Title: Denial-of-Service Attack on web servers

Ali Zarafsani, CSCE University of North Texas

Members:  
Dharan Kumar Kunati

Seemaparvez Shaik

Srija Meryn Tupelly

Mounika Thogiti

Venkata Sai Chandrika Gudipati

# Abstract:

Today, most internet services are run by web applications. Web services include things like email programs, social networks, online banking, and web search engines. A server-side software application generates web content in real-time. Web servers serve as the home for websites. A web server is a machine that runs on an operating system and is connected to a database that houses many apps. An attack on the web server will result from any weakness in the network, operating system, database, or applications. In our project, we decided to evaluate web servers from Apache as they are most frequently used across different companies to check whether they are vulnerable to different DOS attacks. A Denial of Service (DoS) attack is a malicious attempt to reduce a targeted system's accessibility to authorized end users, such as a website or application. It obstructs a server, service, or network's regular traffic by saturating the target or its surrounding infrastructure with an excessive amount of internet traffic. It is a type of cybercrime when the perpetrator saturates a server with internet traffic to prevent people from accessing linked websites and online services.

# i. Introduction:

## The rise in DDOS Attacks:

One of the well-known cyberattacks are DDoS. The frequency and power of recent attacks, as well as the continuously changing attack vectors, make the development of new detection approaches tough, even though there are several viable solutions for the detection of DDoS attacks already in existence. DDOS attacks are increasing day by day. According to a report [1], DDoS attacks will increase by up to 31% in 2021 over the same duration in 2020, to 2.9 million attacks. An exponential increase has been observed in these attacks. The rise in DDOS attacks has been shown in the figure below.

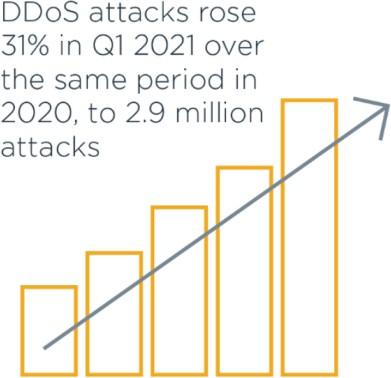


Figure 1: Rise in a DDOS attack

According to a Security Week report, researchers have discovered that there are typically 28,700 separate DDoS attacks that hit the Internet every day. [2] Recent data shows that DDoS attacks are becoming more powerful and frequent at an alarming rate. Nowadays, businesses and large corporations rely on automation and virtualization (cloud computing) to improve the availability and efficiency of their company operations and services. But this massive technological development was too fast for the security revolution to keep up. It is now easier for attackers to carry out any type of cyberattack since the number of vulnerable devices, such as networking and Internet of Things (IoT) devices, is growing faster than attempts to secure these devices. Due to all these factors, there is a need to consider the problem's intensity and seriousness more. We are still far from having a complete and reliable defense against DDoS attacks. We must think in ways that depart from conventional security concepts. To make the internet a safer place, a hybrid system that can manage unforeseen threats, can be broadly implemented, and every internet business has incentives to join and cooperation with each other is required.

## How Much Time a DDoS Attack Lasts?

DDoS assaults range widely in complexity and duration. A DDoS attack may last for a long time or last only briefly.

* Long-Term Attack: A long-term attack is one that is fought over several hours or days. For instance, the DDoS attack on AWS lasted three days before it was finally stopped.
* Burst Attack: These DDoS attacks are waged over a brief period, lasting only a minute or a few seconds.

Burst attacks can be immensely destructive yet being exceedingly rapid. It is now possible to

create more volumetric traffic than ever before thanks to the development of internet of things (IoT) devices and more potent computing equipment. Attackers can generate greater volumes of traffic in a shorter amount of time as a result. Because it is more challenging to trace, a burst DDoS attack frequently benefits the attacker.

## Technical Description of how DDoS work:

Distributed denial of service is known as DDoS. When a threat actor targets an organization's online activities using resources from numerous, distant places, the attack is known as a DDoS. DDoS assaults often concentrate on producing attacks that interfere with network services and equipment's normal operations for example, caching services, routers, and naming services. That is the fundamental issue. It's not necessary for sophisticated DDoS assaults to take advantage of open relays or default settings. They take advantage of expected behavior and the original design of the protocols that are used by modern devices.

