International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 09 Issue 12 ǁ 2021 ǁ PP. 53-58

Server Stress Test Using DDoS Attack

Nishit Shah [#1] , Shravan S [#2]
School of Computer Science and Engineering
Vellore Institute of Technology, Tamil Nadu, India
**School of Computer Science and Engineering*
Vellore Institute of Technology, Tamil Nadu, India

Abstract: *In the present generation, attacks on the web servers and application is the most common form of attacks that are carried out nowadays. The main reason being is most of the web application or services are vulnerable to attacks and can be easily compromised. One of the most popular attacks used is Distributed Denial of Services (DDoS).Most recent websites and web servers are unable to withstand strong attacks like DDoS attack since they lack protection against simple attacks are easily compromised. But we can use this type of attack in penetration testing to test the server stress and help to improve the security on the basis of the level of the withstanding of the website under such type of attacks. The aim of this paper is to test different web application against the DDoS attacks and to also to determine the level to which the servers can protect themselves against malicious attacks.*

Keywords : *Slowloris, Wireshark, DDoS attack, web server, Random Forest Classifer*

Date of Submission: 20-11-2021 Date of acceptance: 05-12-2021

I. Introduction

Stress testing is the process of determining the ability of a network, network, program or device to maintain a certain level of effectiveness under unfavorable conditions. The process can involve quantitative tests done in a lab, such as measuring the frequency of errors of system crashes. The goal of Stress testing is measuring software on its robustness and error handling capabilities under extremely heavy load conditions and ensuring that software doesn't crash under crunch situations. It even tests beyond normal operating points and evaluates how software works under extreme conditions. The main purpose of Stress testing is to accommodate an abnormal traffic spikes and failure to accommodate this sudden traffic may result in loss of revenue and repute. It also displays appropriate error message when the system is under stress. Stress testing your website for DDoS scenarios will give you enough information for you to be on your safety. Considering testing your website for DDoS protection using stress testing solution would have lots of benefits such as: 1.Identify and resolve website infrastructure issues and bottlenecks before the DDoS attacks. 2. Planning for an incident response procedure. 3. Find out the breaking point for your website under overload conditions and optimize for robustness. 4. Devising DDoS mitigation and prevention strategies.5. Scaling and securing IT assets for more resilience.

II. Problem Statement

DDoS attack is one of the most common attacks and it is tough to flag the ill-intended traffic from normal traffic. However, there are ways to counter and defend your website against DDoS attacks. DDoS attack can target any component of your network and IT infrastructure. Attackers look for the opportunity to exploit any vulnerabilities in different layers of your network. Below are among many common DDoS attacks that we see very often:

- **Application Layer Attacks:**

These attacks target your network's application layer by sending HTTP traffic load with malicious intent. When an HTTP request comes to the server, to send a response, the server performs multiple tasks such as load files, querying the database, computing the request, preparing the response etc. With such a huge amount of traffic, their server gets overloaded, and exhausts infrastructure resources and ultimately goes down. Since it is hard to classify these requests as malicious requests due to their nature being similar to actual users, the application layer DDoS attacks are hard to prevent.

- **Protocol Attacks**

These attacks bring down the service by exhausting intermediate resources like state table capacity, load balancers, firewalls, TCP handshakes etc. For example, attackers can send a TCP handshake request for

connection initialization, the server sends back the response and waits for confirmation from the client. But the client never sends the confirmation, and the server keeps wanting for it, causing the server resources to exhaust. These attacks are called state-exhaustion attacks.

III. Literature Review

[1]In this paper, they mentioned that HTTP flood attacks strategy is to exhausts the resources of the victim server by sending massive malicious requests packets such as HTP-GET and HTTP-POST requests.The performance analysis of Apache2 on Ubuntu 160.4 LTS server and IIS10.0 on Windows server 2016 and is performed without and with DDoS attacks. The web server's performance without attacks was as follows: Apache2 responded to the client's requests faster by 2 ms only. Moreover, the standard deviation value of IIS10.0 was fewer in all tests except the last test; hence it was more stable compared to Apache2 web server. Furthermore, the first web server achieved more stable performance. Thirdly, the performance of the web servers is analyzed with SYN flood attack. Overall, the IIS10.0 web server was more stable, efficiency and also much responsiveness during HTTP flood attack. The limitation was to improve the efficiency further.

