Name: **Priyal Jawale**

**Introduction**

Each service we have traditionally accessed in today’s world, such as banking, paying utility bills, purchasing a car or a house, or buying grocery, and watching movie, can be accessed as an online service. With the rapid development of network technology and application, network security is becoming more and more critical. Online games are common, allowing different players to compete simultaneously in the same game from different parts of the world. One of the most popular methods of invasion that often lead to major economic damage and effects is Denial of Service attack. The research on the theory of DoS attack and the methods to detect such attacks becomes very important as the attack techniques and technologies are improved considerably. DoS attacks will disable any of these targets to deny service to legitimate users, either by leveraging some loophole or by overwhelming a critical resource. DoS attacks deplete some limited resources that legitimate traffic requires, or since they exploit a server vulnerability that slows down or results in disabling of user request processing. The legitimate user perceives significant request-response lag in interactive traffic, low quality audio and picture due to media and gaming traffic loss of packets. A DoS attack involves breaching a single instance of a main internet device such as hosting server or a network switch using a single internet connection and interrupting its normal operation. This attack entails manipulating multiple devices such as servers, network switches, or routers positioned across the globe in different geographic locations.

**Survey**

The DoS attack often uses the protocol flaw to deliver the victim computer with a large number of packets. The TCP/IP is used for the internet and the attacker may use the TCP defect. Slowloris is a DoS attack based on TCP that takes advantage of HTTP. The attackers establish multiple connections to HTTP server and keep them alive by sending incomplete HTTP headers on a regular basis.[1] The aim is to cause multiple connections to a single server until it runs out of all allocated sockets and its therefore subjected to DoS. Application layer attacks such as Slowloris are termed stealthy attacks because they are very difficult to make distinctions between legitimate traffic and attacks such as Slowloris traffic. At regular intervals, Slowloris attacks are characterized by traffic bursts.

The DoS attack based on TCP SYN flood attack has long been known to the research community. The attack takes advantage of the three-way mechanism of the conventional TCP handshake. Many TCP implementations set a system state when a SYN packet initiates a TCP connection. Because there are limitations as to how many states can be maintained, attackers send a high volume of TCP SYN packets until some network asset is saturated by the combined effect of all half-open connections. Using spoofed IP address, most of the SYN flood attacks are actually launched.

To separate the TCP, SYN, RST packets, we depend on packet classification. The original motivation for the packet classification was the need to provide network distinctions for IP flows. To identify TCP SYNs and RSTS, the TCP header needs to be accessed. Wustrow[4] et al. used a newer darknet dataset to categorize the darknet traffic, they used features as protocols, port numbers, packet rates and packet sizes. In order to analyse DDoS behaviour from multiple data sources, Mao et al. focused on in-depth packet-level characterization using three different datasets, mostly DDoS traffic [6]. They revealed that TCP is the main protocol used to generate DDoS attacks, and most of the TCP packets in these traces are only based on floods from SYN and ACK.

Also, in the survey it is found that RSTs are created for two major reasons, one is passive in which the RST is transmitted in response to the arrival of a packet intended for a closed port and the other is active in which the RST is started to abort a TCP connection [2]. At the same session, every active RST is associated with the SYN. The flooding SYN traffic has considerable regularity that can be filtered out under SYN flooding attacks. For example, to shut down the victim server for approximately 10 minutes, at least 300,000 SYN packets are required to be inserted by the group of attackers. Nevertheless, the number of RSTs remain largely unchanged during the same period of time.

**Solution**

Deploy an antivirus program and firewall into your network. There are many ways to defend against SYN floods, but Syncookies are the most commonly used solution. If the link timeout of the database is known, the Slowloris attack can be further optimised. This enables the Slowloris to reduce the number of times that incomplete requests need to be sent. There are various techniques, such as load balancing and reverse proxies, that can be used to lower the impact of Slowloris. Another effective mitigation strategy is to limit the frequency on the data plane. Rate limiting can be very useful when it is not possible to block all access to a page.

Network Behaviour Analysis (NBA), which analyses network traffic to detect vulnerabilities which produce irregular traffic flows, such as denial of service (DoS) attacks, other types of malware (e.g. Worms, backdoors) and policy violations. IPS has the ability to take action on specific policies such as blocking the connection, providing warnings, quarantining the local host or combining them. Policies describe the rules that determine what needs to detected and the type of response needed. Policies will include both signature-based rules and rules of anomaly detection in order to learn and set thresholds for normal network traffic. DoS and the rules for recognition are based on traffic statistics. Also, to mitigate the DoS attack one prevention mechanism that can be deploying an antivirus and firewall to the network.

