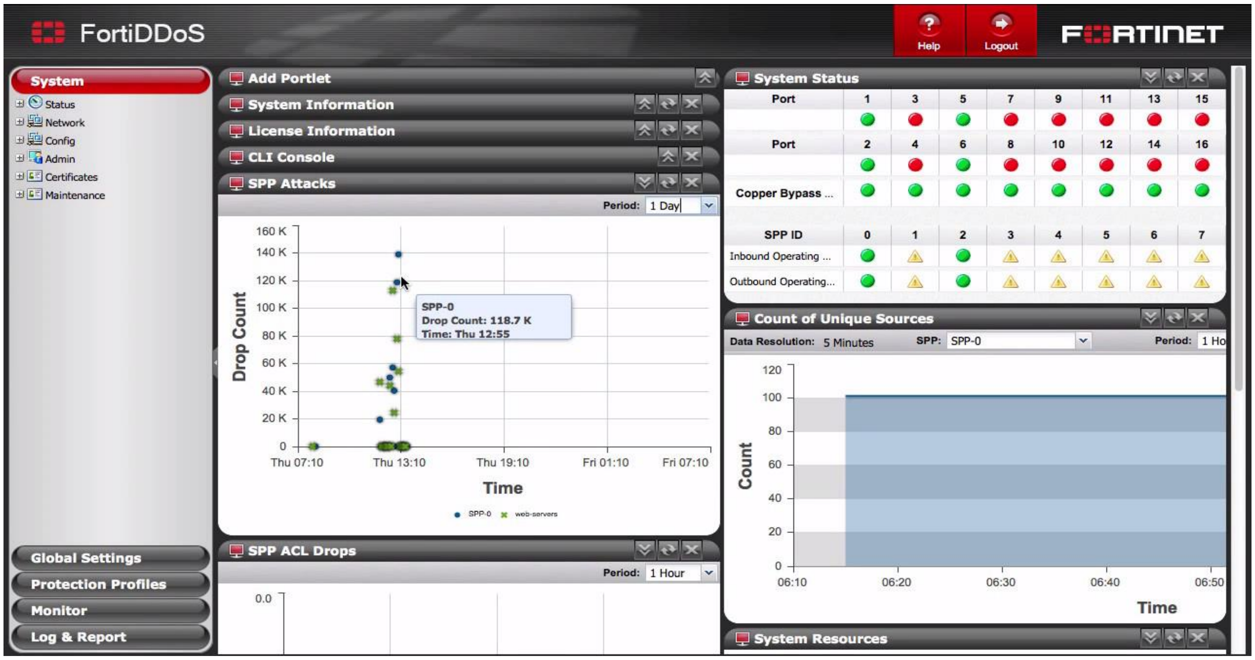
SPP: web-servers Period: 1 Day

System Recommendation

SPP Id:	2	
Layer 3:	● Percentage	○ Factory defaults
Layer 3 percentage:	300	
Layer 3 low traffic threshold:	100	
Layer 4:	● Percentage	○ Factory defaults
Layer 4 percentage:	200	
Layer 4 low traffic threshold:	500	
Layer 7:	● Percentage	○ Factory defaults
Layer 7 percentage:	200	
Layer 7 low traffic threshold:	200	

Figure 5.3.8: Configure the Threshold [27].

Here, we can see the default threshold value for Layer 3,4 & 7 where FortiDDoS calculate the threshold value in this parameter against the attack. Now, we'll keep that configuration for few days as "Detection" mode to track any abnormal or legitimate traffic. After that, we we'll check the Log to find any malicious traffic on the FortiDDoS appliance which is given below:



SPP-0
Drop Count: 118.7 K
Time: Thu 12:55

System Status

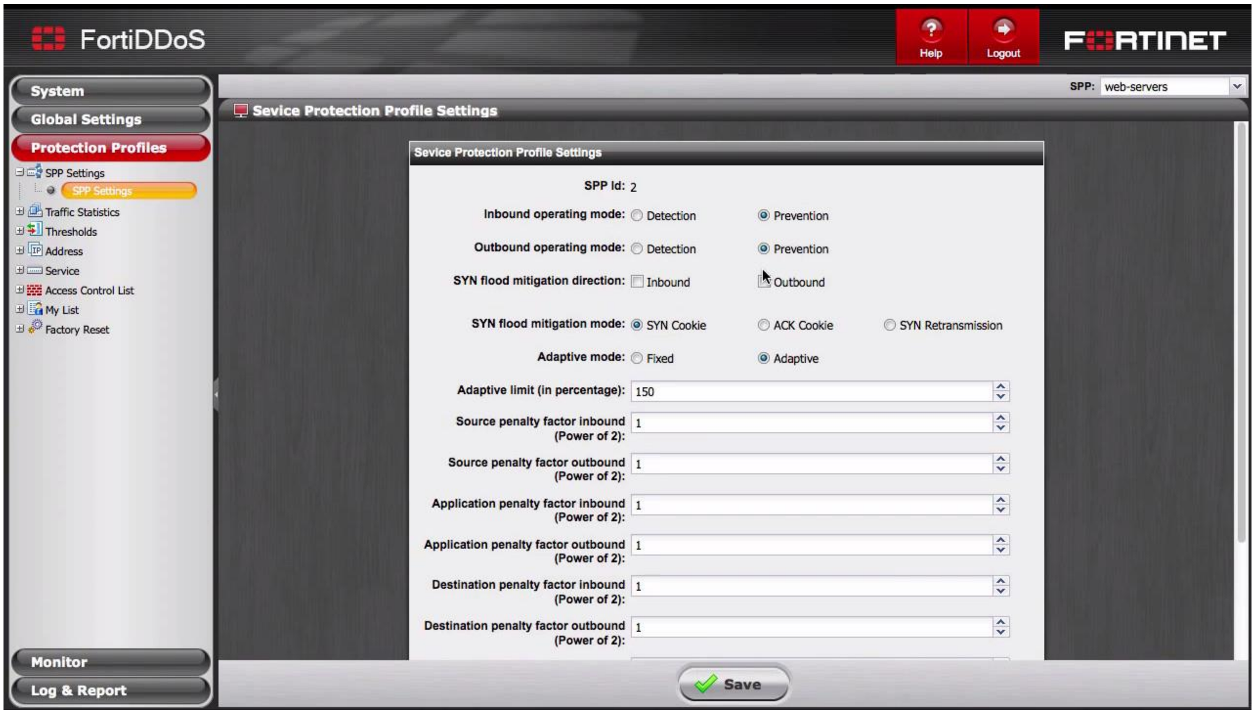
Port	1	3	5	7	9	11	13	15
	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴
Port	2	4	6	8	10	12	14	16
	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴
Copper Bypass ...	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
SPP ID	0	1	2	3	4	5	6	7
Inbound Operating ...	🟢	⚠	🟢	⚠	⚠	⚠	⚠	⚠
Outbound Operating...	🟢	⚠	🟢	⚠	⚠	⚠	⚠	⚠

Count of Unique Sources

Data Resolution: 5 Minutes SPP: SPP-0 Period: 1 Ho

Figure 5.3.9: Check the Log for abnormal traffic [27].

As we can see that, the FortiDDoS find the abnormal traffic in “Detection” mode by checking the Log and now we’ll switch the protection profile from “Detection” mode to “Prevention” mode which is given below:



SPP: web-servers

Sevice Protection Profile Settings

Sevice Protection Profile Settings

SPP Id: 2

Inbound operating mode: ○ Detection ● Prevention

Outbound operating mode: ○ Detection ● Prevention

SYN flood mitigation direction: □ Inbound □ Outbound

SYN flood mitigation mode: ● SYN Cookie ○ ACK Cookie ○ SYN Retransmission

Adaptive mode: ○ Fixed ● Adaptive

Adaptive limit (in percentage): 150

Source penalty factor inbound (Power of 2): 1

Source penalty factor outbound (Power of 2): 1

Application penalty factor inbound (Power of 2): 1

Application penalty factor outbound (Power of 2): 1

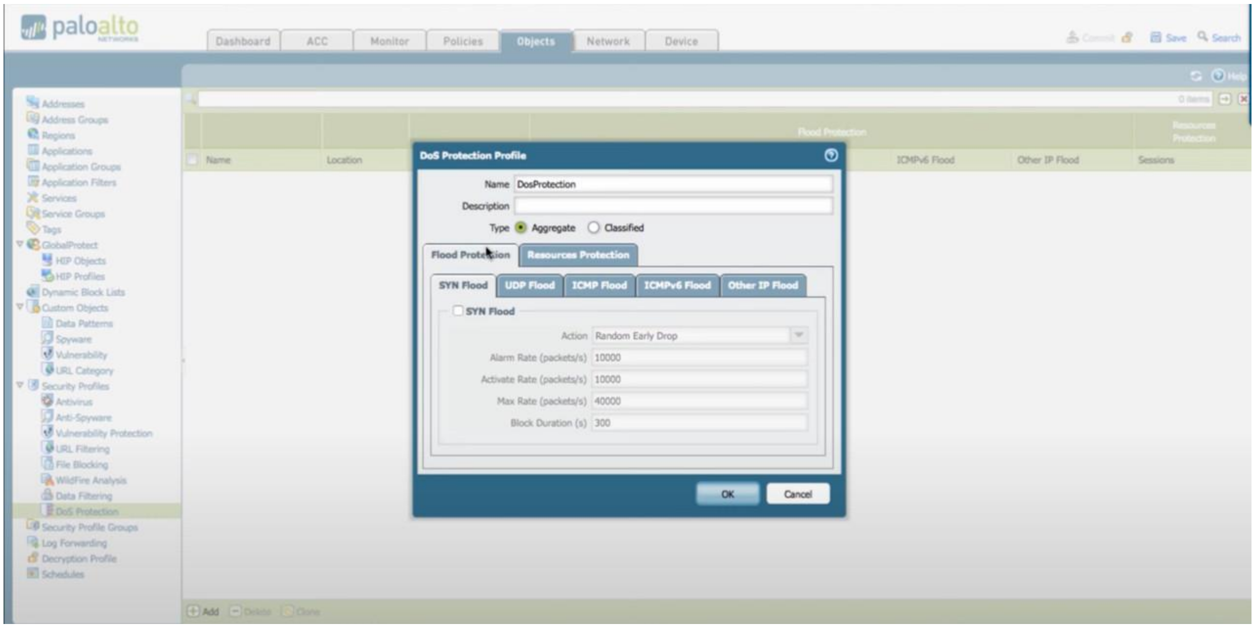
Destination penalty factor inbound (Power of 2): 1

Destination penalty factor outbound (Power of 2): 1

Figure 5.3.10: Set the Protection Profile as Prevention Mode [27].

III. **Palo Alto:** Palo Alto is renowned for its firewall feature in the networking area. It’s unique feature make it more popular in the current world. Now, we’ll demonstrate how can we take steps against DoS / DDoS attack by using Palo Alto Firewall in our network. The overall process is given below step by step:

First of all we need to configure the profile under “Object” tab > “Security Profiles” > “DoS Protection” and the click Add.



DoS Protection Profile

Name: DosProtection

Description:

Type: ● Aggregate ○ Classified

Flood Protection | Resources Protection

SYN Flood | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

□ SYN Flood

Action: Random Early Drop

Alarm Rate (packets/s): 10000

Activate Rate (packets/s): 10000

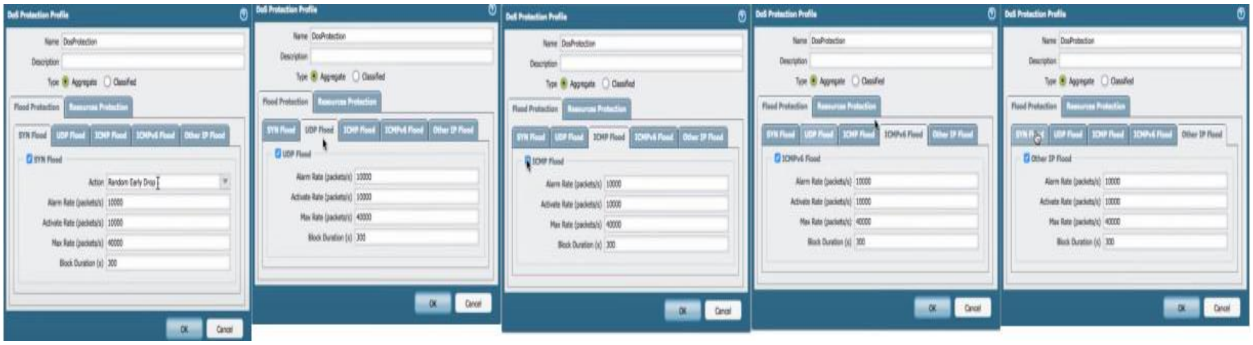
Max Rate (packets/s): 40000

Block Duration (s): 300

OK | Cancel

Figure 5.3.11: Create DoS Protection Profile [28].

Here, we giving a profile name as “DosProtection”, and select the profile type as “Aggregate” and now we’ll select the “Flood Protection” tab and give tick mark on the “SYN Flood”, “UDP Flood”, “ICMP Flood”, “ICMPV6 Flood” and “Other IP Flood” respectively which is given below:



Name: DosProtection

Type: ● Aggregate ○ Classified

☑ SYN Flood — Action: Random Early Drop; Alarm Rate (packets/s): 10000; Activate Rate (packets/s): 10000; Max Rate (packets/s): 40000; Block Duration (s): 300

☑ UDP Flood — Alarm Rate (packets/s): 10000; Activate Rate (packets/s): 10000; Max Rate (packets/s): 40000; Block Duration (s): 300

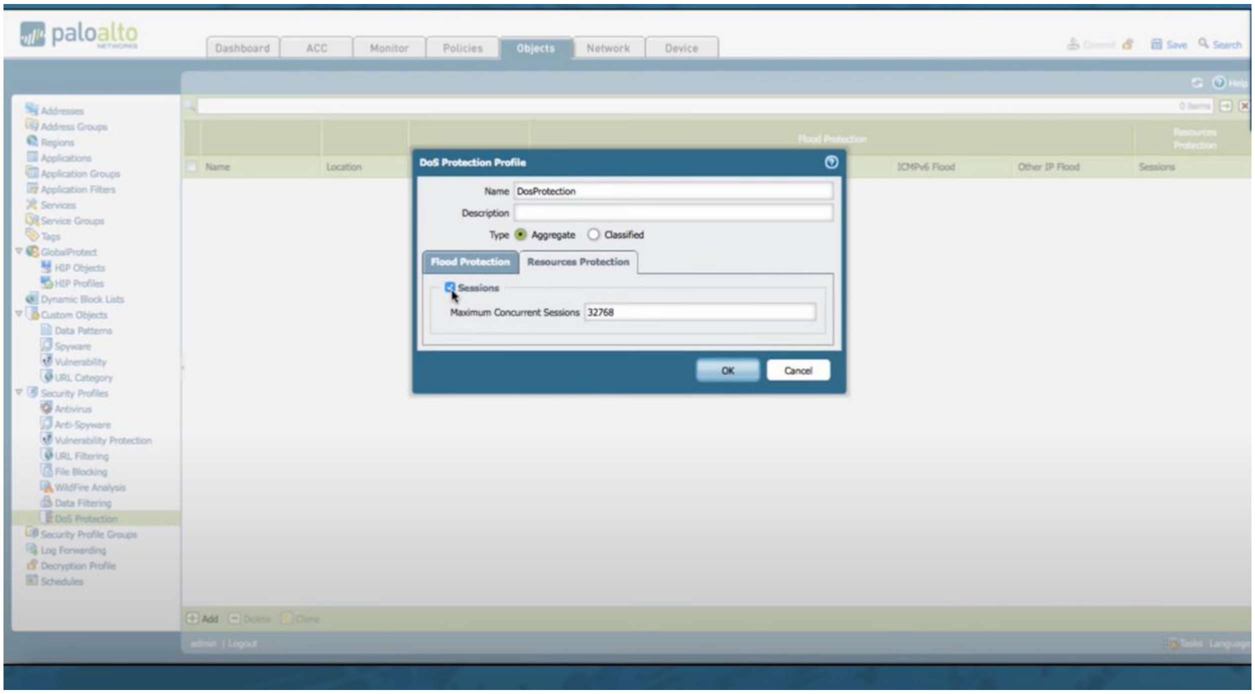
☑ ICMP Flood — Alarm Rate (packets/s): 10000; Activate Rate (packets/s): 10000; Max Rate (packets/s): 40000; Block Duration (s): 300

☑ ICMPv6 Flood — Alarm Rate (packets/s): 10000; Activate Rate (packets/s): 10000; Max Rate (packets/s): 40000; Block Duration (s): 300

☑ Other IP Flood — Alarm Rate (packets/s): 10000; Activate Rate (packets/s): 10000; Max Rate (packets/s): 40000; Block Duration (s): 300

Figure 5.3.12: Select all the Flood types under Flood Protection Tab [28].