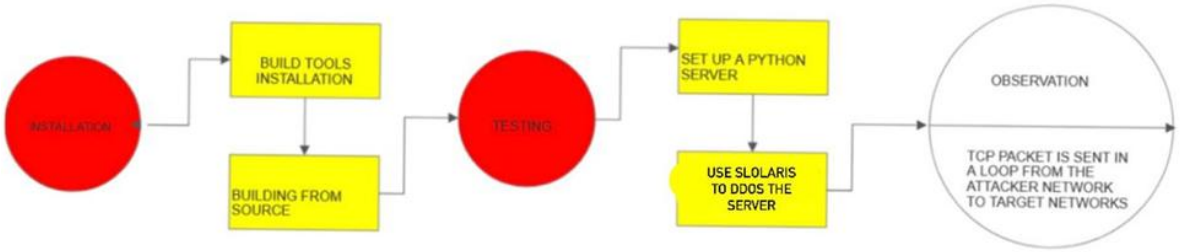
[2]In this paper, the principle point of the DDoS assault is to coordinate the gigantic pernicious traffic from different PCs to casualty worker and organization to flood it. Ansible climate was utilized as a premise to create and convey a DDoS testbed and the testbed was tried for logical analyses and study purposes. Performing and organizing of the assault is upheld by organization as the principle element of the open source Ansible. Proposed climate requires no unique equipment; anyway it upholds properties like simple establishment and the executive's adaptability, circulated climate just as framework execution. Future work lays in including IoT gadgets into mechanized occupation handling to perform IoT DDoS assaults.

[3] In this paper, the proposed situation was carried out during the 1Gbps genuine organization. Likewise, the framework was introduced and designed on the most extreme present day working frameworks. The depended web workers were ready on the NLB Cluster-based web workers in Windows and Linux stages. The investigating was performed with and without the SYN flood DDoS assault in six trial of HTTP demands. The examination basically dependent on the responsiveness, proficiency and steadiness, additionally the normal CPU use and throughput are estimated as measurements of the assessment cycle with a weighty burden. In Cluster-based development without assault, the test results showed that IIS 10.0 is more responsiveness contrasted with the Apache 2 web worker. The normal CPU utilization on Apache 2 web worker is more prominent than that of the IIS 10.0. Likewise, IIS 10.0 has better standard deviation esteem; along these lines, IIS 10.0 is steadier. The throughput of IIS 10.0 bunch based webservers is a lot more prominent than that of Apache 2 web workers. The exploratory outcomes showed that the SYN DDoS assault sway was more on the presentation of Apache 2 web workers. Where, the normal reaction time, standard deviation and mistake rates drastically expanded. Likewise, the throughput of Apache 2 group based web workers diminished during the assault. Subsequently, the IIS10.0 is more responsiveness, stable and has better effectiveness during the assault. Notwithstanding, the normal CPU use of the Apache 2 bunched web workers didn't influence by the SYN assault.

[4]In this paper, they studied on the several DDoS attack categories and families to propose a new DDoS taxonomy for the application layer. Also, they have reviewed the most popular available DDoS datasets and listed the common shortcomings and weaknesses. Also, they provided the most important features for detecting different DDoS attacks. Furthermore, based on the 12 RadViz diagrams of the most influential features for each type of network traffic they provide a detailed analysis for each of them. The limitation inferred was as time passes by the shortcomings and weaknesses vary.

[5]In this paper they proposed that distributed denial of service attacks are prominent cyber-attacks for the last many years. Cloud computing environments are emerging as a common service deployment alternative. At the same time, the cloud is also emerging as an important target for DDoS attacks. Cloud platforms may also use the container as a service (CaaS) deployment model. Among these requirements, serving the benign user requests is the foremost requirement for any victim server. Based on these solutions requirements, they propose a set of novel page separation and resource allocation strategies to achieve service availability for genuine users. The limitation was future work will focus on more effective scheduling algorithms in which turnaround time and response time will be improved.