A DDoS attacker manipulates the typical operation of the network services that we all depend on and trust in an analogous manner to how a social engineer manipulates the default workings of human communication. A DDoS assault overwhelms the targeted organization's resources with HTTP requests and traffic, preventing genuine users from accessing one or more of its services and resulting in a devastating outage. Cybercriminals use a DDoS assault to exploit regular interactions between network devices and servers. In DDOS, we apply patches (often referred to as mitigations) between your network and the threat actor rather than changing the resource that is being attacked.

DDoS attacks are not dependent on a specific network protocol or system flaw. [2] It merely takes advantage of the significant resource imbalance between the victim and the Internet. Due to the open nature of Internet architecture, each machine connected to it is publicly accessible to other devices connected to facilitate communication. Because of this openness, the hacker or attacker community may easily identify any Internet-connected device that is not safe. Thus, the found machine has the attack code on it. The infected machine can also be used to find and infect related machines in the future. Thus, the attacker progressively creates a botnet, or bot attack network. The affected machines can either be referred to as Masters/Handlers or zombies, depending on the attacker malware. Hackers instruct masters to manage zombies by sending commands to them as shown in the figure 2. Attack packets are transmitted by zombies controlled by masters or handlers and converge at the victim to deplete its resources. DDoS attacks primarily target the computational or communicational resources of the victim, including their bandwidth, memory, CPU cycles, file descriptors, and buffers, among other resources.

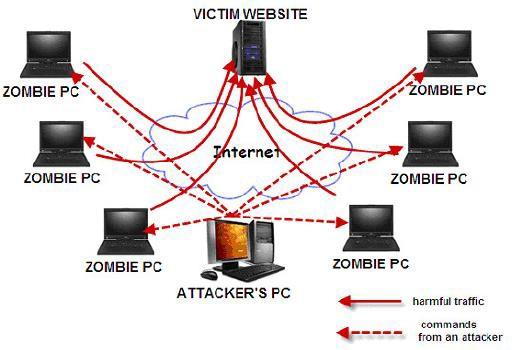


Figure 2: DDoS Attack architecture

# ii. Methods:

## Types of DDoS Attack:

A broad category of cyberattacks known as distributed denial of service (DDoS) obstructs internet resources and services by saturating them with traffic. As a result, the targeted web service is rendered unavailable throughout the DDoS attack. The distributed nature of the malicious traffic, which often comes from a botnet—a globally dispersed network of infected workstations under criminal control—is the distinguishing feature of DDoS attacks. Cybercriminals have created a variety of technological methods throughout the years for using DDoS to take down internet targets. There are three main categories of DDoS attacks the specific approaches are given below:

## Volumetric Attacks:

The most common DDoS assault, these attacks use techniques to produce enormous amounts of traffic to completely saturate bandwidth, causing a traffic jam that prevents legitimate traffic from entering or leaving the targeted site.

## Protocol Attacks:

Protocol assaults target Layer 3 and Layer 4 protocol interactions with nefarious connection requests to use the processing power of network infrastructure resources including servers, firewalls, and load balancers.

## Application Attacks:

Some of the most advanced DDoS attacks take advantage of flaws in Layer 7 of the application layer by initiating connections and requests for processes and transactions that use limited resources like memory and disc space.

# iii. Implementation:

All the hosted code and detailed steps to reproduce the attacks and mitigation rules for snort IDE can be accessed from [Project- Advanced Network Security](https://myunt-my.sharepoint.com/:f:/g/personal/dharankumarkunati_my_unt_edu/EljOl2othm1Bg79p51Z1eyIBatZCZXCgE1BIzK1AhQB6_A?e=41wadW) . Only users with UNT email can access the files. If you are unable to open the files, please contact [dharankumarkunati@my.unt.edu](mailto:dharankumarkunati@my.unt.edu).

## 1. Servers:

The reason we implemented multiple servers is to understand the effectiveness of implemented DDOS attacks and how different servers can respond to these threats.

