****

**Bilkent University**

**CS 479**

# **Introduction to Cyber Security**

**Term Project**

***DDoS Attack Tool***

**Mert Özerdem**

# **1 Introduction**

In this project we have developed a DDoS Attack Tool. Our DDoS attack Tool can perform the following attacks:

* Ping of Death
* SNMP Amplification
* UDP Flood
* HTTP Flood
* Slowloris
* ICMP Smurf Attack.

In order to do this project we have used some open source tools for each of the attacks. Below we will explain the attacks we are performing in more detail.

# **2 Types of Attacks Performed**

In this section we will write about the attacks and the tools we have chosen to use for them.

## **2.1 Ping of Death**

Our tool can perform Ping of Death DDoS attack. Ping of Death manipulates IP protocols by sending malicious pings to a system. In this case, a malformed ping packet flood is sent to the target. Since the TCP stack responds only to a certain type of ping packet, it fails to respond to this, exhausting the system resources.

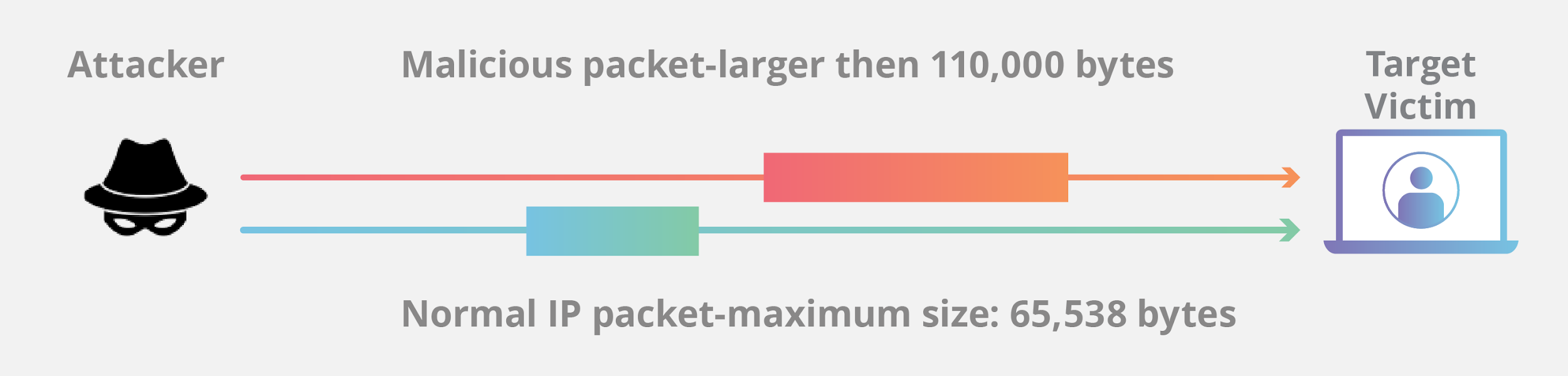


Figure 1. Ping of Death Attack Illustration

To perform this attack we have used Ping of Death open source library. Below there are some screenshots of Ping of Death attack done by our application.