IV. Block Diagrams



V. Tools Used

Slowloris

For our project we will be using Slowloris tool. Slowloris is a denial of service attack program which allows an attacker to overwhelm a targeted server by opening and maintaining many simultaneous HTTP connections between the attacker and the target. It is an application layer attack which operates by utilizing partial HTTP requests. The attack functions by opening connections to a targeted Web server and then keeping those connections open as long as it can.

The Slowloris attack happens in 4 steps:

- The attacker first opens multiple connections to the targeted server by sending multiple partial HTTP request headers.
- The target opens a thread for each incoming request, with the intent of closing the thread once the connection is completed. In order to be efficient, if a connection takes too long, the server will timeout the exceedingly long connection, freeing the thread up for the next request.
- To prevent the target from timing out the connection, the attacker periodically sends partial request header to the target in order to keep the request alive.
- The targeted server is never able to release any of the open partial connections while waiting for the termination of the request. Once all available threads are in use, the server will be unable to respond to additional request made from regular traffic, resulting in denial of service.

Parrot OS

Parrot Linux is a free and open-source operating system used mainly by security professionals. Just like Linux, this is a Debian-based GNU/Linux distribution intended for the Kali Linux alternative. When we say Debian-based, it means the code libraries developed follow Debian based development. It is a complete guide for protection and security operations, but it also includes everything we need to build our programs or defend our network privacy while surfing the internet. That is probably the reason it is considered as one of the best penetration testing OS.

Parrot OS is an Ubuntu desktop version. The finish is more clean and matte. It is divided into two parts, top, and bottom. The part none the top has information such as Programs, Device, Locations, etc. which is a lot similar to Kali Linux. It along with a use graph also provides some cool details about CPU temperature .Parrot OS has a variety of multimedia support options. Besides, just like Kali Linux it also has updates for IoT applications that have cloud connectivity and support.

ADVANTAGES

- Free: We can view the source code and customize it according to our requirements. It is free and open-source.
- Lightweight: This operating system has proved to be incredibly light and runs exceptionally quickly, even on very old ones.
- Secure: It is all revised, published regularly, and protected. It's all under our complete control.

Parrot OS Requirements

- Graphical acceleration is not needed
- A minimum of 16 GB of space is needed for installation on the hard disk
- A minimum of 320MB of RAM is appropriate.
- A minimum dual-core Processor of 1 GHz is required

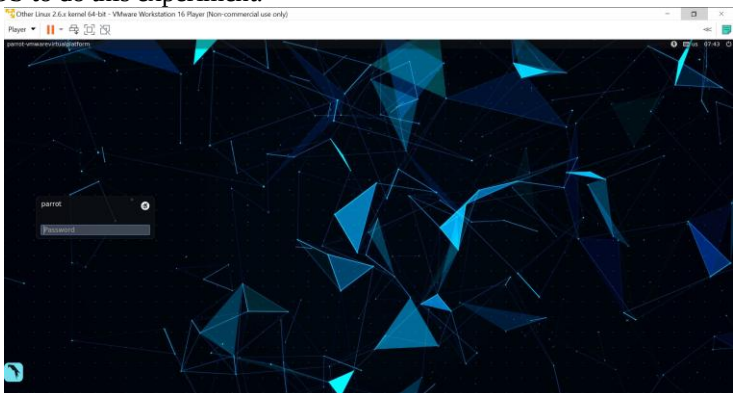
Wire Shark

Using Wireshark captures network traffic on the local network and stores that data for offline analysis. It displays the fields, along with their meanings as specified by different networking protocols. It uses pcap to capture packets so it can only capture packets on the types of networks that pcap supports.

VI. Our Methodology

Step 1: Start VMware to operate Parrot OS

We have used Parrot OS to do this experiment.