### Simple web server using Raspberry Pi Pico W:

The Raspberry Pi Pico is a microcontroller board developed by Raspberry Pi Foundation. It is built on a Raspberry Pi RP2040 microcontroller and features a flexible, dual-core ARM Cortex-M0+ processor running at up to 133 MHz. The board has 2MB of onboard Flash memory and 264KB of SRAM, and several digital and analog input/output (I/O) pins to connect to sensors, actuators, and other devices. It also has a USB port for connecting to a computer and programming the board using the Raspberry Pi Pico Integrated Development Environment (IDE). The board is small and lightweight and have a wireless network interface card making it ideal to simulate attacks on IOT devices

We have written main.py and secret.py. We must connect to the local Wi-Fi so the index file(webpage) can be accessed from the network. The secret.py will have the SSID and Password to connect to the available WIFIs. Once we run the main.py, the server will be up and online, and anyone in the network can be connected to our raspberry pi and turn the led on or led off.

Graphical user interface, text, application, email

Description automatically generated

This is the basic index page we built with which we can control the raspberry pi’s onboard led.

### Apache web server:

We created an index.html page and used the Apache web server installed by default in kali Linux. The index file should be pasted in /var/www/ and if you are using ubuntu you must manually install Apache using below commands

Sudo apt-get install apache2

Graphical user interface, text

Description automatically generated

### Apache server running in google cloud systems:

This is the third server we choose and instead of running it in our local system, we ran it in google cloud and gave more ram, system resources etc. to manage the website.

Graphical user interface, text

Description automatically generated

By implementing 3 different web servers with different sets of resources. We want to evaluate the effectiveness of DDOS attacks and what are the mitigation methods for each kind of resource and cost analysis.

## 2. DDOS Attack tools:

We have gone through many tools and written simple scripts to utilize these tools as well to perform DDOS attacks on these websites.

Flood attacks:

A flood attack involves sending a large volume of traffic to a target system using zombies. In this manner, IP traffic increases the network data transfer utilization of the target framework. The flood attack can also be conducted by UDP, ICMP, HTTP, and SIP packets, resulting in UDP flood, ICMP flood, HTTP surge, and SIP surge attacks. The afflicted person is assaulted by continually transmitting UDP (User Datagram Protocol) packages to a predetermined or arbitrary port.

### ICMP flood attack:

A significant amount of ICMP packet requests is issued to the target in this attack. When the sent bundles are larger than 65535 bytes, the victim's host computer becomes unresponsive. The script used to perform this attack is my\_icmp\_flood.sh in our hosted folder. We used the hping3 utility to produce copious amounts of ICMP traffic.

Graphical user interface, text, application

Description automatically generated

### TCP SYNFlood Attack:

TCP SYN flood, also called SYN flood, is a type of Distributed Denial of Service (DDoS) attack ​that uses a part of the normal TCP three-way handshake to use up a server's resources ​and make it unusable. With SYN flood DDoS, the attacker sends TCP connection requests faster than the machine​ being attacked can handle them. This causes the network to become full.​

Text

Description automatically generated

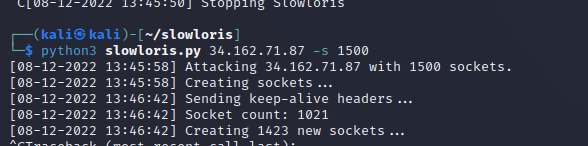
### Slowloris Attack:

Slowloris is a HTTP Denial of Service attack that affects servers that

work with threads. This is how it works: We start asking HTTP for a lot of things.