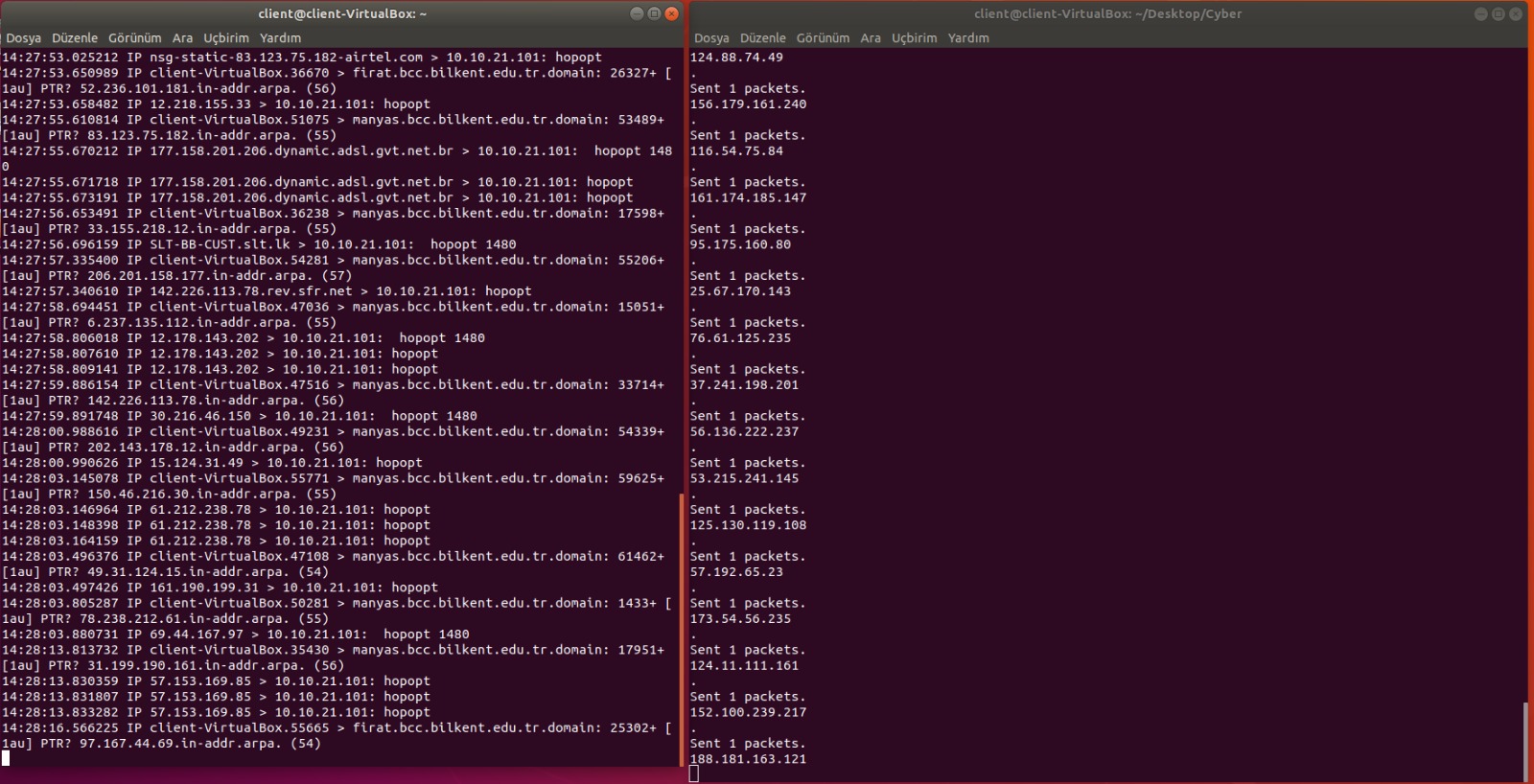


Figure 2. Ping of Death Attack in Action

## **2.2 SNMP Amplification**

Our tool can perform SNMP Amplification DDoS attack. SNMP stands for Simple Network Management Protocol. In the typical form of this attack, an attacker uses a bot network comprised of many hosts to send an SNMP “GetBulkRequest” query (although any other SNMP queries could also be used, including a simple “Get”). As seen below, this query generates a very powerful attack because the size of the response to the query is much larger than the query itself. The SNMP query is sent to a large number of reachable devices with the default community string of public (or another well known community string). When sending this query the attacker spoofs the IP address of the query source, setting the source as the IP address of the intended victim.

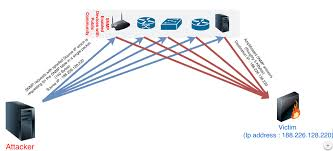


Figure 3. SNMP Amplification Attack Illustration

To perform this attack we have used SNMP Amplification open source library.

## **2.3 UDP Flood**

Our tool can perform UDP Flood DDoS attack. The User Datagram Protocol (UDP) is a sessionless networking protocol. A UDP flood targets random ports on a computer or network with UDP packets. The host checks for the application listening at those ports, but no application is found.

