Understanding Denial of Service (Dos) Attacks Using OSI Reference Model

Gulshan Kumar
Assistant professor
SBS State Technical campus
Ferozepur (Punjab) -India

ABSTRACT:
Network security is a specialized field consisting of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources as well as ensuring their availability through proper procedures. Many security mechanisms, tools are being developed and deployed to defend against network attacks and to make the network computing resources available to the legitimate users. In spite of all these efforts, the organizations around the world continue to suffer security attacks specially called Denial of Service (DoS) attacks. DoS attacks constitute one of the major threats and among the hard security problems in today's Internet. These attacks can easily consume computing and communication resources of the victim or disrupt the log availability of resources to the intended users with a short period of time. The problem is a serious concern in today's network security field. Several defence mechanisms have been proposed to tackle the problem of DoS attacks. This paper highlights a structural way to understand DoS attacks with respect to different layers of the OSI reference model. Moreover, various attack vectors, attack tools, trends in detection and mitigation mechanisms are delineated.

Keywords– Cyber attacks, Data Breaches, Denial of Service attacks, Intrusions, Network Security, Security Intelligence, Security Threats

I. INTRODUCTION:

The main objectives of network security are availability, integrity, and confidentiality [9]. Denial of Service (DoS) attacks disrupts the availability of network resources. DoS attacks have been a significant problem for many years, but remain to be un-resolved. In the recent past, DoS attacks are assumed to be an important issue in the field of network security as these attacks incidents continue to prevail [2]. A recent research survey conducted in the first quarter of 2014 by Prolexic highlights that there is a 47 percent increase in total DDoS attacks in comparison to first quarter of 2013 [14]. These attacks can be easily launched by exploiting flaws in Internet protocols like TCP/IP and UDP. Moreover, availability of free attack tools like Backtrack, Meta sploit, Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC) and many more, also simplifies the attack process.
These tools automate the process of creating DoS types of attacks, allowing even non-technical people to quickly and easily threaten their choice of website.

A Denial of Service (DoS) attacks usually either involves attackers sending messages to exploit certain vulnerabilities leading to the abnormality or paralysis of network based systems, or sending an enormous amount of regular messages swiftly to a single node to run out the system resources that result in crash of the entire system [12]. A DoS attack is called a Distributed Denial of Service (DDoS) attack if it gets originated from multiple distributed sources. In DDoS attacks, a large number of controlled bots (also referred to as zombies) are used from distributed locations to initiate huge amount of traffic against the victim(s).

Generally, DoS attackers exploit TCP/IP/UDP protocols for launching these attacks. Either, they direct a huge amount of abnormal network packets towards the victim(s), that results overloading of their network resources such as consuming entire bandwidth, memory, etc. Or they exploit vulnerabilities in network protocols to fail the functioning of network devices. In both the cases, network resources or services are restricted or prevented for the intended users. Major difficulty in detecting such attacks is that network traffic consists of mix of normal or legitimate traffic and abnormal or attack traffic. Moreover, in most of the cases, attack traffic looks like normal traffic.

With the rapid growth of technology application service providers, network service providers, cloud services and availability of network capable mobile devices, our dependence on the networks is increasing day by day [12]. For example, we are now more dependent over the network for online banking, information retrieval, online shopping and many more. This has changed the scenario in terms of business and other information based systems, but also opened an avenue for network attackers to mount a large number of attacks against network resources. Motives for these attacks appear equally diverse like personal reasons, the prestige, criminal, commercial, or ideological in nature [7, 8, 17, 18, and 4].

In this paper, we attempt to introduce the DoS attacks by presenting the state-of the-art in the field through a classification of DDoS attacks with respect to different layers of Open System Interconnection (OSI) reference model and a recent trend in the defence mechanisms that can be used to combat these attacks.
Article overview: following this introduction, section 2 highlights the adversaries behind the DoS attacks. Section 3 introduces the basic functions of the OSI reference model. Section 4details the possibilities of DoS attacks with respect to the layers of OSI reference model. Next Section describes the possible DoS attack detection and mitigation mechanisms and their current trends in the field of network security. Finally, the paper concludes the current scenario of DoS attacks.