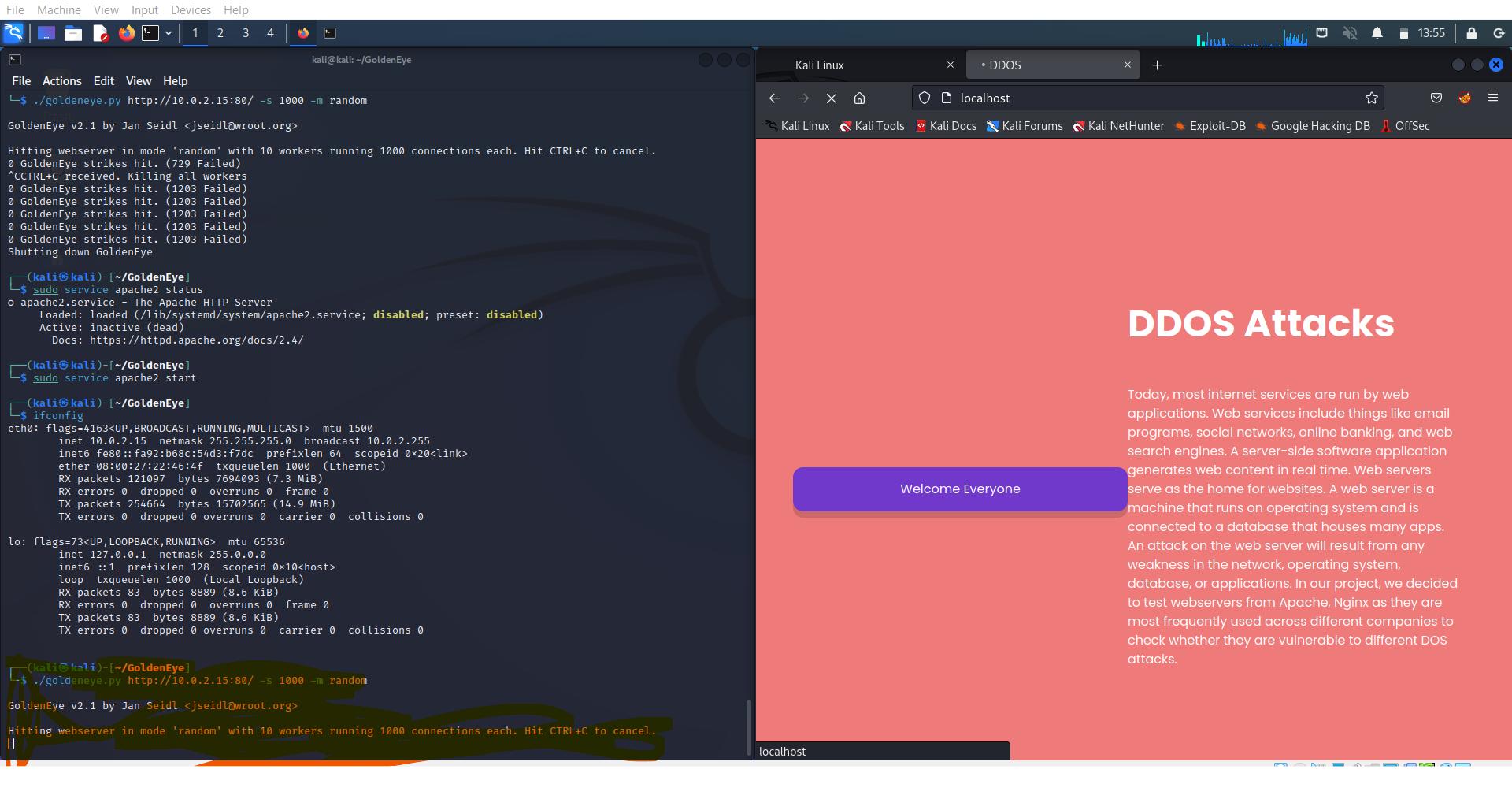
Every 15 seconds or so, we send headers to keep the connections open. We'll never end a connection unless the server tells us to. If the server ends a connection, we make a new one

and keep doing what we were doing before.