In “Resource Protection” tab we’ll tick the “Session” and keep the default “Maximum Concurrent Session” as it is which is given below:



DoS Protection Profile

Name: DosProtection

Description:

Type: ● Aggregate ○ Classified

Flood Protection | Resources Protection

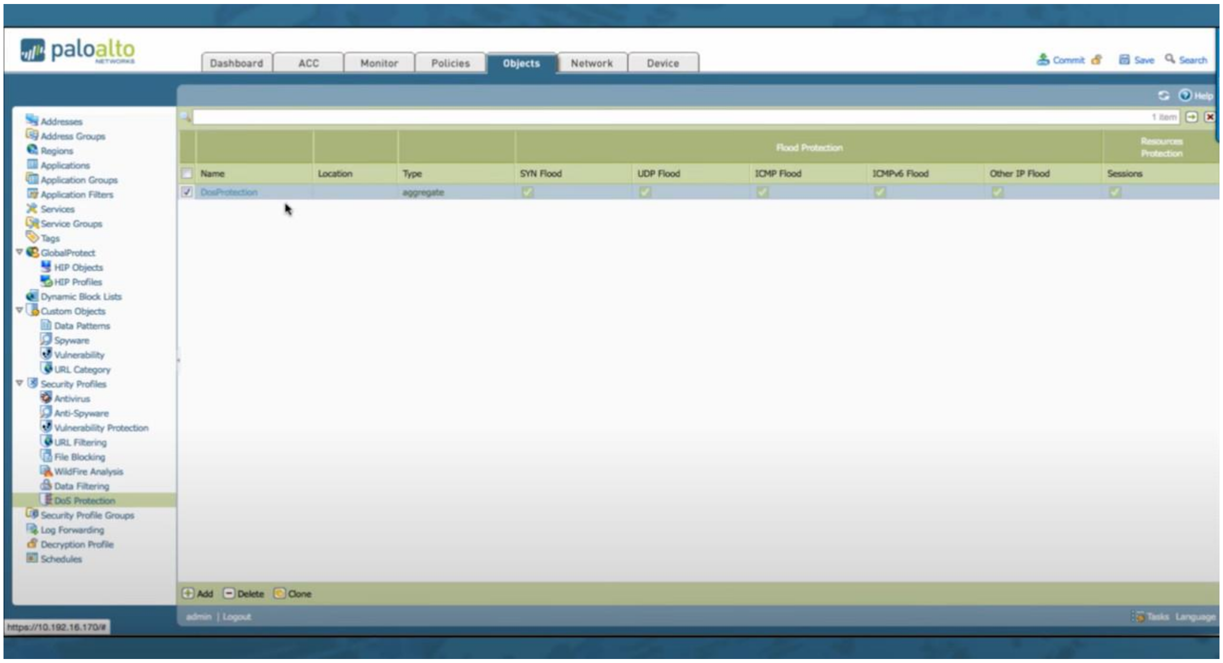
☑ Sessions

Maximum Concurrent Sessions: 32768

OK | Cancel

Figure 5.3.13: Select the Session under Resource Protection Tab [28].

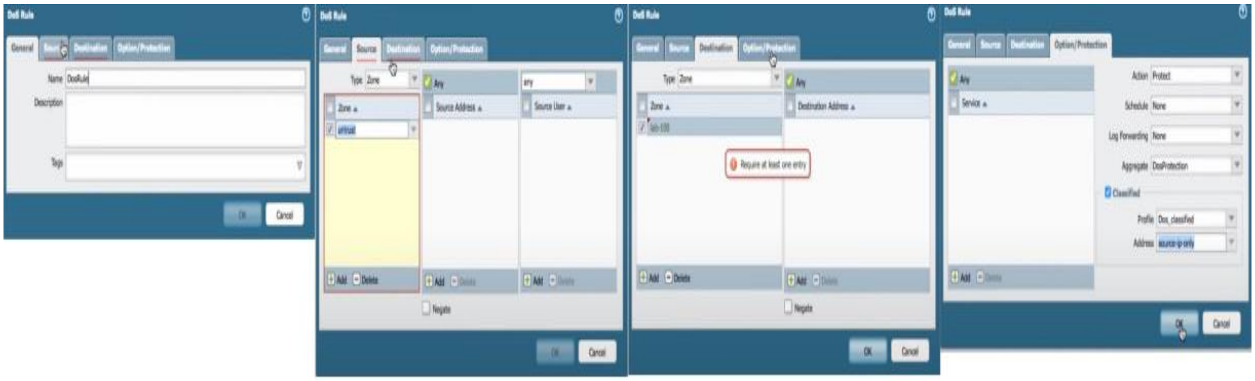
After Save the configuration we'll see our below configuration-



			Flood Protection					Resources Protection
Name	Location	Type	SYN Flood	UDP Flood	ICMP Flood	ICMPv6 Flood	Other IP Flood	Sessions
DosProtection		aggregate	✓	✓	✓	✓	✓	✓

Figure 5.3.14: Configuration of DoS Protection Profile under Object [28].

Now, we go to the Policy tab to configure the DoS Policy as similar way. After clicking the Add button we'll configure the "General", "Source", "Destination" and "Option / Protection" tab respectively which is appended below:



Name DosRule
Description
Tags

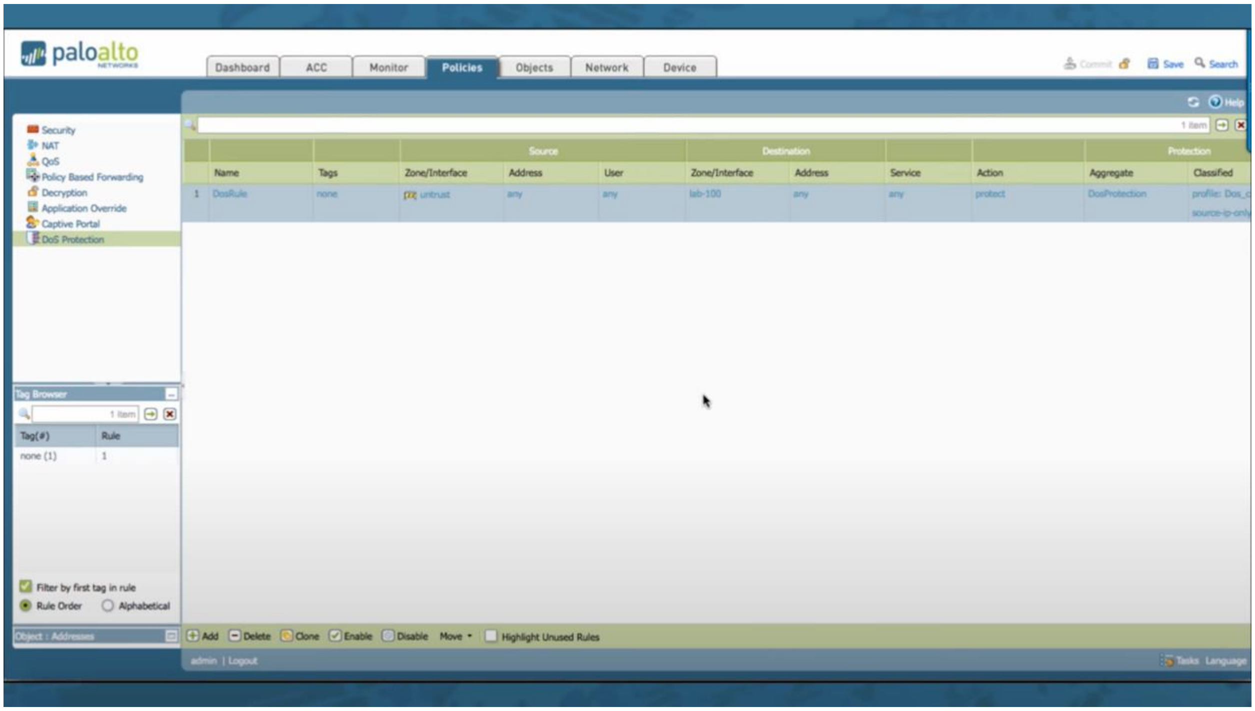
Type Zone
Zone
☑ untrust
☑ Any
Source Address
any
Source User
□ Negate

Type Zone
Zone
☑ lab-100
☑ Any
Destination Address
Require at least one entry
□ Negate

☑ Any
Service
Action Protect
Schedule None
Log Forwarding None
Aggregate DosProtection
☑ Classified
Profile Dos_classified
Address source-ip-only

Figure 5.3.15: Configuration all DoS Rule under Policy Tab [28].

Now, Click ok and Commit the configuration to save our configuration and then we get the following illustration:



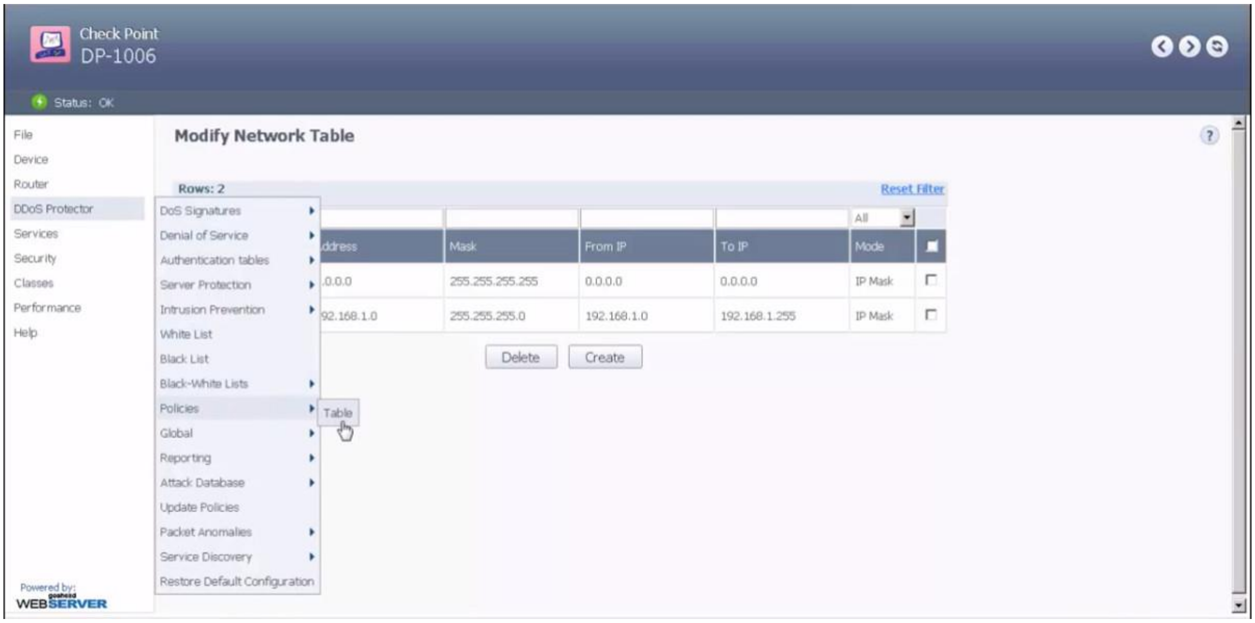
			Source			Destination				Protection	
	Name	Tags	Zone/Interface	Address	User	Zone/Interface	Address	Service	Action	Aggregate	Classified
1	DosRule	none	untrust	any	any	lab-100	any	any	protect	DosProtection	profile: Dos_c source-ip-only

Tag(#)	Rule
none (1)	1

Figure 5.3.16: Configuration of DoS Rule after Commit [28].

IV. **Check point:** At this stage we'll discuss about world's another most famous network device manufacturer named Check Point. Here, we only discuss about how Check Point DDoS Protector can be configured on the Check Point DP-1006 with screenshots which is given below:

To configure DDoS protection steps first of all we need to enter the Check Point DP-1006 device by using its username and password and then Click the "DDoS Protector" and to create a "Policy" we need to select & "Table" which is shown in below:



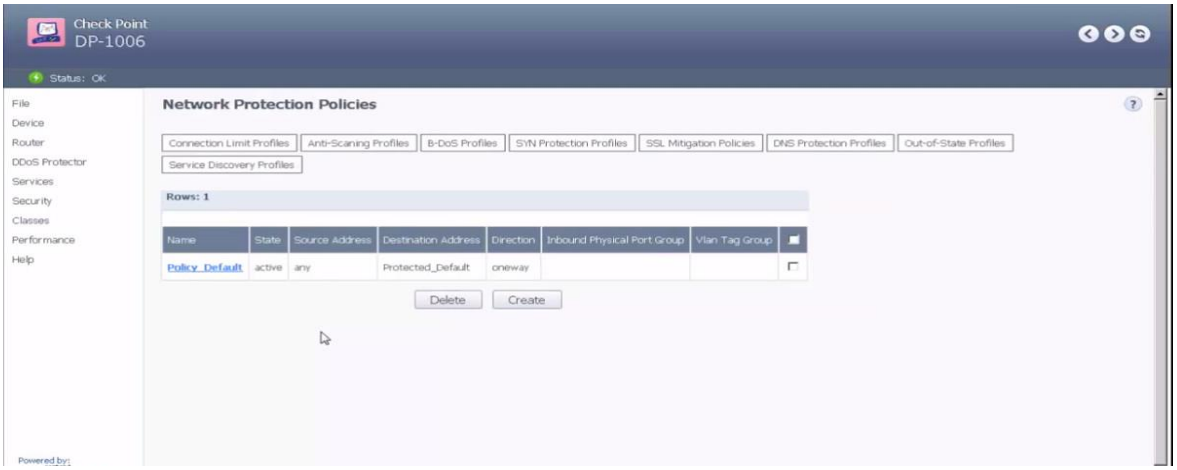
Modify Network Table

Rows: 2

ddress	Mask	From IP	To IP	Mode	
.0.0.0	255.255.255.255	0.0.0.0	0.0.0.0	IP Mask	□
92.168.1.0	255.255.255.0	192.168.1.0	192.168.1.255	IP Mask	□

Figure 5.3.17: Create a Policy under DDoS Protector Tab [29].

After that, Click "Policy Default" to configure the policy which is given below:



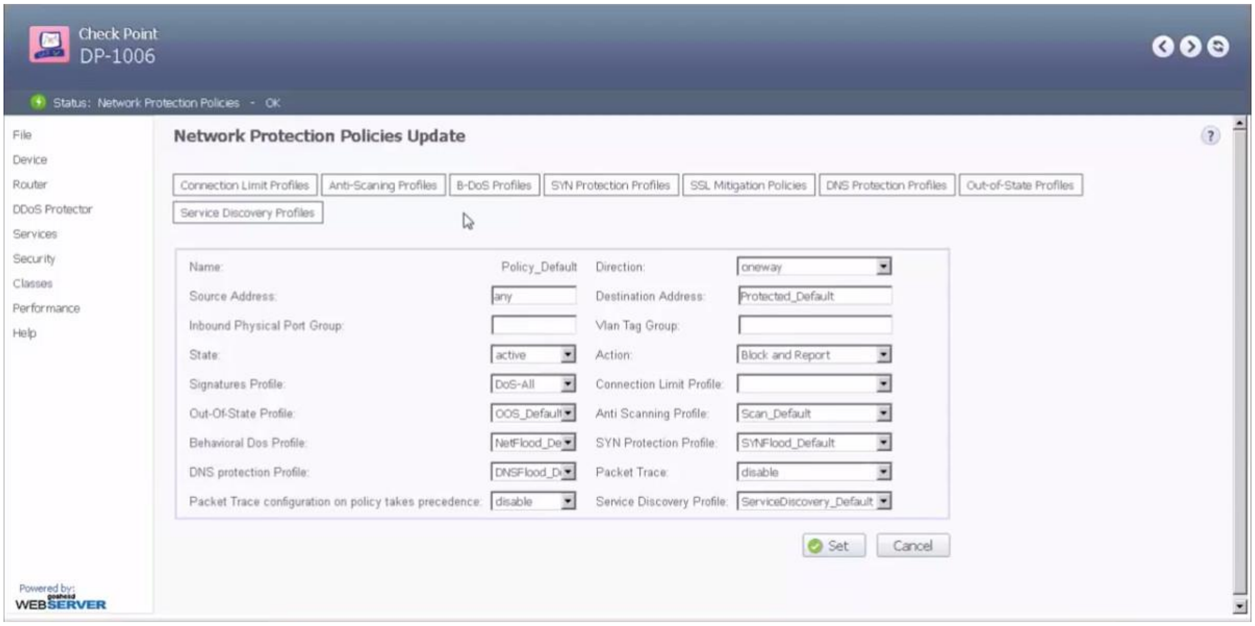
Network Protection Policies

Rows: 1

Name	State	Source Address	Destination Address	Direction	Inbound Physical Port Group	Vlan Tag Group	
Policy_Default	active	any	Protected_Default	oneway			□

Figure 5.3.18: Create Network Protection Policy [29].

Keep the Configuration by-default which is appended below:

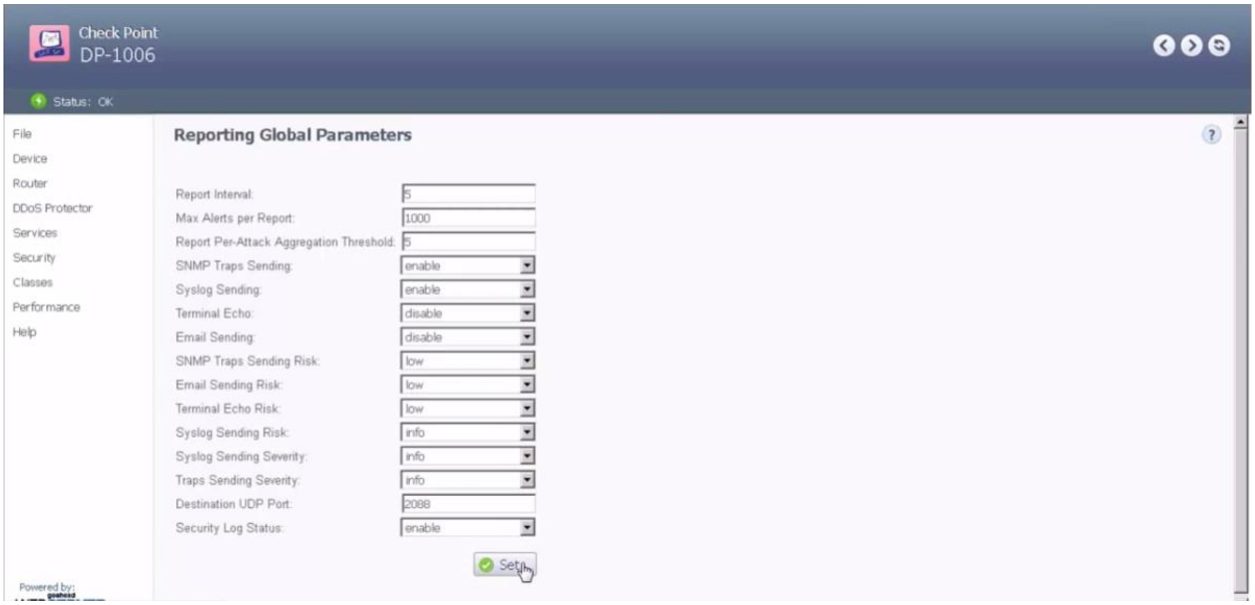


Network Protection Policies Update

Name:	Policy_Default	Direction:	oneway
Source Address:	any	Destination Address:	Protected_Default
Inbound Physical Port Group:		Vlan Tag Group:	
State:	active	Action:	Block and Report
Signatures Profile:	DoS-All	Connection Limit Profile:	
Out-Of-State Profile:	OOS_Default	Anti Scanning Profile:	Scan_Default
Behavioral Dos Profile:	NetFlood_De	SYN Protection Profile:	SYNFlood_Default
DNS protection Profile:	DNSFlood_D	Packet Trace:	disable
Packet Trace configuration on policy takes precedence:	disable	Service Discovery Profile:	ServiceDiscovery_Default

Figure 5.3.19: Configure Network Protection Policy [29].