II. BRIEFS OF OSI MODEL

In the recent past, with the skyrocketing popularity of network based information systems and applications has come a sudden increase in the numbers, types, magnitudes, and costs of attacks that particularly intend their vulnerabilities. Usually, these attacks belong to the following categories:

- Denial of Service (DoS) attacks
- Attacks that steal confidential data, such as SQL injection and other command injection attacks

Recently, there occurred a large number of DoS attack incidents. DoS attacks take many forms, and utilize many attack vectors. The sheer number of DoS attacks makes their study and understanding for a better prevention challenging. Many researchers classified DoS attacks based upon different criteria like degree of automation, random scanning, communication mechanism, exploited vulnerabilities [11], attacked protocol level, attack rate dynamics, impact [5] and many more. The detailed classification can be further studied in [11, 5, 16].
The researchers attempted to present a clear cut view of DoS attacks and their countermeasures. But still, we believe that a more simplified and effective view for these attacks can help the people think about the attacks, their impact and hence their countermeasures. In order to present a simplified view of attacks, we examined those using different layers of the OSI reference model. Because, the OSI reference model details each phase of the process involved to connect a computer to the network. Most of the researchers, developers and manufacturers use the OSI model as a common platform to improve network communications.
There are seven layers in total, each fulfilling its own purpose in a connected network framework called the OSI

Model. In a nutshell, the OSI model is separated into seven layers that transport data up and down the chain, from the user, all the way to the physical server and back again as depicted in Fig. 1 [10].

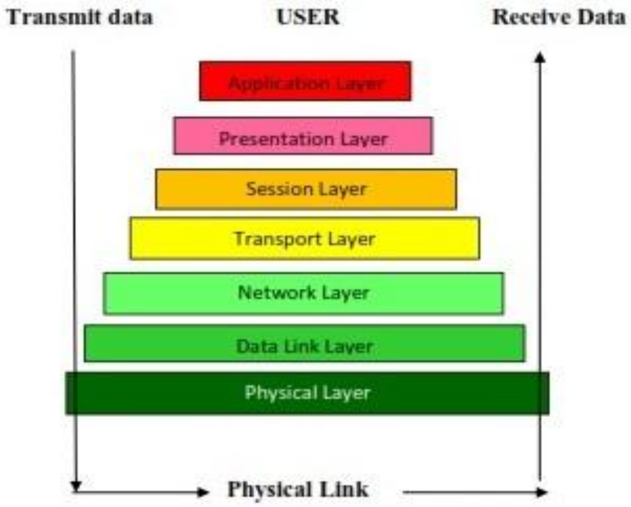
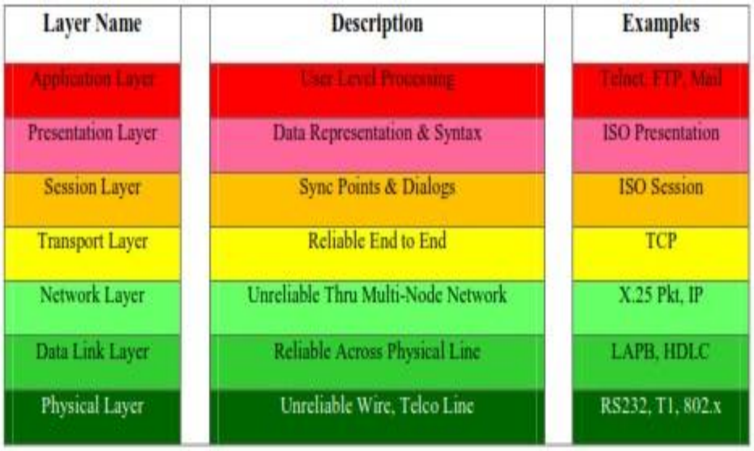