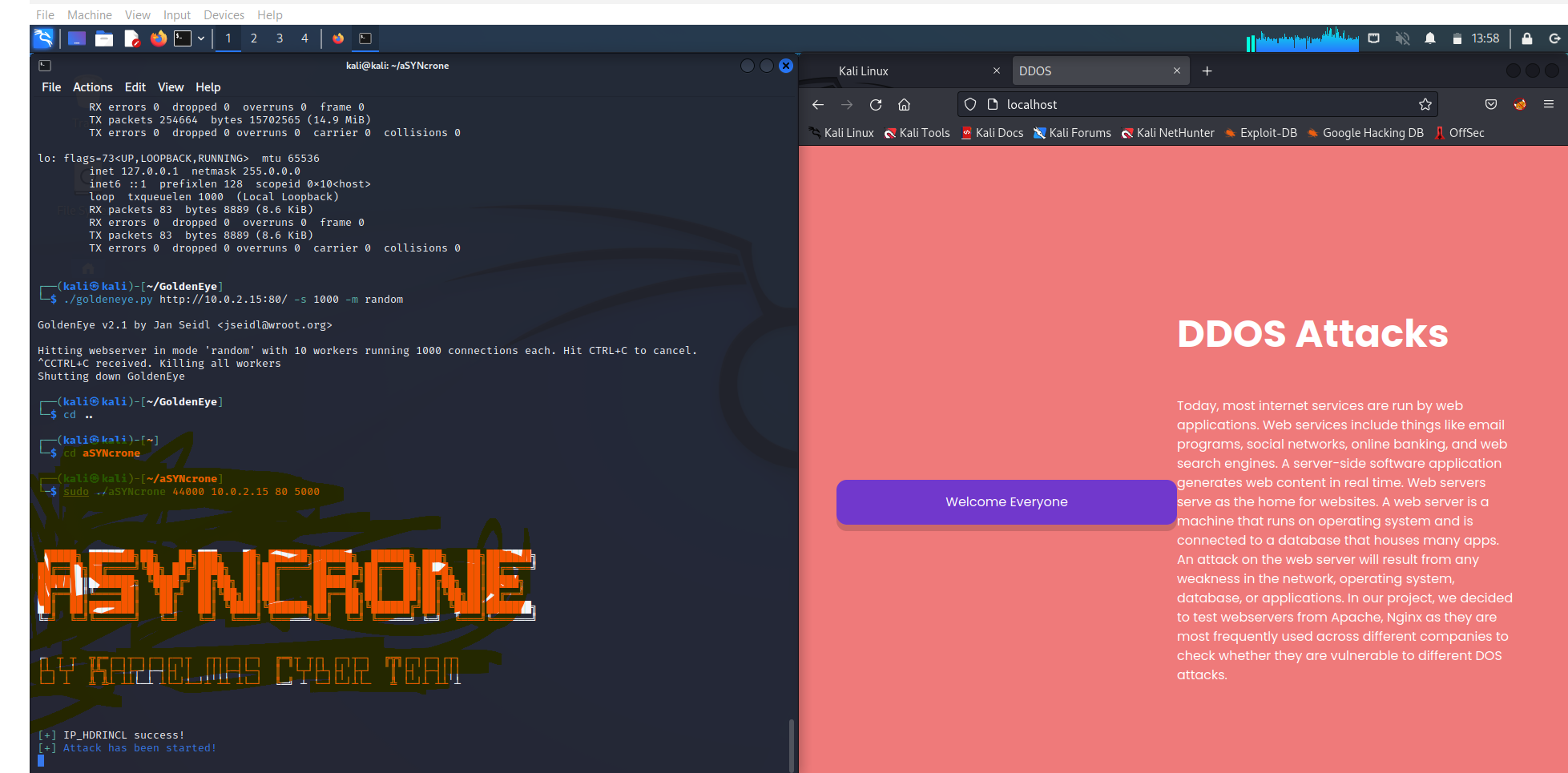
### GoldenEye Attack:

Goldeneye is a free tool that can be found on GitHub. We can use this tool to do a denial-of-service attack. It is a structure made with .NET Core. This tool gives you a lot of base classes and add-ons that you can use in your everyday work. This tool lets a single computer shut down the web server of another computer. It does this by sending HTTP traffic, which is perfectly legal. It sets up a full TCP connection and then only needs a few hundred requests at regular times over an extended period of time. So, the tool doesn't have to send a lot of traffic to use up all of the connections on a server.