Now, we set the “Global Parameters” from DDoS Protector < Reporting < Global Parameters which is shown in below:



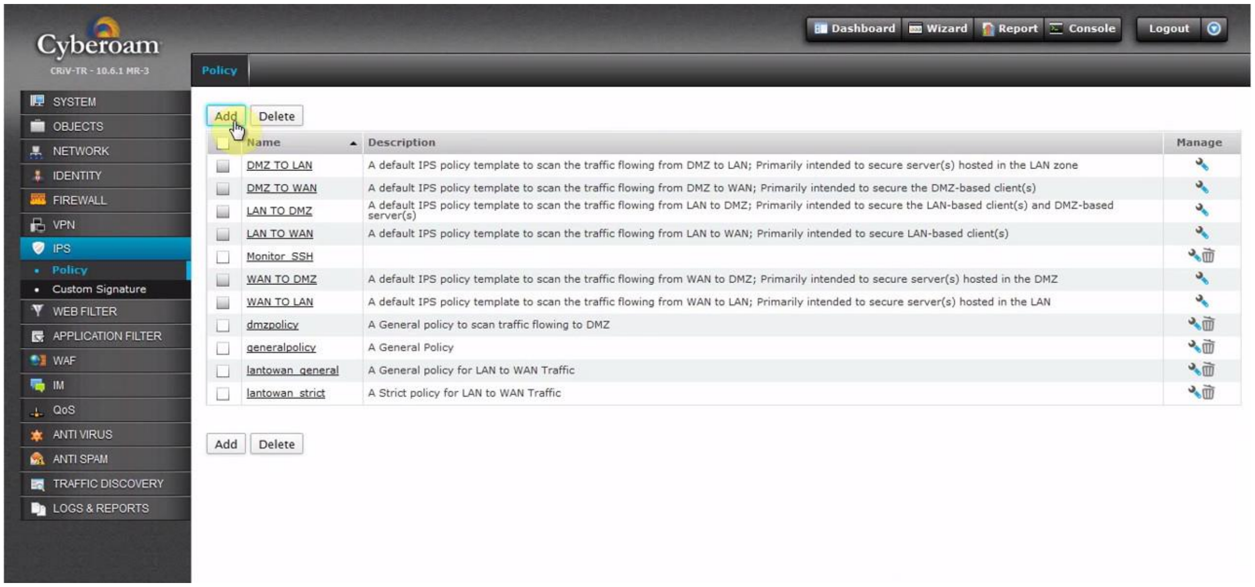
Reporting Global Parameters

Report Interval:	5
Max Alerts per Report:	1000
Report Per-Attack Aggregation Threshold:	5
SNMP Traps Sending:	enable
Syslog Sending:	enable
Terminal Echo:	disable
Email Sending:	disable
SNMP Traps Sending Risk:	low
Email Sending Risk:	low
Terminal Echo Risk:	low
Syslog Sending Risk:	info
Syslog Sending Severity:	info
Traps Sending Severity:	info
Destination UDP Port:	2088
Security Log Status:	enable

Figure 5.3.20: Set the Global Parameter [29].

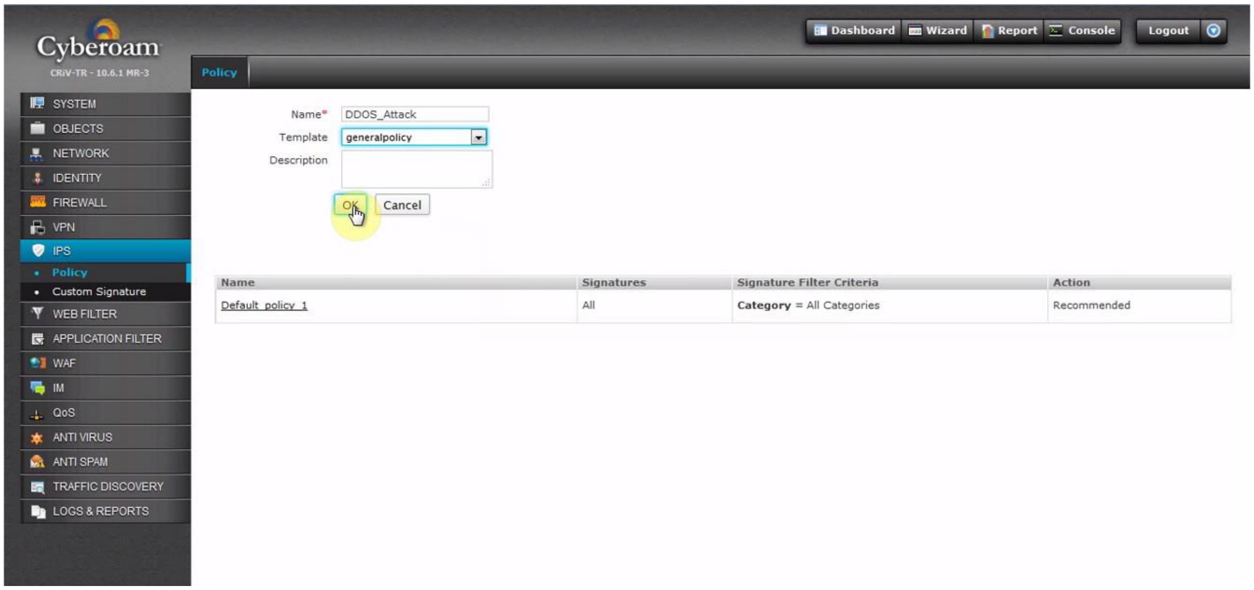
V. **Cyberoam:** Cyberoam is the global network security appliance provider which is also a Sophos subsidiary in the current network industry. Here, we demonstrate the steps against DDoS protection on Cyberoam Next Generation Firewall which is given below step by step:

At first we need to enter the appliance by using the administrative username and password. Now, Go to IPS < Policy and Click “Add” to create a new IPS Policy named "DDOS_Attack" and then select the "generalpolicy" from ‘Template’.



Name	Description	Manage
DMZ TO LAN	A default IPS policy template to scan the traffic flowing from DMZ to LAN; Primarily intended to secure server(s) hosted in the LAN zone	
DMZ TO WAN	A default IPS policy template to scan the traffic flowing from DMZ to WAN; Primarily intended to secure the DMZ-based client(s)	
LAN TO DMZ	A default IPS policy template to scan the traffic flowing from LAN to DMZ; Primarily intended to secure the LAN-based client(s) and DMZ-based server(s)	
LAN TO WAN	A default IPS policy template to scan the traffic flowing from LAN to WAN; Primarily intended to secure LAN-based client(s)	
Monitor_SSH		
WAN TO DMZ	A default IPS policy template to scan the traffic flowing from WAN to DMZ; Primarily intended to secure server(s) hosted in the DMZ	
WAN TO LAN	A default IPS policy template to scan the traffic flowing from WAN to LAN; Primarily intended to secure server(s) hosted in the LAN	
dmzpolicy	A General policy to scan traffic flowing to DMZ	
generalpolicy	A General Policy	
lantowan_general	A General policy for LAN to WAN Traffic	
lantowan_strict	A Strict policy for LAN to WAN Traffic	

Figure 5.3.21: Create Policy from IPS [30].