Fig. 1 Layers of OSI reference model

Each layer contains a set of protocols and responsible for sending/receiving protocol data unit (PDU) to/from its counterpart. These protocols are responsible for carrying out its assigned functions. The brief break down of functions of different layers is as shown in Fig. 2 and described in following paragraphs:



Layer Name	Description	Examples
Application Layer	User Level Processing	Telnet, FTP, Mail
Presentation Layer	Data Representation & Syntax	ISO Presentation
Session Layer	Sync Points & Dialogs	ISO Session
Transport Layer	Reliable End to End	TCP
Network Layer	Unreliable Thru Multi-Node Network	X.25 Pkt, IP
Data Link Layer	Reliable Across Physical Line	LAPB, HDLC
Physical Layer	Unreliable Wire, Telco Line	RS232, T1, 802.x

Fig. 2 Functions and protocols in the OSI reference model

Layer 7 Application layer allows the access to network resources. It is responsible for sending and receiving data from one application to another. The unit of communication (PDU) at this layer is message/data.

Layer 6 Presentation layer is responsible to format data for exchange between points of communication like translates, encrypts and compress the data.

Layer 5 Session layer is responsible for governing / establishing / terminating sessions over the network.

Layer 4 Transport layer is aimed to provide reliable delivery of message/data from one process to another. It ensures error free, in sequence and without duplication of transmission of packets. The unit of communication (PDU) at this layer is a segment, datagram or packet depending upon protocol used in this layer.

Layer 3 Network layer is handling the movement of packets from source to destination. It provides addressing and routing to the packets. The unit of communication (PDU) at this layer is the packet.

Layer 2 Data link layer manages the error free transmission of data over physical media. The unit of communication (PDU) at this layer is a frame.

Layer 1 Physical Layer deals with transmission of 0s and 1sover transmission media. Its function involves translation of bits into signals. The unit of communication (PDU) at this layer is bit.

III. DOS ATTACKS AND OSI REFERENCE MODEL

In this paper, we attempt to introduce the DoS attacks by presenting an updated perspective for their classification and recent trends in detection& mitigation mechanisms. DoS attacks are classified with respect to seven layers of the OSI reference model. Such classification will present a simplified and clear view of DoS attacks. It will definitely help to achieve a better communication and cooperation between researchers and hence better defence mechanisms.

Description of DoS attacks with respect to different layers of the OSI reference model is as below:

3.1 Application layer attacks

Application-layer DoS attacks are abit more complicated. They disable specific functions or features as opposed to an entire network. Usually, these attacks are used against financial institutions to divert IT and security administrators from security breaches. As per report of 2nd quarter 2014 conducted by Prolexic, the most common application-layer attacks were HTTP GET floods (7.5 percent of all attacks mitigated in Q2), HTTP POST floods (2.3 percent), PUSH floods (0.8 percent) and HEAD floods (0.2 percent) [15].

This kind of attacks is done generally for specific targeted purposes, including disrupting transactions and access to databases, requires comparatively less re- sources. These attacks are some of the most difficult attacks to extenuate against because they mimic human behaviour as they interact with the user interface. The application layer of the OSI reference model has two main categories of protocols as follows [1]:

- Protocols that directly service users (e.g., HTTP, FTP, IMAP, Telnet, SMPT/POP, IRC, XMPP, SSH etc.)
- Support protocols that fortify various system functions (e.g., DNS, SNMP, BOOTP/DHCP, TLS/SSL, SIP, RTP, NTP etc.).