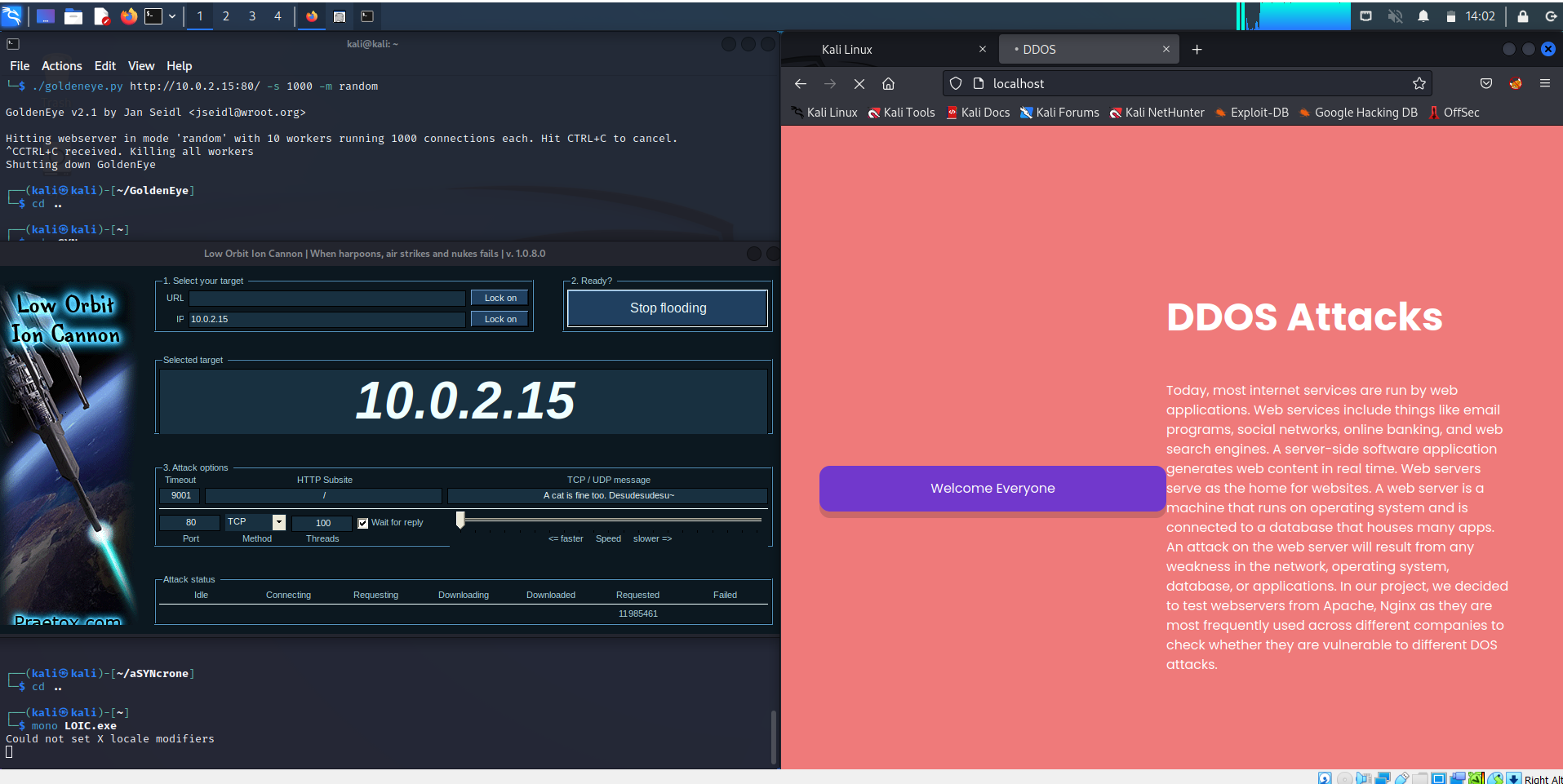
### aSYNncrone:

aSYNchrone is a C language-based, multi-function SYN Flood DDoS Weapon. Disable the destination system by sending an SYN packet intensively to the destination



### LOIC

LOIC (Low Orbit Ion Cannon) is a tool that is used to launch distributed denial-of-service (DDoS) attacks. DDoS attacks involve overwhelming a website or server with a large amount of traffic, to make it unavailable to users. LOIC works by allowing a single computer to generate a large amount of network traffic, which is then sent to the target website or server. This traffic can be generated in a number of ways, such as by sending a large number of requests or by sending data packets that are larger than usual. The goal is to overwhelm the target with so much traffic that it is unable to manage the incoming requests, causing it to become unavailable to users. LOIC was originally developed as a network stress testing tool, but it has been widely used by hackers to launch DDoS attacks. It is often used in combination with a botnet, which is a network of compromised computers that can be used to launch attacks. This allows the attacker to generate even more traffic, making the attack more effective. Using LOIC to launch DDoS attacks is illegal and can result in significant penalties. It is important to protect yourself and your devices from being used in DDoS attacks, by keeping your software and security tools up to date and being careful about the links and attachments you open.