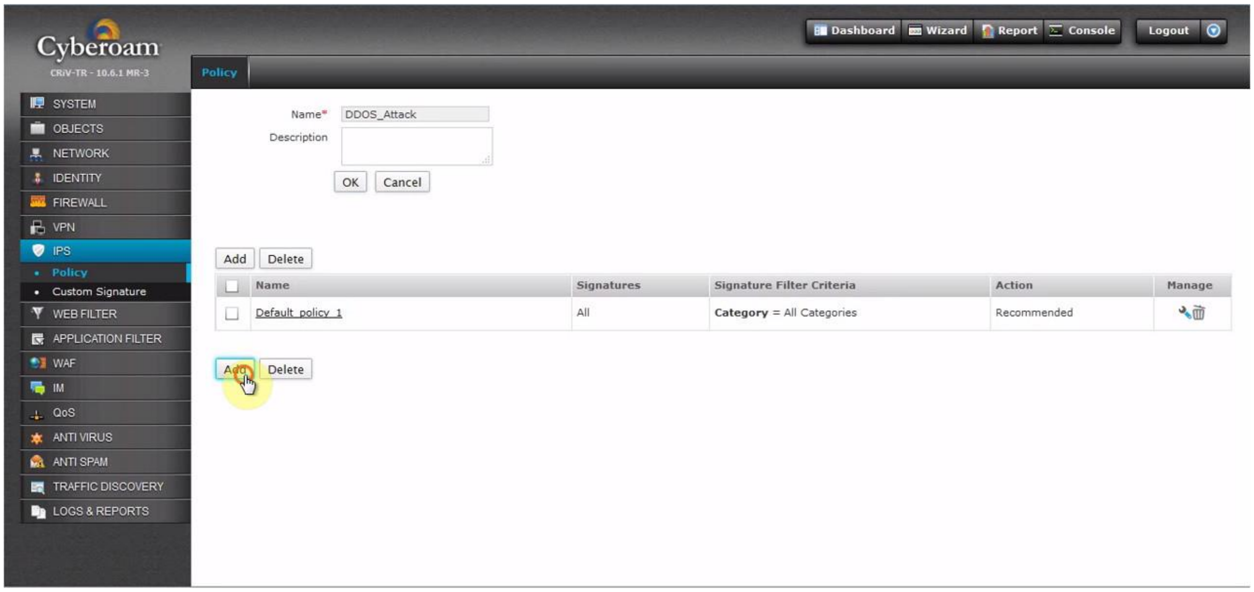


Name* DDOS_Attack
Template generalpolicy
Description

Name	Signatures	Signature Filter Criteria	Action
Default_policy_1	All	**Category** = All Categories	Recommended

Figure 5.3.22: Add the Policy Name and Template [30].

Now, click “Add” to configure the “Rule” for the “IPS Policy”.



Name* DDOS_Attack

Description

OK Cancel

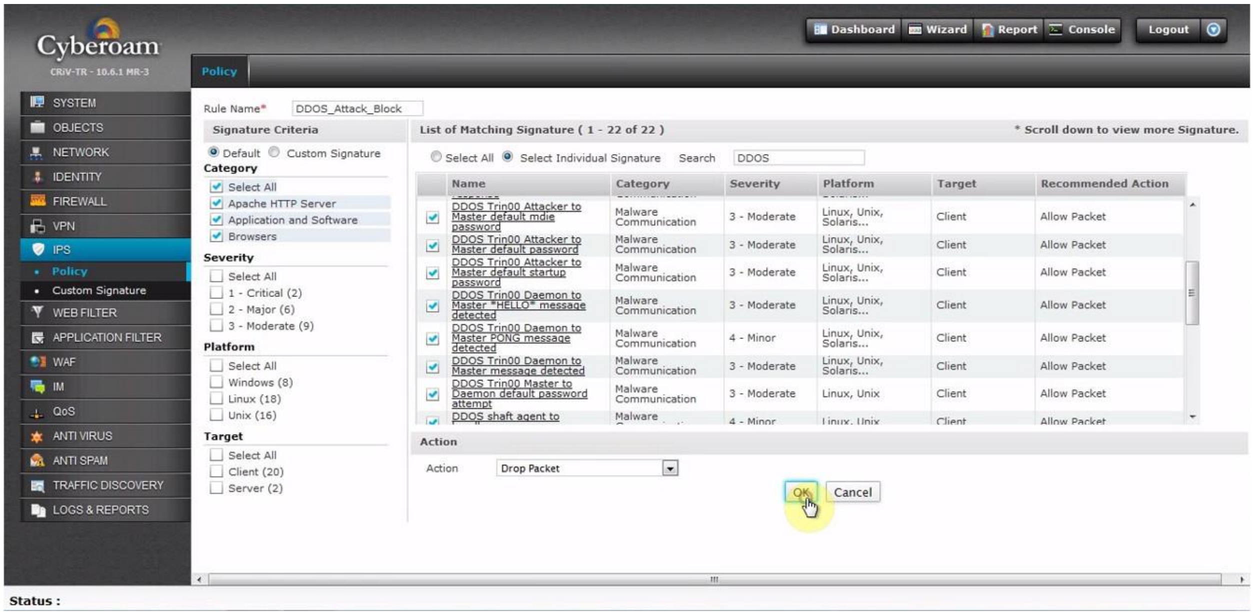
Add Delete

□	Name	Signatures	Signature Filter Criteria	Action	Manage
□	Default_policy_1	All	**Category** = All Categories	Recommended	

Add Delete

Figure 5.3.23: Add the Rule name for the Policy [30].

Now, name the Rule name as “DDOS_Attack_Block” and select all “Individual Signature” and search for DDoS signatures and select all the Name which relates only to DDOS and finally select the “Drop Packet” under Action function and then Click Ok to save the Rule configuration.



Rule Name* DDOS_Attack_Block

Signature Criteria

● Default ○ Custom Signature

Category

☑ Select All
☑ Apache HTTP Server
☑ Application and Software
☑ Browsers

Severity

□ Select All
□ 1 - Critical (2)
□ 2 - Major (6)
□ 3 - Moderate (9)

Platform

□ Select All
□ Windows (8)
□ Linux (18)
□ Unix (16)

Target

□ Select All
□ Client (20)
□ Server (2)

List of Matching Signature (1 - 22 of 22) * Scroll down to view more Signature.

○ Select All ● Select Individual Signature Search DDOS

	Name	Category	Severity	Platform	Target	Recommended Action
☑	DDOS Trin00 Attacker to Master default mdie password	Malware Communication	3 - Moderate	Linux, Unix, Solaris...	Client	Allow Packet
☑	DDOS Trin00 Attacker to Master default password	Malware Communication	3 - Moderate	Linux, Unix, Solaris...	Client	Allow Packet
☑	DDOS Trin00 Attacker to Master default startup password	Malware Communication	3 - Moderate	Linux, Unix, Solaris...	Client	Allow Packet
☑	DDOS Trin00 Daemon to Master *HELLO* message detected	Malware Communication	3 - Moderate	Linux, Unix, Solaris...	Client	Allow Packet
☑	DDOS Trin00 Daemon to Master PONG message detected	Malware Communication	4 - Minor	Linux, Unix, Solaris...	Client	Allow Packet
☑	DDOS Trin00 Daemon to Master message detected	Malware Communication	3 - Moderate	Linux, Unix, Solaris...	Client	Allow Packet
☑	DDOS Trin00 Master to Daemon default password attempt	Malware Communication	3 - Moderate	Linux, Unix	Client	Allow Packet
☑	DDOS shaft agent to	Malware	4 - Minor	Linux, Unix	Client	Allow Packet

Action

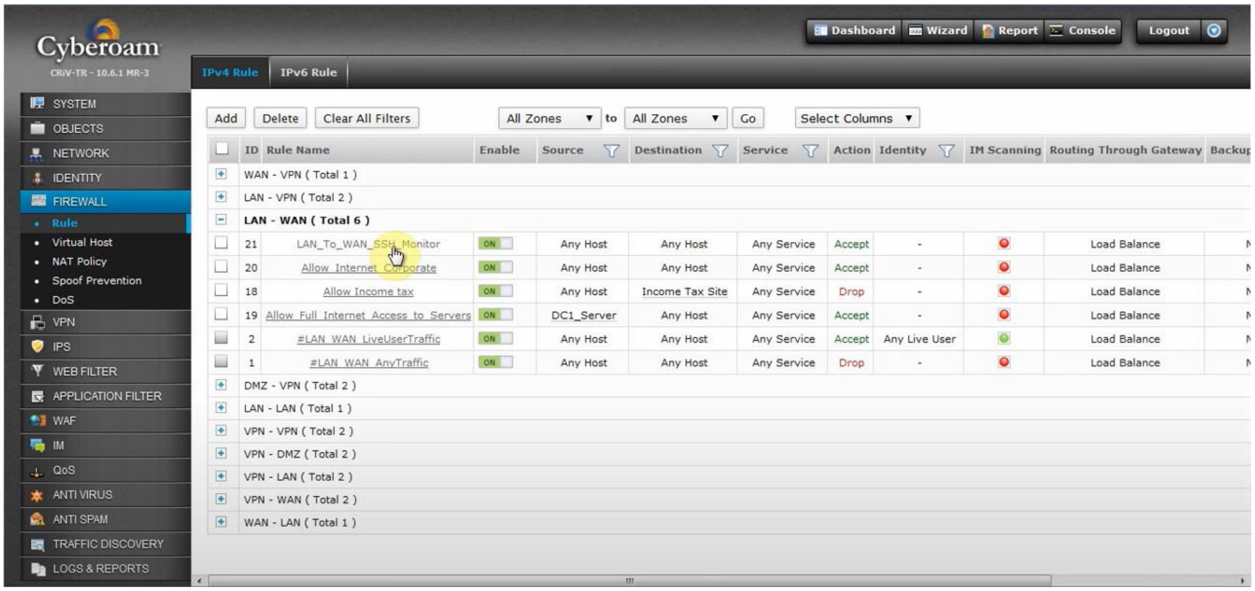
Action Drop Packet

OK Cancel

Status :

Figure 5.3.24: Configure the Rule Name, Select Individual Signature & Action [30].

