SQL Injection with Kali Linux

A PROJECT REPORT

Submitted by

Meenakshi Gayathri [RA2111029010009]
Gayathri R[Reg No: RA2111029010033]
Mrinalini Vettri [Reg No: RA2111029010054]

Under the Guidance of

Dr. Sowmiya. B

Assistant Professor, Department of Computing Technologies *in*

partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTING TECHNOLOGIES

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR– 603 203

NOV 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR–603 203

BONAFIDE CERTIFICATE

Certified that 18CSE412J (Offensive Security) project report titled "**SQL Injection with Kali Linux**" is the bonafide work of **Meenakshi Gayathri [RA2111029010009] Gayathri R[Reg No: RA2111029010033]** and **Mrinalini Vettri [Reg No: RA2111029010054]**who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported here in does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate.

SIGNATURE

Dr. Sowmiya. B
Assistant Professor
Department of Computing Technologies
Institute of Science and Technology

SIGNATURE

Dr. M. PUSHPALATHA
HEAD OF THE DEPARTMENT
Department of Computing Technologies
SRM Institute of Science and Technology SRM

SRM Institute of Science and Technology Own Work Declaration Form

Degree/Course : B. Tech in Computer Science and Engineering

Student Names : **Meenakshi Gayathri S , Gayathri R , Mrinalini Vettri**

Registration Number: RA2111029010009 , RA2111029010033 , RA2111029010054

Title of Work :

I/We here by certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism, as listed in the University Website, Regulations, and the Education Committee guidelines.

I / We confirm that all the work contained in this assessment is our own except where indicated, and that we have met the following conditions:

- Clearly references / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web, etc.)
- Given the sources of all pictures, data, etc. that are not my own.
- Not made any use of the report(s) or essay(s) of any other student(s)either past or present
- Acknowledged in appropriate places any help that I have received from others (e.g., fellow students, technicians, statisticians, external sources)
- Compiled with any other plagiarism criteria specified in the Course hand book / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

DECLARATION:
I am aware of and understand the University's policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above. **Student 1 Signature:** **Student 2 Signature:** **Date:**
If you are working in a group, please write your registration numbers and sign with the date for every student in your group.

TABLE OF CONTENTS

S. No.	Title	Page No.
1.	Abstract	1
2.	Introduction	2
3.	Common Denial of Service Attacks	3
4.	Distributed DoS (DDoS)	4
5.	Difference between Denial of Service and Distributed Denial of Service	5
6.	Problems caused by Denial-of-Service Attacks	5
7.	Detecting DoS Attacks	6 - 8
8.	Conclusion	9
9.	References	10

ABSTRACT

This project report delves into the Denial of Service (DoS) attack detection, leveraging open-source tools and network monitoring techniques. In lieu of traditional machine learning models, the approach focuses on real-time analysis of network traffic using tools like Wireshark, coupled with customized scripts for anomaly detection.

The project initiates with a detailed exploration of various DoS attacks and its vectors and the associated patterns within network traffic. Special emphasis is placed on understanding the distinctive characteristics of DoS attacks.

The implementation involves the integration of Wireshark for packet-level analysis and other open-source tools for traffic monitoring. Customized scripts are developed to identify anomalies in network behavior.

Validation of the proposed solution is carried out through extensive testing in a controlled environment, simulating various DoS attack scenarios. The results demonstrate the system's effectiveness in accurately detecting and responding to anomalous network activities, showcasing the practicality and efficiency of the implemented approach.

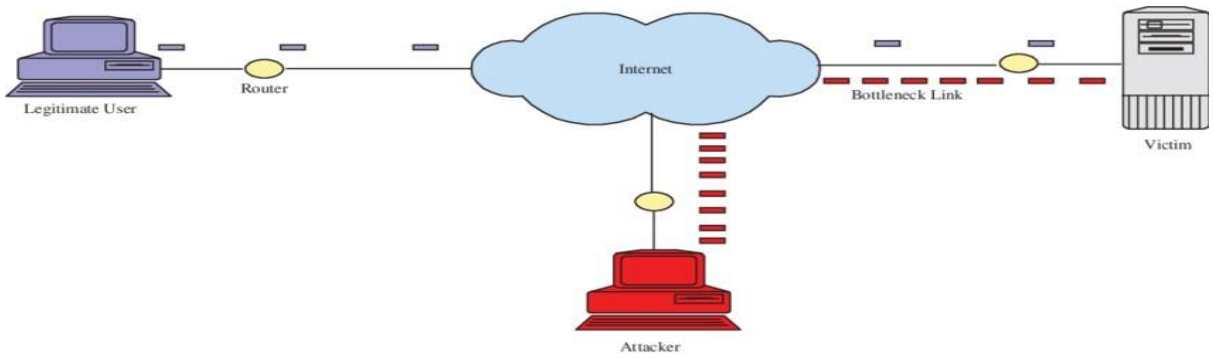
INTRODUCTION

In the interconnected world of today, where our lives are intricately woven into the digital fabric, the threat of cyberattacks looms larger than ever. One particularly disruptive form of cyber threat is the Denial-of-Service (DoS) attack, a malevolent act that renders legitimate users helpless by obstructing access to essential information systems and services.