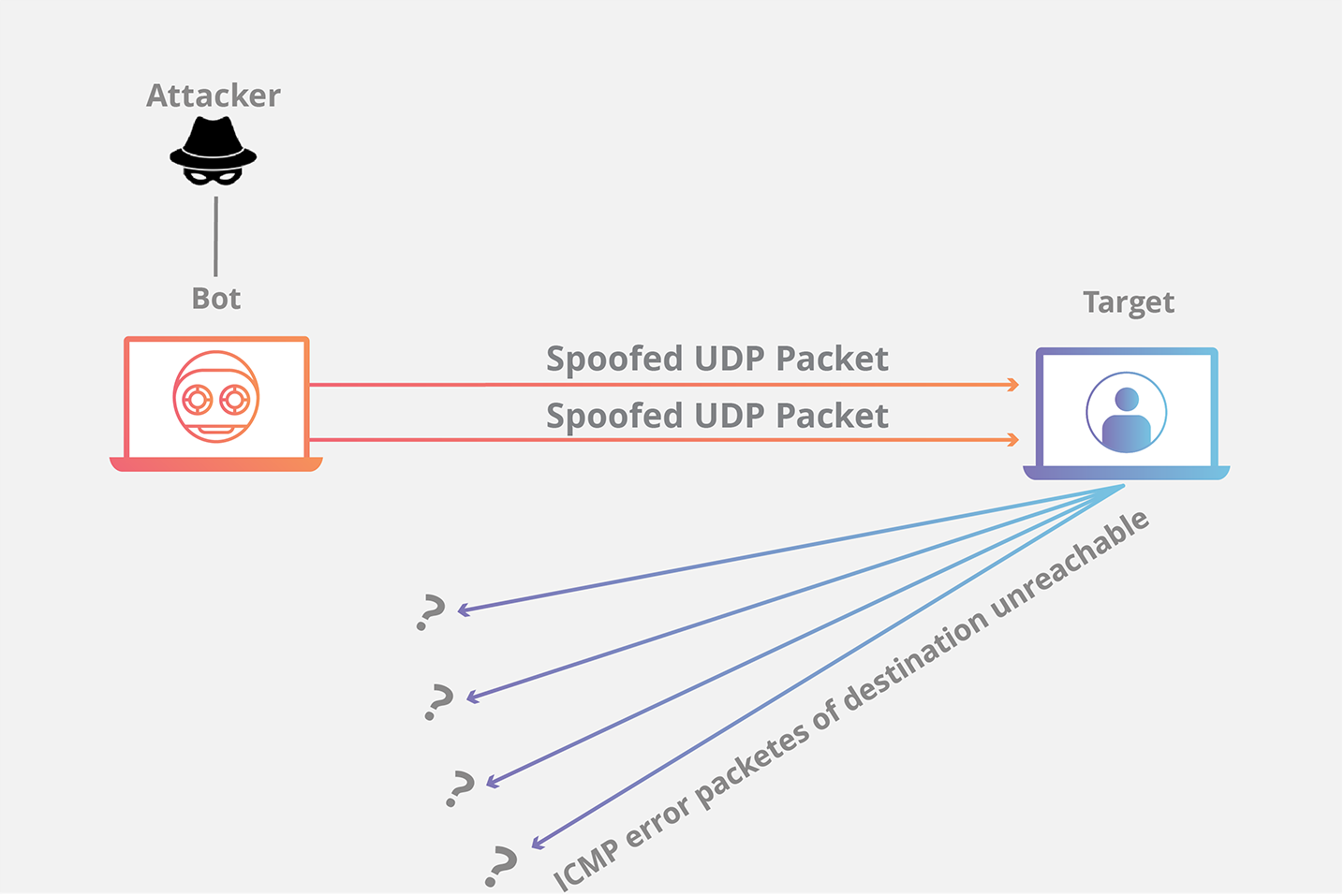


Figure 4. UDP Flood Attack Illustration

To perform this attack we have used UDP open source library. Below there are some screenshots of UDP Flood attack done by our application.

# 

Figure 5. UDP Flood Attack in Action

## **2.4 HTTP Flood**

Our tool can perform HTTP Flood DDoS attack. In an HTTP flood DDoS attack, the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to every single request.