### NTP amplification attack:

An NTP amplification attack is a volumetric distributed denial-of-service (DDoS) attack that uses a Network Time Protocol (NTP) server functionality to overwhelm a targeted network or server with an amplified amount of UDP traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic.

## 3. Protection Techniques from DDoS Attack:

### Get an idea about normal and abnormal traffic:

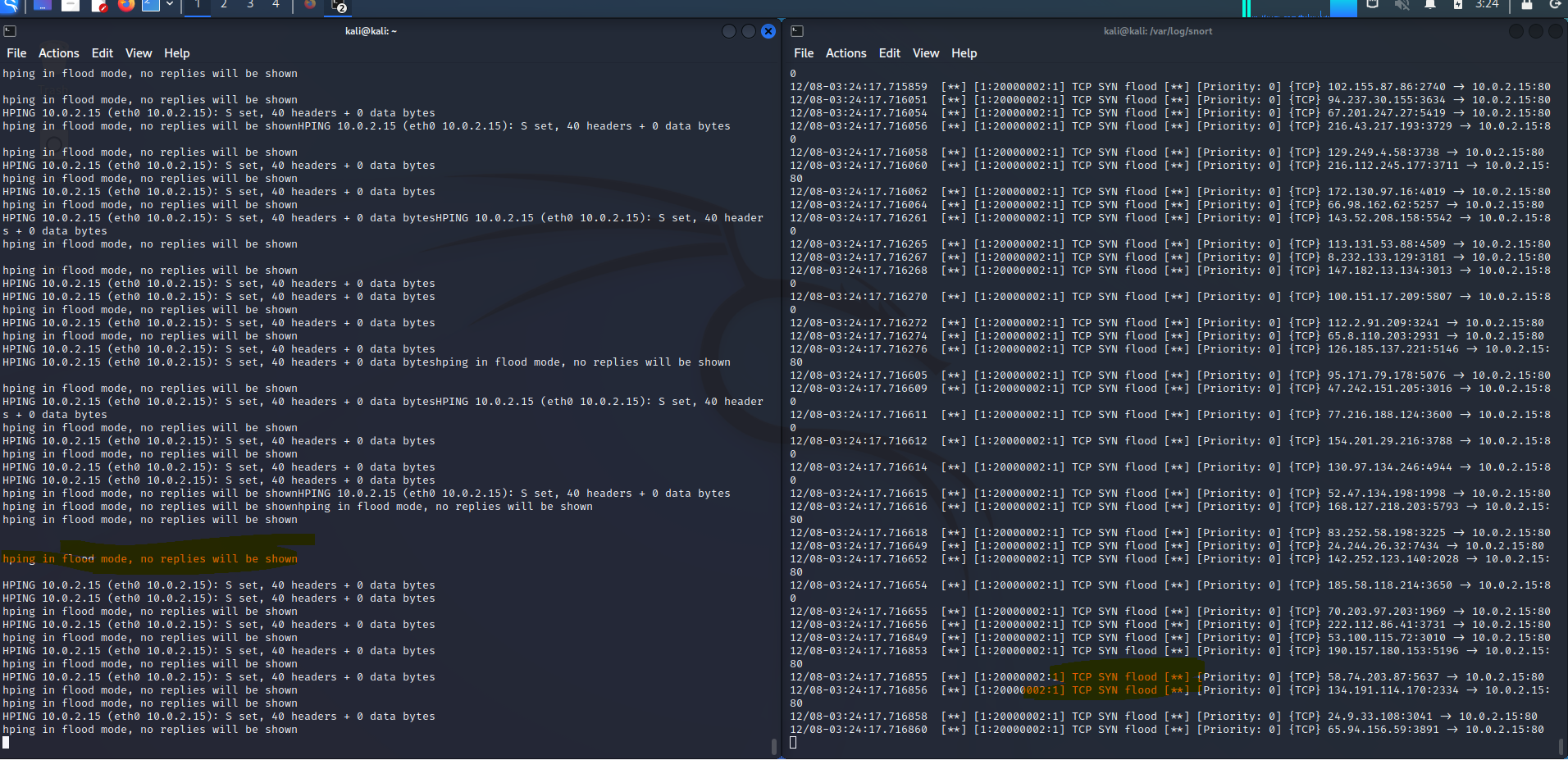
The absolute baseline is to be able to accept only as much traffic as our host can manage without compromising availability if we notice elevated levels of traffic hitting a host. Rate limiting is the name of this idea. By examining each packet individually, more sophisticated protection systems can go one step further and intelligently admit only authorized traffic. To accomplish this, you must be able to compare each packet to a baseline of the qualities of excellent traffic that the target typically receives.