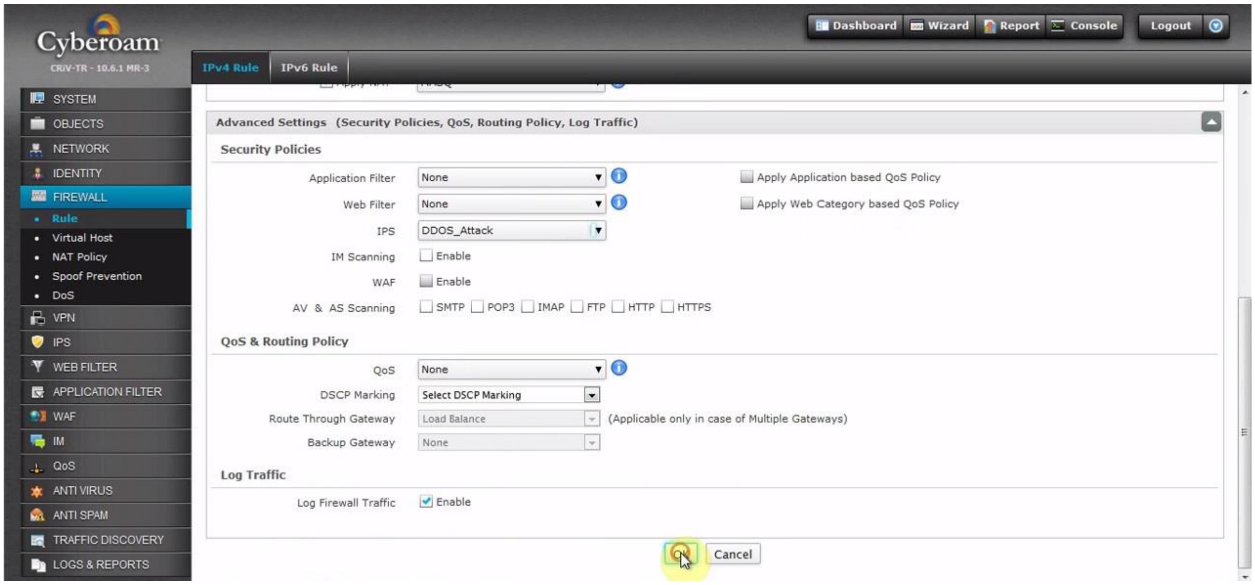
At this stage, go to FIREWALL < Rule < LAN - WAN < Click LAN_To_WAN_SSH_Monitor.



ID	Rule Name	Enable	Source	Destination	Service	Action	Identity	IM Scanning	Routing Through Gateway	Backup
WAN - VPN (Total 1)										
LAN - VPN (Total 2)										
LAN - WAN (Total 6)										
21	LAN_To_WAN_SSH_Monitor	ON	Any Host	Any Host	Any Service	Accept	-	●	Load Balance	N
20	Allow_Internet_Corporate	ON	Any Host	Any Host	Any Service	Accept	-	●	Load Balance	N
18	Allow Income tax	ON	Any Host	Income Tax Site	Any Service	Drop	-	●	Load Balance	N
19	Allow_Full_Internet_Access_to_Servers	ON	DC1_Server	Any Host	Any Service	Accept	-	●	Load Balance	N
2	#LAN_WAN_LiveUserTraffic	ON	Any Host	Any Host	Any Service	Accept	Any Live User	●	Load Balance	N
1	#LAN_WAN_AnyTraffic	ON	Any Host	Any Host	Any Service	Drop	-	●	Load Balance	N
DMZ - VPN (Total 2)										
LAN - LAN (Total 1)										
VPN - VPN (Total 2)										
VPN - DMZ (Total 2)										
VPN - LAN (Total 2)										
VPN - WAN (Total 2)										
WAN - LAN (Total 1)										

Figure 5.3.25: Configure the Firewall Rule for LAN - WAN [30].

Now, Click IPS and select "DDOS_Attack" and then Click Ok which to save the Firewall Rule is shown in below:



Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)

Security Policies

Application Filter: None — □ Apply Application based QoS Policy

Web Filter: None — □ Apply Web Category based QoS Policy

IPS: DDOS_Attack

IM Scanning: □ Enable

WAF: □ Enable

AV & AS Scanning: □ SMTP □ POP3 □ IMAP □ FTP □ HTTP □ HTTPS

QoS & Routing Policy

QoS: None

DSCP Marking: Select DSCP Marking

Route Through Gateway: Load Balance (Applicable only in case of Multiple Gateways)

Backup Gateway: None

Log Traffic

Log Firewall Traffic: ☑ Enable

Figure 5.3.26: Select the DDOS_Attack from IPS [30].

When the IPS policy is once applied, Cyberoam keeps monitoring the packets that match the configured “IPS signature”. If any such packets are found, Cyberoam drops that particular packet successfully which then protect the network against DDoS attack.

Now-a-days, networking manufacturer are working hard for deliver the best appliance to protect DDoS attack. As we can see from our above discussion there are various criteria to setup the configuration against DDoS and it can be vary from vendor to vendor. In this chapter, I had only mention the world’s famous networking device manufacturer which they deliver their customer for protecting the DDoS attack and earlier I was proposed my personal solutions against DDoS attack. Here, I couldn’t show the configuration process for different vendor to protect DDoS attack because it is impossible to me to do show it in real time in a live network and it is also tough to manage such kind of several appliance to show the process for the same. So, I Google for it to find the best way and as well as easy process to show the configuration demonstration from the particular resources. I think I learned a lot about this and introducing the new parameter during configuration process. I had try my best to show it for demonstration and as well as understanding also.

CHAPTER 6

Conclusion

DDoS attack is considered as the premium security issues in the present internet world. Protection against DDoS attack should be taken in an effective way by the companies and ISPs. DDoS detection is considered as one of the main steps to avoiding the DDoS issues. In chapter 3, I have demonstrate a DoS simulation where I was tried to show how a DoS attacks look like which is a TCP SYN flood based on Python script over a VM. We have observed that after executing the attack the particular website response slowly or it was take more time to restore the page. In chapter 4, I have tried to discuss most of the DDoS attack tools and its detection method also. Now-a-days, the behavior of DDoS attack evolving day by day so the tools of this attack is changed or developed at the same time. It is very important to when a web server got the attack by a network admin or system admin. If we can't coordinate the attack strategies it will then tough to defend the attack. I think early detection is very much helpful to defend the attack. In chapter 5, I have discuss my proposed solution to protect DDoS attack and how can we configure the steps against DDoS attack in our network devices by using different network manufacturer in the world. Here, I merge today's most famous and effective network appliance for their configuration steps against DDoS attack with the screenshots. As the attack evolving day by day so we shouldn't depend on the appliances but we should also gather information when and what's the status of the attack to successfully prevent it. If we doesn't maintenance the most unsafe machines from the internet then attacker can use them to execute the DDoS attack by using their vulnerabilities. So, we have to focus on that particularly very strongly if we always keep our system/network safe from such a dangerous attack which is mainly connected to the internet. As well as, we have to take measures in a various level to ensure the protection against it. Actually, most of the people aren't aware about the security issues in today's insecure internet world so that we have loose many valuable data or information for the same. The number of website increases day by day so that we should also take prevention protect them from such a DDoS attack. I have put in a lot of effort and thought to build this project. May be there is some limitations in this project I think so. If I get time in future I'll try to develop this project fruitful and will provide more information. As I'm responsible for networking jobs in my organization and I've achieved a number of network security certificates so that I think such a project will be very much helpful for my future endeavor and as well as my upcoming career. It took three months to complete the project. I must say that these three month were an amazing experience of my life. The practical knowledge I gathered through this project will have enormous effect in my life.

References

[1] Sites.cs.ucsb.edu. 2021. [online] Available at: <https://sites.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf> [Accessed 5 March 2021].

[2] Internet Systems Consortium, I., 2021. Internet Domain Survey. [online] Isc.org. Available at: <https://www.isc.org/survey/> [Accessed 5 March 2021].

[3] C. Douligeris, A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Computer Networks, Volume 44, Issue 5, pp. 643-666, April 2004.

[4] C. Douligeris, A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 03), Darmstadt, Germany, pp. 190-193, Dec. 14-17, 2003.