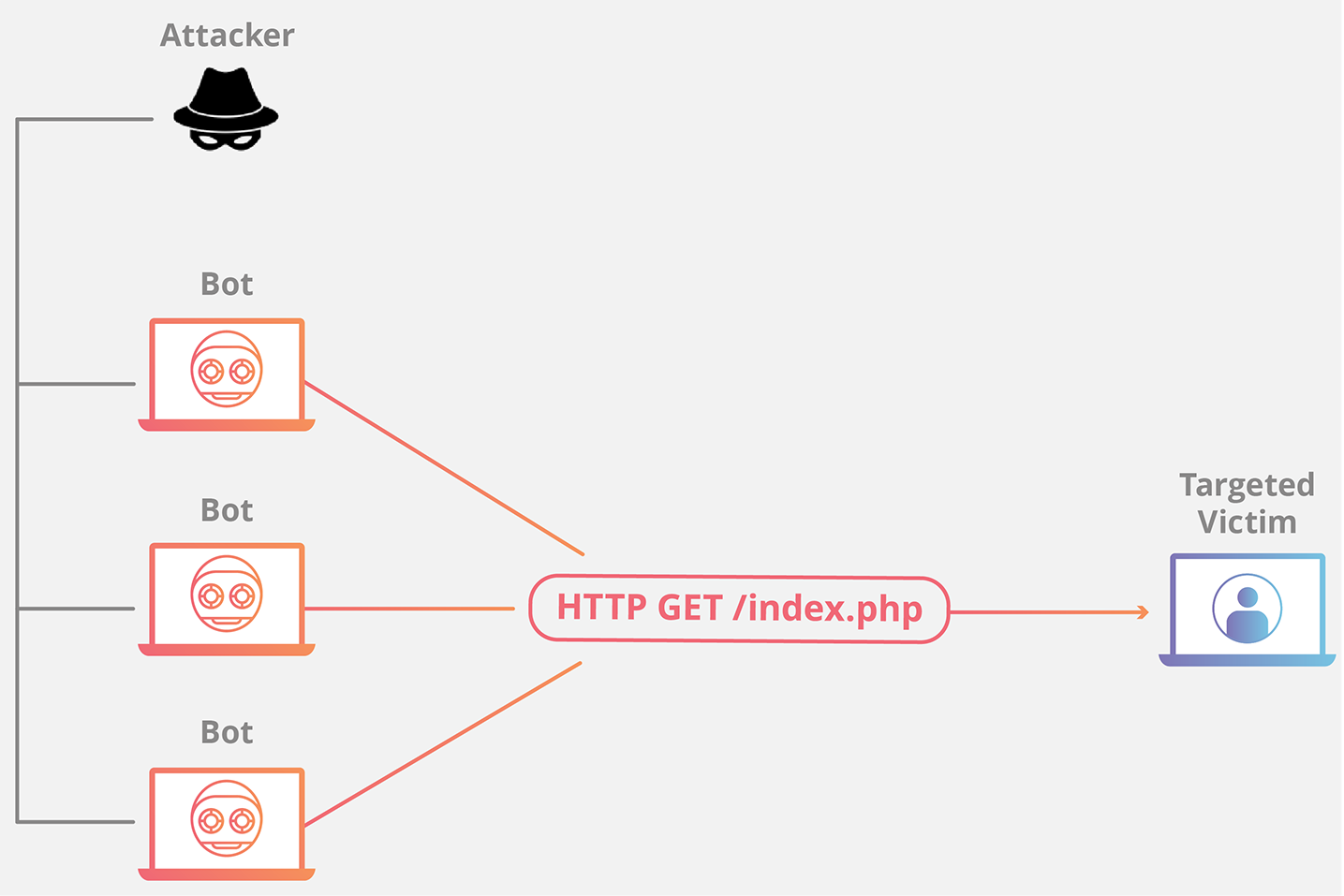


Figure 6. HTTP Flood Attack Illustration

To perform this attack we have used HULK open source tool. Below there are some screenshots of HTTP Flood attack done by our application.

# 

Figure 7. HTTP Flood Attack in Action

## **2.5 Slowloris**

Our tool can perform Slowloris DDoS attack. Denial of service usually relies on a flood of data. Slow Loris takes a more elegant approach, and almost bores a server to death.

Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, waiting for each of the attack requests to be completed.

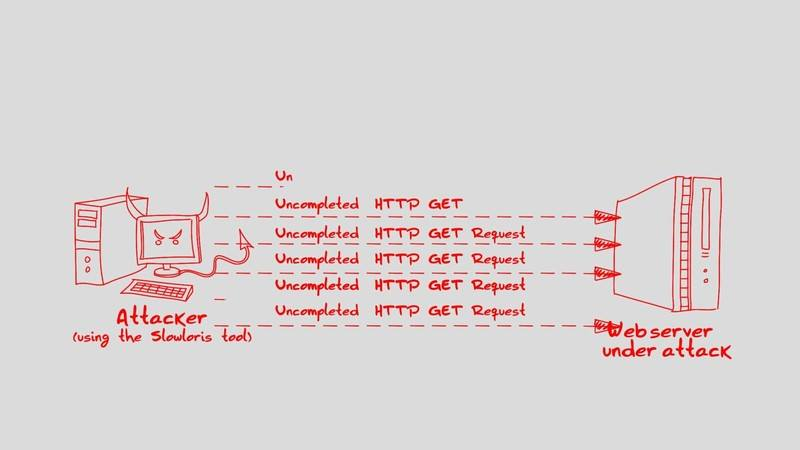


Figure 8. Slowloris Attack Illustration

Periodically, the Slowloris sends subsequent HTTP headers for each request, but never actually completes the request. Ultimately, the targeted server’s maximum concurrent connection pool is filled, and additional (legitimate) connection attempts are denied.

perl slowloris.pl -dns (Victim URL or IP).

Below there is the command and the screenshot of SlowLoris Attack.

perl slowloris.pl -dns (Victim URL or IP)