At its core, a DoS attack disrupts the normal functioning of a computer, network, or service, making it inaccessible to its intended users. The assailant achieves this by overwhelming the targeted host with an excessive amount of traffic, pushing it to the brink until it either cannot respond or succumbs to the sheer volume of data, crashing in the process.

The primary motivation behind a DoS attack can vary, ranging from ideological reasons to sheer malicious intent. Hacktivists may target organizations to voice their grievances or protest certain actions, while cybercriminals may seek financial gain by disrupting online services and demanding ransom payments to restore normalcy.

The repercussions of a DoS attack extend beyond mere inconvenience. Organizations often find themselves grappling with significant downtime, leading to lost productivity and revenue. Moreover, the erosion of user trust and damage to the reputation of the targeted entity can have lasting effects, impacting its standing in the digital landscape.



DoS Attack

Common denial of service attacks

There are many different methods for carrying out a DoS attack. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

- In a **Smurf Attack**, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.

- A **SYN flood** attack occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

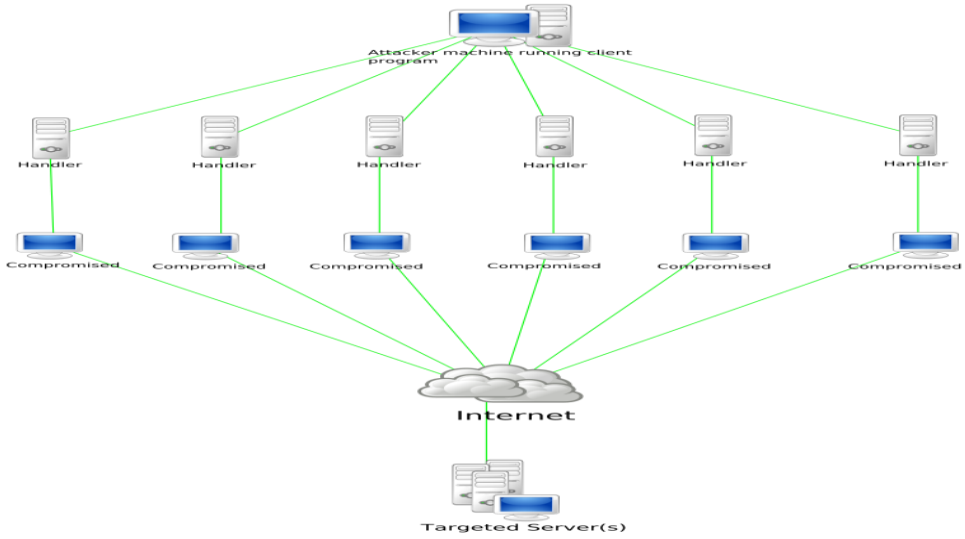
Individual networks may be affected by DoS attacks without being directly targeted. If the network's internet service provider (ISP) or cloud service provider has been targeted and attacked, the network will also experience a loss of service.

Denial-of-service attacks are characterized by an explicit attempt by attackers to prevent legitimate use of a service. There are two general forms of DoS attacks: those that crash services and those that flood services. The most serious attacks are distributed.

Distributed DoS (DDoS)

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. A DDoS attack uses more than one unique IP address or machines, often from thousands of hosts infected with malware. A distributed denial of service attack typically involves more than around 3–5 nodes on different networks; fewer nodes may qualify as a DoS attack but is not a DDoS attack.

Multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and the behaviour of each attack machine can be stealthier, making it harder to track and shut down. Since the incoming traffic flooding the victim originates from different sources, it may be impossible to stop the attack simply by using ingress filtering. It also makes it difficult to distinguish legitimate user traffic from attack traffic when spread across multiple points of origin.



DDoS Attack

Difference between Denial of Service (DoS) and Distributive Denial of Service (DDos) attack

- A **Denial of Service (DoS)** attack uses only a small number of attacking systems (possibly just one) to overload the target. This was the most common type of attack in the early days of the Internet, where services were relatively small in scale and security technology in its infancy. However, nowadays, a simple DoS attack is often simple to deflect as the attacker is easy to identify and block. One notable exception here may be industrial control systems, where equipment may have a low tolerance to bogus traffic, or may be connected via low bandwidth links that are easily saturated.

- In a **Distributed Denial of Service (DDoS)** attack, the attacker enlists the help of (many) thousands of Internet users to each generate a small number of requests which, added together, overload the target. These participants may either be willing accomplices (such as attacks initiated by loosely organised illegal "hacktivist" groups) or by unwitting victims whose machines have been infected with malware.

Problems caused by Denial-of-Service attacks

- Downtime
- Revenue Loss

- Reputation Damage
- Loss of Trust
- Operational Costs
- Mitigation Expenses
- Intellectual Property and Data Loss
- Data Breach Risks
- Customer Support Challenges

Detecting DoS Attack

There are various methods to detect DoS attacks like strengthening firewall rules, etc but the methods used in this project can be used by anyone even a non-technical person to detect a DoS attack.