**Findings**

* Used Slowloris tool to execute DOS attack at Ubuntu machine ip\_address: 192.168.2.38(attacker machine)
* Used the xampp server
* Executed the code to read the network traffic on victim machine Ubuntu ip\_address: 192.168.2.39

Given how well these attacks work, I have chosen as features a set of six performance metrics that can potentially define these attacks. The first five features are

1. source port
2. destination port
3. source ip address
4. destination ip address
5. protocol.

The other feature includes SYN\_Flag, ACK\_Flag and RST\_Flag.

When the condition SYN\_Flag ==0 and ACK\_Flag==0, it is observed that the victim server is flooded with SYN\_Flag requests and no ACK\_Flag which determines the DoS attack i.e SYN flood attack.

It is also observed in the captured traffic the RST\_Flag is always zero when the attacker is sending HTTP connection requests to the victim server which indicates DoS attack. The RST\_Flag is used to reset the connection when the attacker sends ACK with RST\_Flag the connection is established the server can abort

**Snapshot**

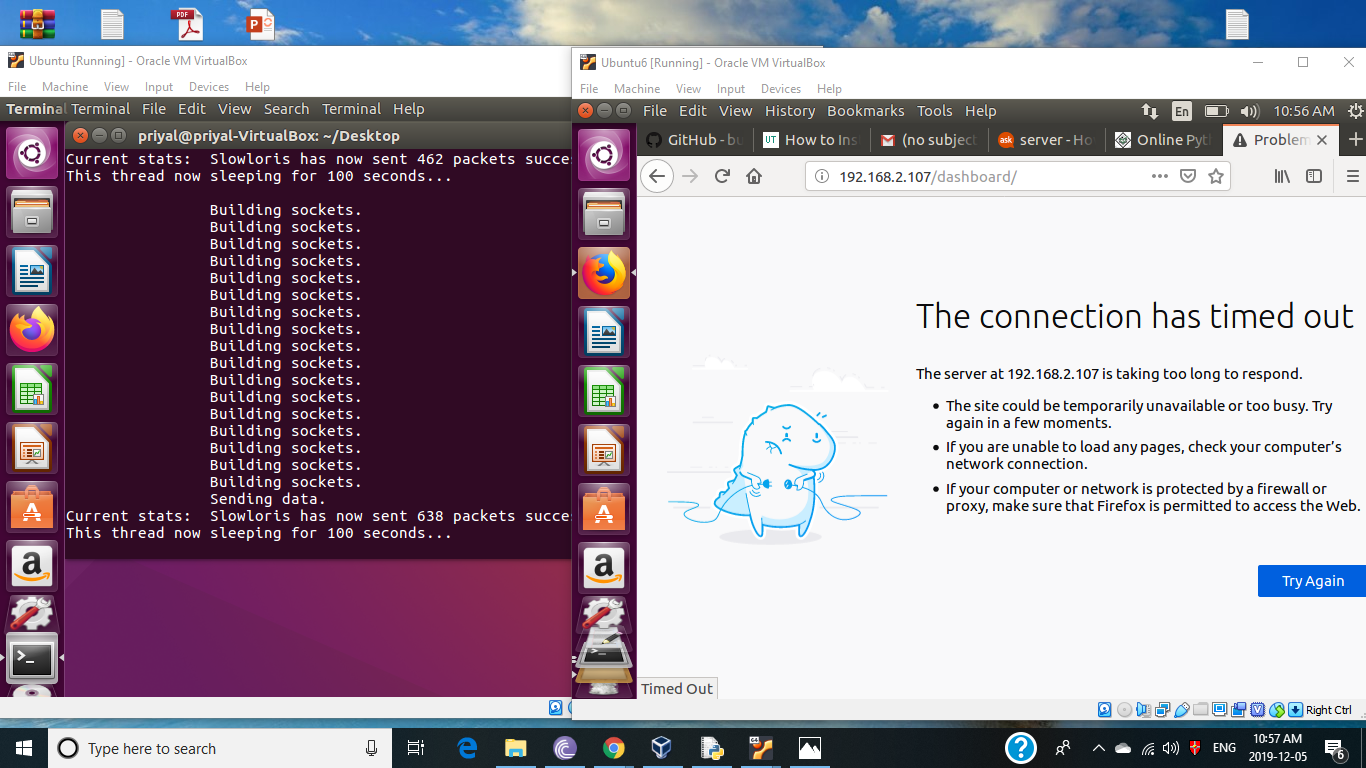


Figure 1: Slowloris attack – xampp server down

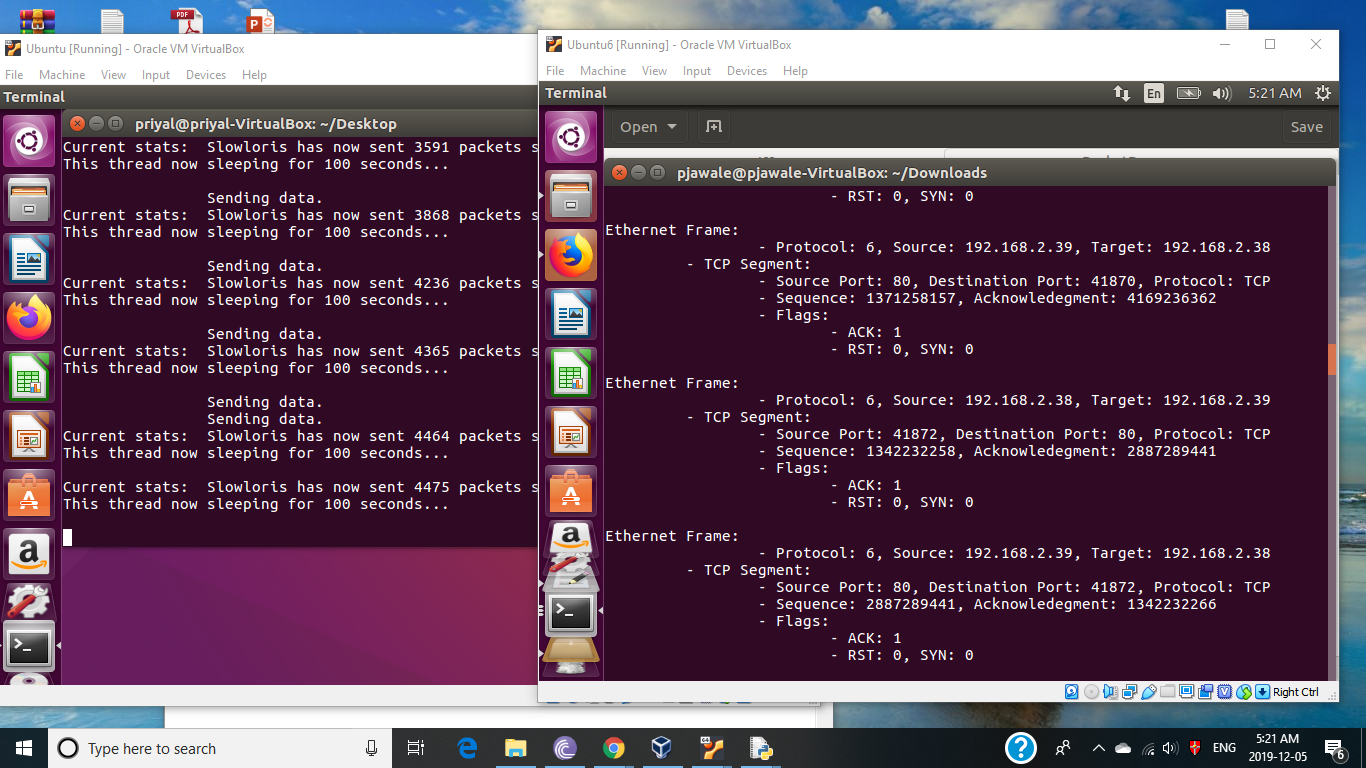


Figure 2: Traffic Flow displaying the features.