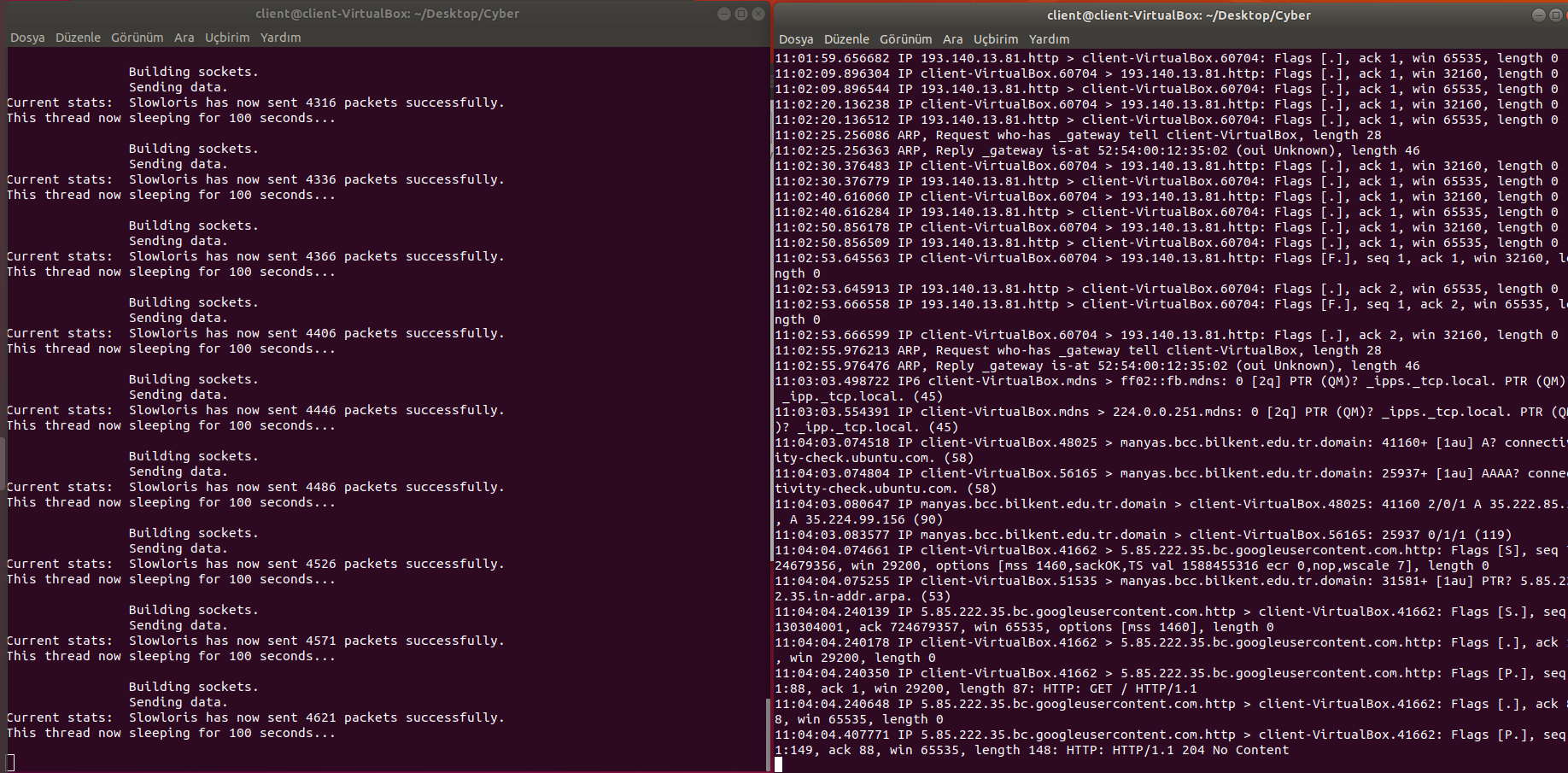


Figure 9. Slowloris Attack in Action

## **2.6 ICMP Smurf Attack**

Our tool can perform ICMP Smurf Attack DDoS attack.The Smurf attack is a DDOS in which large numbers of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

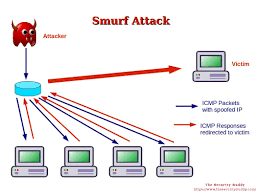


Figure 10. ICMP Smurf Attack Illustration

Below there is the command and a screenshot of our ICMP Smurf Attack.