### Reduce surface Area for the Attack:

Reducing attackable surface area to limit attacker options and enable the construction of defenses in a specific location is one of the first methods to reduce DDoS attacks. We must make sure that no ports, protocols, or applications are opened for our application or resources from which they do not anticipate receiving any communication. reducing the potential attack points and enabling us to focus our mitigation efforts.

### SNORT

Snort is a free and open-source network intrusion detection system (IDS) and intrusion prevention system (IPS) developed by Sourcefire. An IDS is a tool that monitors network traffic and alerts administrators when it detects suspicious activity, such as an attempted cyber-attack. An IPS is like an IDS, but it also has the ability to take action to block or stop suspicious activity before it can cause harm. Snort works by analyzing network traffic and comparing it against a set of rules or patterns that are known to be associated with malicious activity. If Snort detects traffic that matches one of these rules, it will generate an alert. This alert can be sent to an administrator, who can then take action to investigate and respond to the threat. Snort is widely used by organizations to protect their networks from a variety of threats, including viruses, worms, and other types of malwares. It can be run on a variety of operating systems, including Linux, Windows, and Mac OS. Snort is highly customizable, allowing administrators to fine-tune its settings and rules to match the specific needs of their network. In addition to its IDS and IPS capabilities, Snort also includes other features that can help administrators protect their networks. These include support for network protocol analysis, real-time alerting, and the ability to perform network-based forensics. These capabilities make Snort a powerful tool for detecting and responding to cyber threats.



As we can see in the screenshot snort was able to detect the flood attack and then we can decide an action course based on snort alerts.

## 4. Conclusion:

We have performed DDOS attacks on 3 web servers each with increasing complexity and better system resources but all of them were vulnerable to DDOS attacks. We were able to install mitigation technique SNORT in Apache servers and were able to detect the attacks, but it comes at a cost as some system resources were used to continuously monitor incoming traffic. But we could not mitigate those attacks in simple microcontrollers like Raspberry Pie. These are chips used in lots of IOT devices in our homes and they all are vulnerable to DDOS attacks and to mitigate them is a colossal challenge as cost of mitigation techniques is greater.

## 5. References:

[1] [What Is a DDoS Attack and How Does It Work | Cybersecurity | CompTIA](https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works)

[2] [Sci-Hub | Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud. IEEE Access, 8, 181916–181929 | 10.1109/ACCESS.2020.3028690](https://sci-hub.se/10.1109/ACCESS.2020.3028690#:~:text=Bhardwaj%2C%20A.%2C%20Mangat%2C%20V.%2C%20%26%20Vig%2C%20R.%20%282020%29.,Attacks%20in%20Cloud.%20IEEE%20Access%2C%208%2C%20181916%E2%80%93181929.%20doi%3A10.1109%2Faccess.2020.3028690)

[gkbrk/slowloris: Low bandwidth DoS tool. Slowloris rewrite in Python. (github.com)](https://github.com/gkbrk/slowloris)

[NewEraCracker/LOIC: Low Orbit Ion Cannon - An open source network stress tool, written in C#. Based on Praetox's LOIC project. USE ON YOUR OWN RISK. WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES. (github.com)](https://github.com/NewEraCracker/LOIC)

[asynchrone (github.com)](https://github.com/asynchrone/)

[hping3 | Kali Linux Tools](https://www.kali.org/tools/hping3/)

[Hosting a simple web server with Google Cloud – Happy Snail Programming](https://happysnailprogramming.com/2020/12/22/hosting-a-simple-web-server-with-google-cloud/)

[Raspberry Pi Documentation - Configuration](https://www.raspberrypi.com/documentation/computers/configuration.html#configuring-networking)

[Configuring An Apache Server In Linux – Systran Box](https://www.systranbox.com/configuring-an-apache-server-in-linux/)

## 6. Project Link:

[DHARAN656/ANS-DDOSattacks (github.com)](https://github.com/DHARAN656/ANS-DDOSattacks)