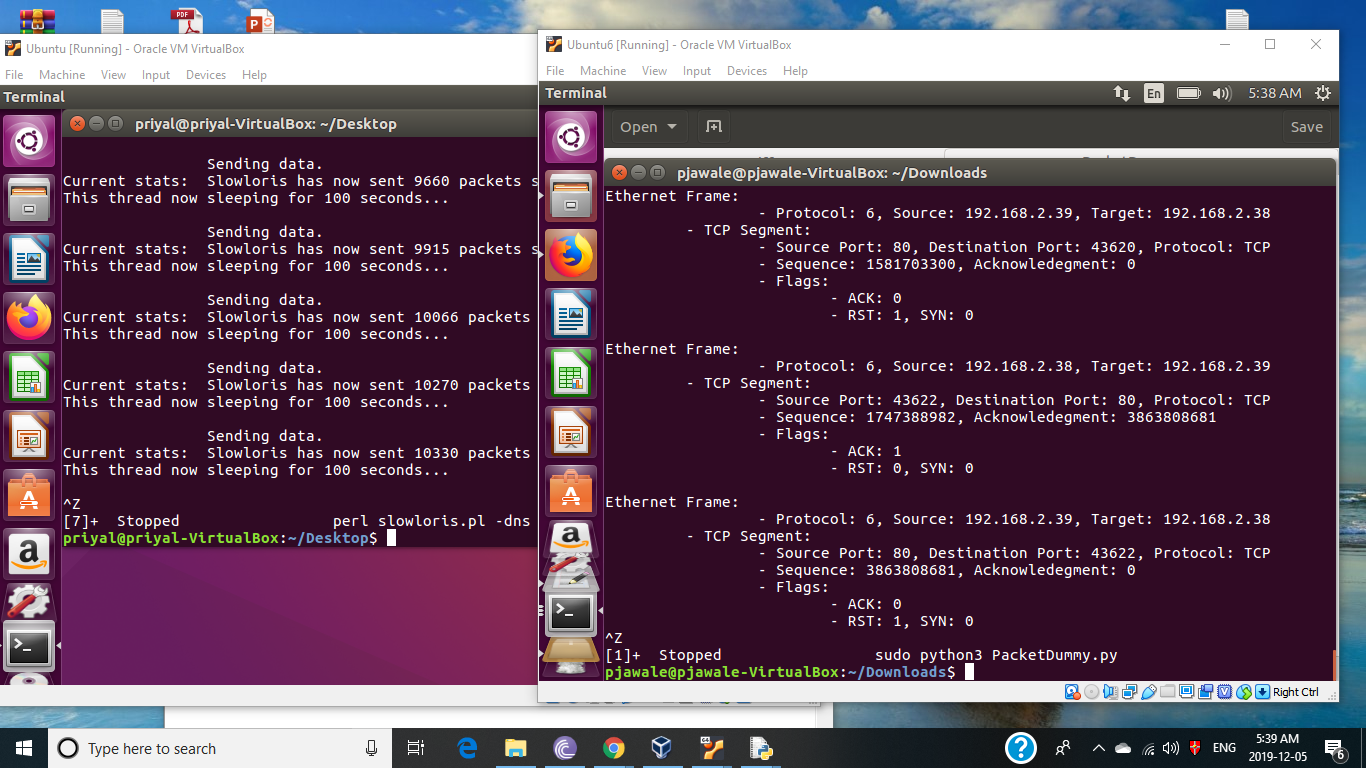


Figure 3: RST value set when there is no attack.

**References**

1] A. Aqil, A. O. F. Atya, T. Jaeger, S. V. Krishnamurthy, K. Levitt, P. D. Mcdaniel, J. Rowe, and A. Swami, “Detection of stealthy TCP-based DoS attacks,” *MILCOM 2015 - 2015 IEEE Military Communications Conference*, 2015.

2] H. Wang, D. Zhang, and K. G. Shin, “Detecting SYN flooding attacks,” *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*.

3] E. Balkanli, A. N. Zincir-Heywood, and M. I. Heywood, “Feature selection for robust backscatter DDoS detection,” *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, 2015.

4] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, “Internet background radiation revisited,” *Proceedings of the 10th annual conference on Internet measurement - IMC 10*, 2010.

5] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson, “Characteristics of internet background radiation,” *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement - IMC 04*, 2004.

6] Z. M. Mao, V. Sekar, O. Spatscheck, J. V. D. Merwe, and R. Vasudevan, “Analyzing large DDoS attacks using multiple data sources,” *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense - LSAD 06*, 2006.

7] A. R. Yusof, N. I. Udzir, A. Selamat, H. Hamdan, and M. T. Abdullah, “Adaptive feature selection for denial of services (DoS) attack,” *2017 IEEE Conference on Application, Information and Network Security (AINS)*, 2017.

8] W. Liu, “Research on DoS Attack and Detection Programming,” *2009 Third International Symposium on Intelligent Information Technology Application*, 2009.

9] S. Pu, “Choosing parameters for detecting DDoS attack,” *2012 International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP)*, 2012.

10] M. Hefeeda and A. Habib, “Detecting Dos Attacks And Service Violations In Qos-Enabled Networks,” *Handbook of Security and Networks*, pp. 191–220, 2011.

11] G. Carl, G. Kesidis, R. Brooks, and S. Rai, “Denial-of-service attack-detection techniques,” *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.