[5] D. Moore, C. Shannon, D. J. Brown, G. Voelker, S. Savage. "Inferring Internet Denial-of- Service Activity",ACM Transactions on Computer Systems, 24 (2), pp 115-139, 2006.

[6] Juniper Network, "Combating Bots and Mitigating DDoS Attacks (Solution brief)", Juniper Networks, Inc, 2006.

[7] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms," ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April 2004.

[8] J. Molsa, "Mitigating denial of service attacks: A tutorial," Journal of computer security, 13, pp. 807-837, IOS Press, 2005.

[9] Peer.asee.org. 2021. [online] Available at: <https://peer.asee.org/senior-design-project-ddos-attack-detection-and-defense-simulation.pdf> [Accessed 6 March 2021].

[10] K. Kumar, R.C. Joshi and K. Singh, "An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks", iriss, 2006, IIT Madras.

[11] Cs.uccs.edu. 2021. [online] Available at: <http://cs.uccs.edu/~gsc/pub/master/acearns/doc/angThesis-final.pdf> [Accessed 6 March 2021].

[12] UKFast Blog. 2021. DDoS Attacks: A History of their Evolution| UKFast blog. [online] Available at: <https://www.ukfast.co.uk/blog/2019/04/16/ddos-attacks-history-of-evolution/> [Accessed 6 March 2021].

[13] Cybersecurity Magazine. 2021. The History and Future of DDoS Attacks - Cybersecurity Magazine. [online] Available at: <https://cybersecurity-magazine.com/the-history-and-future-of-ddos-attacks/> [Accessed 6 March 2021].

[14] 2021. [online] Available at: <https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/> [Accessed 6 March 2021].

[15] Cybersecurity Magazine. 2021. The History and Future of DDoS Attacks - Cybersecurity Magazine. [online] Available at: <https://cybersecurity-magazine.com/the-history-and-future-of-ddos-attacks/> [Accessed 6 March 2021].

[16] Learning Center. 2021. DDoS Attack Types & Mitigation Methods | Imperva. [online] Available at: <https://www.imperva.com/learn/ddos/ddos-attacks/> [Accessed 7 March 2021].

[17] Cs.sjsu.edu. 2021. [online] Available at: <http://www.cs.sjsu.edu/faculty/stamp/students/Panicker_Anil.pdf> [Accessed 7 March 2021].

[18] eSecurityPlanet. 2021. Types of DDoS Attacks | eSecurity Planet. [online] Available at: <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/> [Accessed 7 March 2021].

[19] Digitalattackmap.com. 2021. Digital Attack Map. [online] Available at: <https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18699&view=map> [Accessed 23 March 2021].

[20] Radware.com. 2021. Seven Common DDoS Attack Tools. [online] Available at: <https://www.radware.com/security/ddos-knowledge-center/ddos-attack-types/common-ddos-attack-tools/> [Accessed 23 March 2021].

[21] Softwaretestinghelp.com. 2021. 8 Best DDoS Attack Tools (Free DDoS Tool Of The Year 2021). [online] Available at: <https://www.softwaretestinghelp.com/ddos-attack-tools/> [Accessed 23 March 2021].

[22] Kentik.com. 2021. [online] Available at: <https://www.kentik.com/kentipedia/ddos-detection/> [Accessed 26 March 2021].

[23] Log Analysis | Log Monitoring by Loggly. 2021. DDoS monitoring: how to know you're under attack | Loggly. [online] Available at: <https://www.loggly.com/blog/ddos-monitoring-how-to-know-youre-under-attack/> [Accessed 26 March 2021].

[24] Scholarworks.sjsu.edu. 2021. [online] Available at: <http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1101&context=etd_projects> [Accessed 26 March 2021].

[25] Iopscience.iop.org. 2021. ShieldSquare Captcha. [online] Available at: <https://iopscience.iop.org/article/10.1088/1742-6596/1237/3/032040> [Accessed 26 March 2021].

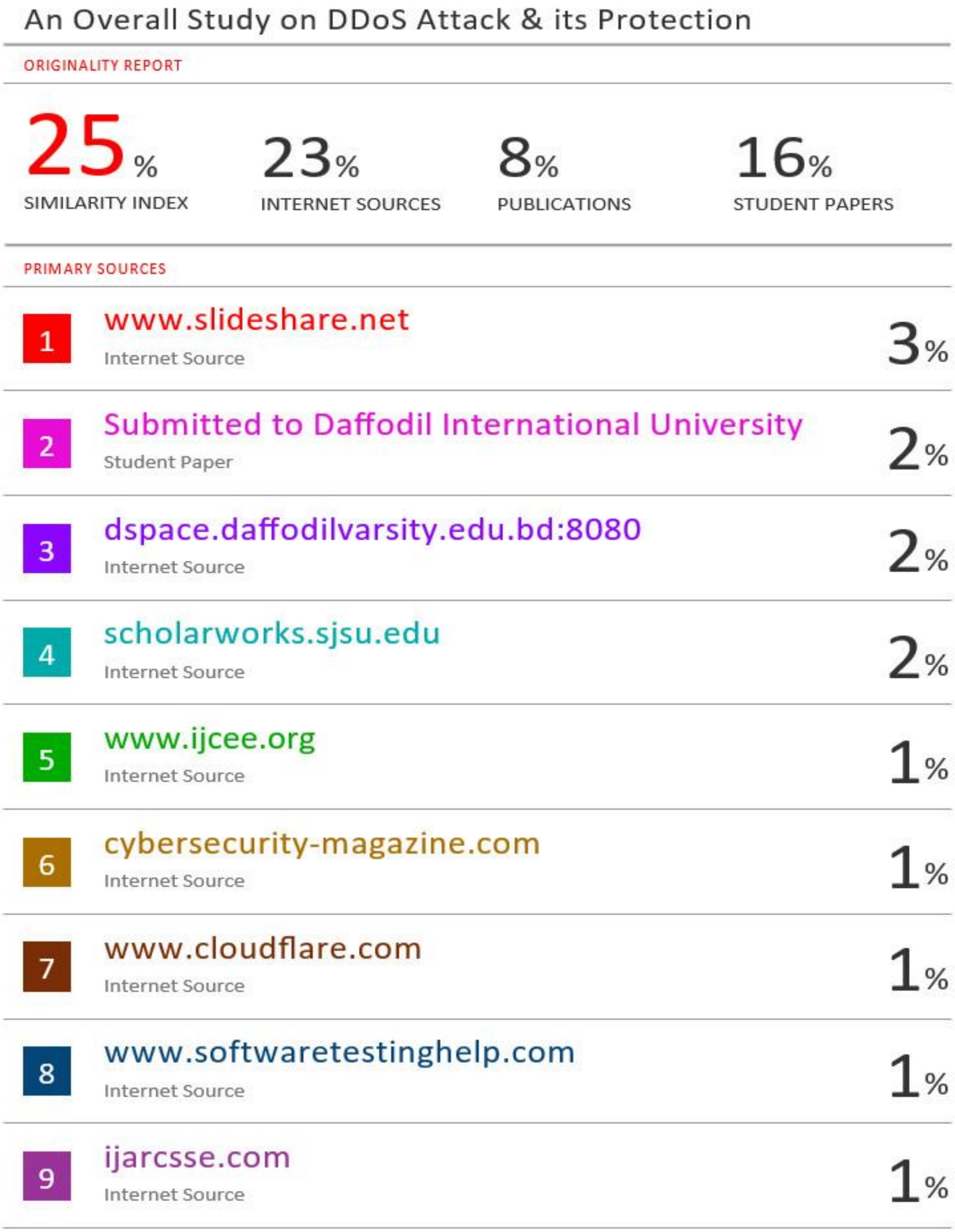
[26] Ciscolive.com. 2021. [online] Available at: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2663.pdf> [Accessed 28 March 2021].

[27] Fortinet Video Library latest. 2021. Latest. [online] Available at: <https://video.fortinet.com/latest/how-to-set-up-fortiddos-4-0> [Accessed 31 March 2021].

[28] Knowledgebase.paloaltonetworks.com. 2021. How to Set Up DoS Protection. [online] Available at: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmTCAS> [Accessed 31 March 2021].

[29] Youtube.com. 2021. Before you continue to YouTube. [online] Available at: <https://www.youtube.com/watch?v=gJHMbqHvmfs&ab_channel=samborskyi.com> [Accessed 1 April 2021].

[30] Youtube.com. 2021. Before you continue to YouTube. [online] Available at: <https://www.youtube.com/watch?v=n1wpq0Se0ls&ab_channel=KnowITFree> [Accessed 1 April 2021].



An Overall Study on DDoS Attack & its Protection

ORIGINALITY REPORT

25%	23%	8%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.slideshare.net Internet Source	3%
2	Submitted to Daffodil International University Student Paper	2%
3	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
4	scholarworks.sjsu.edu Internet Source	2%
5	www.ijcee.org Internet Source	1%
6	cybersecurity-magazine.com Internet Source	1%
7	www.cloudflare.com Internet Source	1%
8	www.softwaretestinghelp.com Internet Source	1%
9	ijarcsse.com Internet Source	1%