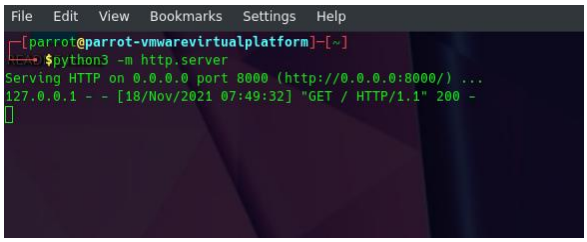


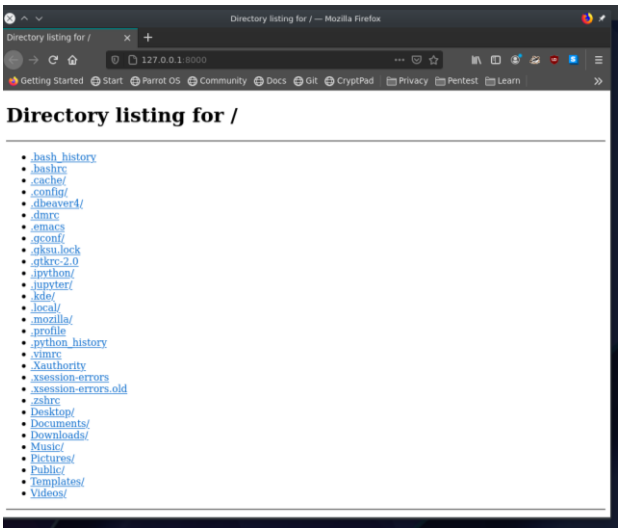
Step 2: Start the web server in the command prompt (Konsole)

To begin the web server, we open the Parrot OS command prompt which is called Konsole. In the terminal we enter the following command to do so.

python3 –m http.server

After giving this command, we open the web browser and go to ***127.0.0.1:8000.*** The directory list will appear indicating that everything is working normal





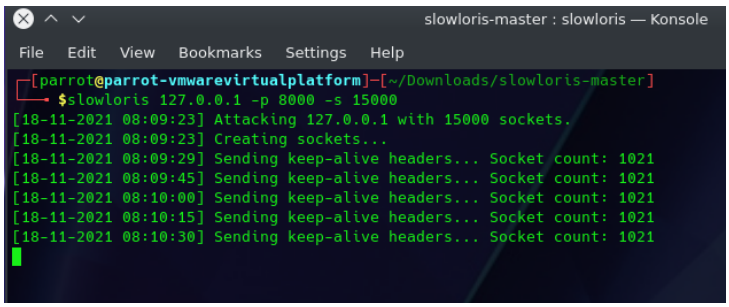
Step 3: Attack the server using slowloris

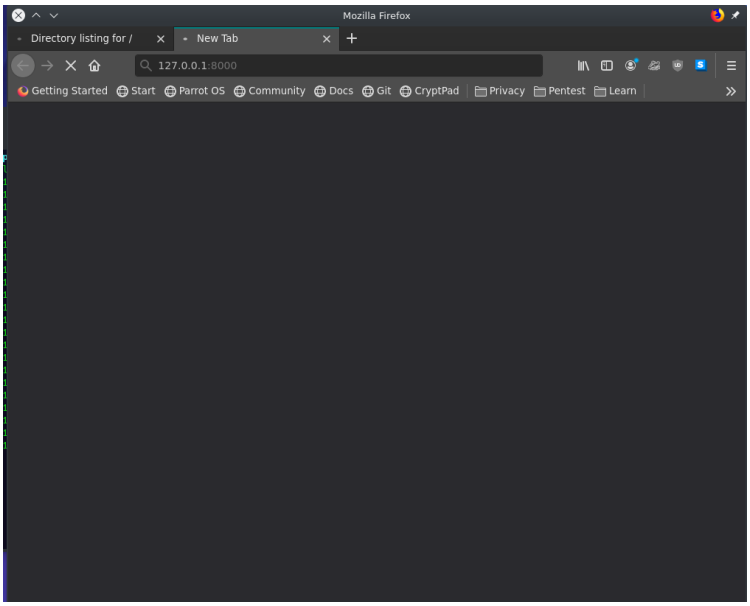
Using slowloris tool, we will attack the 127.0.0.1:8000 server. For that we will enter the folder which contains slowloris.py file. This is the python code which can do DDoS attack.