sudo hping3 --icmp --spoof Target\_IP BroadCast\_IP

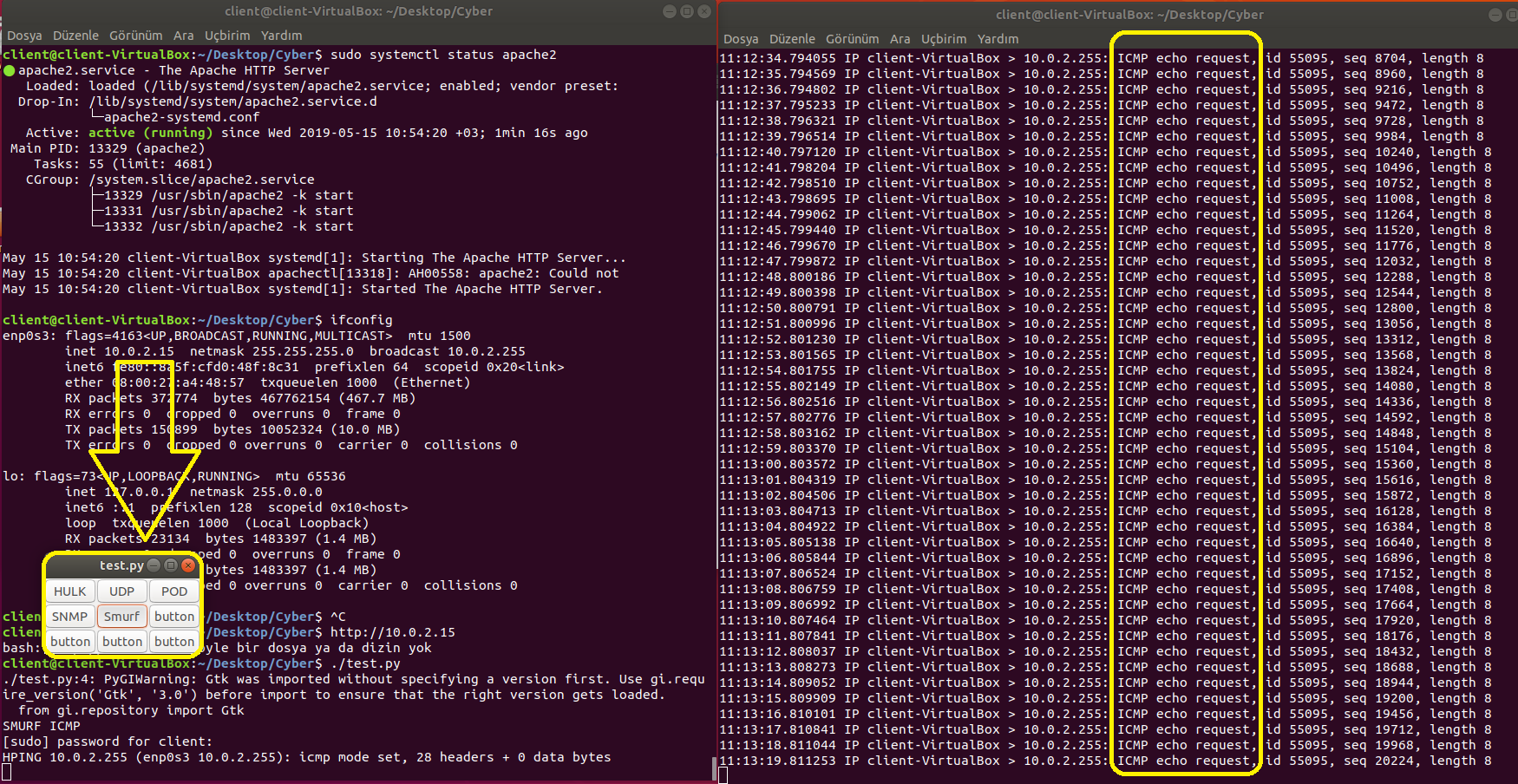


Figure 11. ICMP Smurf Attack in Action

In here we see that a click of a button we can perform ICMP smurf attack as you see from the right terminals network ICMP requests is flooded.

# **3. Similar Tools**

Below there are some similar tools.

## **3.1 DAVOSET**

DAVOSET is yet another nice tool for performing DDOS attacks. The latest version of the tool has added support for cookies along with many other features. You can download DAVOSET for free from Packetstormsecurity.

## **3.2 OWASP DOS HTTP POST**

It is another nice tool to perform DOS attacks. You can use this tool to check whether your web server is able to defend DOS attack or not. Not only for defense, it can also be used to perform DOS attacks against a website.

## **3.3 PyLoris**

PyLoris is said to be a testing tool for servers. It can be used to perform DOS attacks on a service. This tool can utilize SOCKS proxies and SSL connections to perform a DOS attack on a server. It can target various protocols, including HTTP, FTP, SMTP, IMAP, and Telnet. The latest version of the tool comes with a simple and easy-to-use GUI. Unlike other traditional DOS attacking tools, this tool directly hits the service.

## **3.4 Tor’s Hammer**

Tor’s Hammer is another nice DOS testing tool. It is a slow post tool written in Python. This tool has an extra advantage: It can be run through a TOR network to be anonymous while performing the attack. It is an effective tool that can kill Apache or IIS servers in few seconds.

## **3.5 R-U-Dead-Yet**

R-U-Dead-Yet is a HTTP post DOS attack tool. For short, it is also known as RUDY. It performs a DOS attack with a long form field submission via the POST method. This tool comes with an interactive console menu. It detects forms on a given URL and lets users select which forms and fields should be used for a POST-based DOS attack.

## **3.6 XOIC**

XOIC is another nice DOS attacking tool. It performs a DOS attack an any server with an IP address, a user-selected port, and a user-selected protocol. Developers of XOIC claim that XOIC is more powerful than LOIC in many ways. Like LOIC, it comes with an easy-to-use GUI, so a beginner can easily use this tool to perform attacks on other websites or servers.

## **3.7 LOIC**

LOIC is one of the most popular DOS attacking tools freely available on the Internet. This tool was used by the popular hackers group Anonymous against many big companies’ networks last year. Anonymous has not only used the tool, but also requested Internet users to join their DDOS attack via IRC.