Application layer DoS attacks are more worrying than the attacks at other layers because of following reasons [6]:

- High obscurity: These attacks follow Legitimate TCP or UDP connections, so it is very difficult to differentiate them from legitimate users.
- Highly efficient: These attacks require very less number of connections.
- Affect multiple applications: They may affect many different applications. Any one of the protocols examined above may be subject to a DDoS attack [1]. Many of them targets HTTP to exhaust a web server's vitality.
- Highly targeted: These attacks are highly-targeted oriented. Generally, these attacks are tailored to aim a specific application. For example, web servers that run a combination of Java, PHP5, and ASP.NET may be targeted by specially crafted HTTP requests, which may collide with the web server´s hashing operation "when unique requests return non-unique and overlapping responses¨.
- Simplicity in exploitation: These attacks may exploit the simplicity in the application layer. For example, a simultaneous refresher of browsers by thousands of users may collapse the server soon or later.
- Multiple effects: These attacks may affect many victims directly or indirectly. For example, a DNS attack at a single DNS provider may affect all of its customers [3].

- Requirement of limited resources: These attacks require limited resources, so limited investment by attackers can result a successful attack.
- Follow normal traffic rules: Traffic involved in these attacks seems to be legitimate as it follows the protocol rules, rate and complete TCP handshake process. It follows all the basic requirements that a normal traffic flows.

Application layer DOS attacks can be categorized into following categories [6]:

1. High-Bandwidth Attacks
2. Low-Bandwidth Attacks
3. Attacks that Steal Data

Although HTTP is the most under attack protocol, other protocols are attacked as well, such as; DNS dictionary attacks consisting of registrar hijacking, and redirection cache poisoning, VoIP (SIP INVITE Flood Attack), SMTP buffer overflow attacks [3] as described in Table 1.As per the report of Arbour's network, most commonly protocols targeted for application layer attacks are depicted in Fig. 3 [3].

Table 1 most commonly exploited protocols at application layer

Protocol	Attack method
HTTP	HTTP Malformed Attacks, HTTP Request At- tacks, HTTP Idle Attacks
DNS	DNS Query/Answer Malformed Packet, DNS Query-Length Buffer Overflow, DNS Query Buffer Overflow, Man-in-the-Middle, DNS Cache Poisoning Attacks, DNS Amplification Attacks, DNS Dictionary Attacks
VoIP	SIP INVITE Flood Attacks, SIP Call Setup Request Attacks, SIP Malformed Packet At- tacks, Real-Time Transport Protocol (RTP), Flood/Quality of Service (QoS) Attacks
SMTP	SMTP Error Denial of Service, Mailbox Denial of Service Attack (Excessive Email Size), SMTP Mail Flooding attacks, SMTP Buffer Overflow Attacks: Different SMTP commands can cause the SMTP server to crash or execute arbitrary