After that, we give the following command to perform the attack

Slowloris 127.0.0.1 –p 8000 –s 15000

-p indicates port number, in this case it's 8000 and –s indicates number of sockets. We have created 15000 sockets.

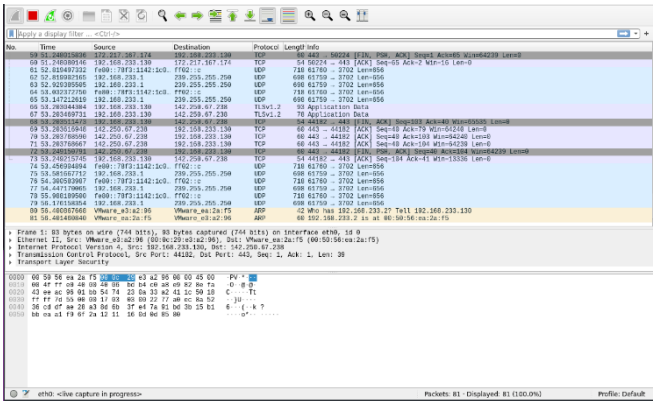




We can see that the server which we attacked is not loading. This is because extremely high number of requets that is being sent to the server.

Step 4 : Use Wireshark to capture the packets

We will use wireshark to capture the packets that is being sent to the server



Step 5: Load the csv data into Machine Learning Model

For predicting the attacks, we use Random Forest Classifier. This algorithm is a classifer that contains decision trees on various subsets of the given datset and takes to improve the predictive accuracy of the datset.

```
In [7]: import numpy as np
        import matplotlib.pyplot as plt
        import pandas as pd

In [8]: datasets = pd.read_csv('DDoSdata.csv')
        dataset2 = datasets.copy()
        dataset2 = datasets.drop(['flgs'],axis=1)
        X = dataset2.iloc[:, [2,3]].values
        Y = datasets.iloc[:, 4].values
```

Step 6: Retrieve the accuracy score

In the end of Random Forest Classifier model, we get the confusion matrix and accuracy score

```
In [15]: from sklearn.metrics import confusion_matrix, accuracy_score
         cm = confusion_matrix(Y_Test, Y_Pred)
         print(cm)
         accuracy_score(Y_Test, Y_Pred)

         [[282239      0      0      0      0      0      0]
          [     0 194751      0      0      0      0      0]
          [     0      0      3      0      0      0      0]
          [     0      0      1    210      0      0      0]
          [     0      0      0      0   4505      0      0]
          [     0      0      0      0      0     66      0]
          [     0      0      0      0      0      0      1]]

Out[15]: 0.9999979243465843
```

VII. Result

After using python sklearn for Random Forest Classifier, we see that these predictions are 99% accurate. The training set is fit on our model and then predictions are made or test set. We got a high prediction because the dataset has enough entries to make an accurate prediction.

VIII. Conclusion

Slowloris tool has been proven to be one of the most powerful tool for Distributed Denial of Service attack (DDoS attack). This is because slowloris creates many HTTP requests and attacks the web sever periodically. DDoS is favourable for the trespasser who wish for the valid user to cooperate with the safety measures of its essential and sensitive information. Once the system gets attacked by DDoS it might not be found easily and its prevention is also not the easiest one. The only way to get relieved from this is to determine whether any injuries are caused by it and to take action to recover from it.

Also ot predict if Slowloris tool would impact a website and to what extent does it impact the system, Random Forest Classifer is the best as it gives 99% accuracy on our test data and precisly tells us the impact Slowloris has based on data observed by Wireshark.

References

[1]. R.R Zebari,S.R.M Zeebaree,K. Jacksi, "Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers" 2018

[2]. L.Huraj, A.Marek "Realtime attack environment for DDoS experimentation" 2019

[3]. S.R. M. Zeebaree ,R.Zebari, K.Jacksi "Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers " 2020

[4]. I.Sharafaldin, A.H.Lashkari, S.Hakak, A.A.Ghorbani "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy" 2019

[5]. A.Patidar, G.Somani "Serving while attacked: DDoS attack effect minimization using page separation and container allocation strategy" 2021