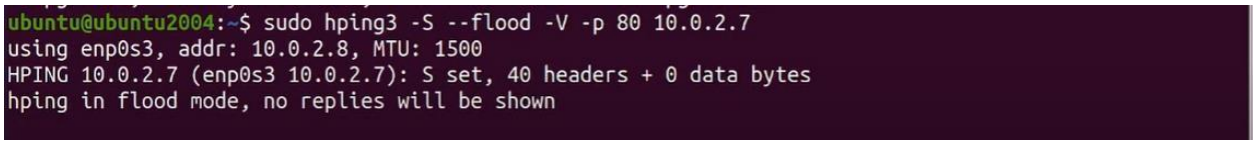
The methods and tools which we have used to detect DoS attack are –

** The tools which we have used to do DoS attack here in this project are “hping3” and “aSYNcrone” and we are mainly doing SYN flood attack.

1. **Wireshark** - Wireshark is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

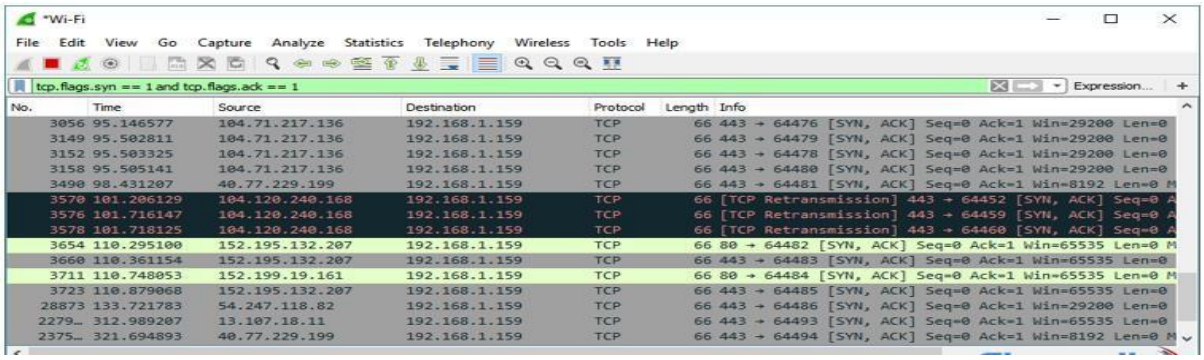
Steps to do to detect DoS attack detection using Wireshark –

1. First we start doing DoS attack using our “hping3” tool from our machine on to our target machine by using this command “sudo hping3 -S –flood -V -p <target port> <target ip address>”. Hping3 is a tool comes pre-installed with Kali Linux.



2. Then we open the Wireshark GUI console on the victim machine and start analysing the packets there first you need to select your network interface which you can find typing “ifconfig” command in your terminal.
3. If in the Wireshark window you see packet continuously coming from a single ip address in bulk or bulk packets are coming like this as shown in picture

below and hitting the ip address of your machine then you can confirm that someone is trying to DoS attack on your machine.



2. **Snort3** - Snort 3 is the next generation IPS (Intrusion Prevention System). It is an open-source software and can be downloaded from GitHub.

Steps to do to detect DoS attack using snort3 are –

1. First we are going to do DoS attack using “aSYNcrone” tool which is an opensource tool and can be downloaded from GitHub by using the command “. /aSYNcrone <source port> <target IP> <target port> <thread number>”.

2. Then in our target machine we start snort by using this command “sudo snort

-A console -c /etc/snort/snort.conf" and then our snort start analysing the packets. The special thing about snort is that it can identify and differentiate between normal and harmful packets and can give output in terminal unlike Wireshark.

3. If you see anything like packets getting captured and see something like "Classification: Potentially bad traffic or Attempted Information Leak" or something like that as shown in picture below then you can confirm that someone is trying to do DoS attack on your system.

Other advance methods that can be implemented to detect and prevent DoS attacks are –

- Upstream filtering
- Application front – end hardware
- Strengthening firewall rules
- Blackholing and sink holing
- Blocking vulnerable Ports, etc.
- Enrol in a DoS protection service that detects abnormal traffic flows and redirects traffic away from your network. The DoS traffic is filtered out, and clean traffic is passed on to your network.
- Packets and traffic filtering

Conclusion

In conclusion, the project aimed to test network security and determine the overall effects of a denial-of-service attack against a targeted website/network. The project involved testing a denial-of-service SYN flood attack against a targeted system on our local network. We also used virtual machines to set up our testing environment

as well as used some tools to analyse the network traffic during the simulation. The results of the project indicate that the detection of denial-of-service attacks is a challenging task, but it is possible to detect them using the mentioned tools. The study also proposes a creative, effective, efficient, and comprehensive prevention and detection of an actual Denial of Service (DoS) attack.

References

1. DoS Attack - Definition, Examples and Prevention (crashtest-security.com)
2. Denial of Service (DoS) guidance - NCSC.GOV.UK
3. Understanding Denial-of-Service Attacks | CISA
4. Denial-of-service attack - Wikipedia