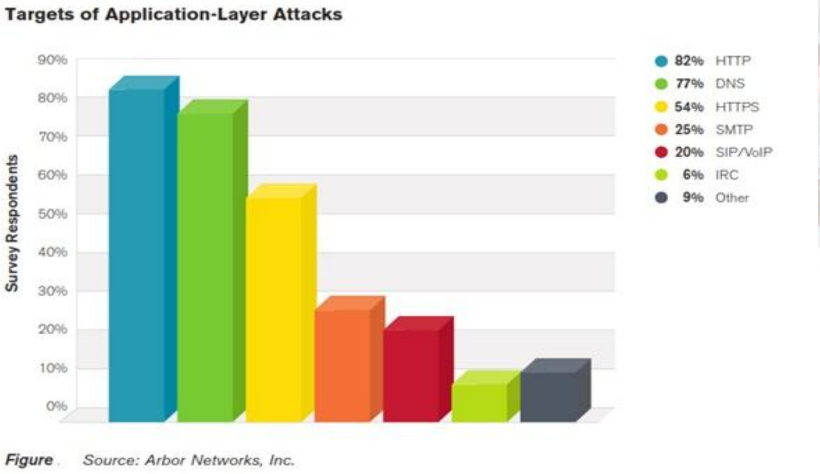


Fig. 3 Most commonly protocols targeted for application layer attacks

3.2 Presentation layer attacks

The presentation layer DoS attack involves malformed Secure Socket Layer (SSL) requests. SSL (or TLS) provides security in web services like banking, online shop- ping etc. Because of the security features, most of the well-liked organizations are migrating to SSL for providing improved security in their services [3]. Nowadays, most transactions are protected by SSL. But, it has also attracted more attention of the attackers. The TCP protocol - TCP handshake is a common victim of a DoS attack. After finishing the TCP handshake, there is a session of the network layer for SSL handshake. During SSL handshake, there is the exchange of messages to validate the authenticity of both communicating entities. They establish the encryption key and options for the secure communication afterwards.

There are several attacks which exploit the SSL handshake to exhaust server resources. The Pushdo botnet carry out this simply by sending garbage data to a target SSL server. The SSL protocol is computationally expensive and it generates extra workload on the server to process garbage data as a legitimate handshake. In this process, the server may stop accepting SSL connections or it may restart them. A device like Firewalls fails in this scenario, because both the entities have successfully finished the TCP handshake. And now they are sending traffic to an authorized service. Generally, attackers use SSLto tunnel HTTP based DoS attacks.SSL DDoS Attacks may be classified into two categories:

- Protocol misuse attacks
- SSL Traffic Floods

3.3 Session layer attacks

Session layer manages the establishment, termination and synchronization of sessions within an operating system over a network system. The attackers exploit logon and log off protocols for mounting DoS attacks in the session layer. For ex- ample, Telnet DoS attack. The Telnet application allows a terminal to remotely communicate with the counterpart. Telnet with IP network sends and receives the data remotely using port 23. Telnet attacks can be categories into three classes as follows [13].

Telnet communication sniffing Telnet brute force attack Telnet DoS - Denial of Service

3.4 Transport layer attacks

Transport layer DoS attacks are generally volume based attack son a network infrastructure. As per the report of Prolexic, eighty-nine percent of Q2 2014 DDoS attacks targeted the infrastructure layer; the remaining 11 percent were application attacks [15]. The most common infrastructure attacks included SYN floods (26 percent of all attacks mitigated in Q2), UDP floods (25 percent), NTP (7.4 percent) and ICMP (6.6 percent).

These attacks are dependent upon generation and transmission of huge volume of network traffic to disrupt or completely block the availability of network services/resource for legitimate users. Such attacks generally involve exploitation of TCP and UDP protocols for saturating network resources.

3.5 Network Layer attacks

Network layer DoS attacks involve injecting a victim network with more traffic than it can handle. As a result of additional network traffic, the victim network starts responding slow or it drops some packets. The loss of packets may cause a flood of retransmitted requests, which further increase the network traffic. In- creased network traffic saturates the network and it becomes unavailable for the intended users. For example, in Ping flood attack, ICMP data flood the network and consumes the whole bandwidth. The network starts denying the services. Other examples of network attacks include Smurf attack, ping of death, DNS amplification attacks, ACK attacks, reflection attacks etc. As per report conducted by Prolexic in Q2 of 2014, the most common reflection attack vectors included NTP (7.35 percent), CHARGEN (4.54 percent) DNS (4.00 percent) and SNMP (3.03 percent) [15]. During the attack at this layer, network bandwidth is generally saturated by imposing extra load. As a result, bandwidth becomes unavailable for the intended users.

3.6 Data link layer attacks

The data link layer is responsible for establishing/ maintaining and deciding how to transfer data over the physical layer. PDU used here in this layer is frame. IEEE
802 standards are used as protocols for communication at this layer. Attacks at this layer can vary from address resolution protocol (ARP) cache poisoning for wired clients to de-authentication of wireless clients. The most critical attacks at the data link layer involve Content Address Table (CAM) exhaustion, ARP spoofing, DHCP starvation attacks, MAC address spoofing, VLAN attacks and many more. These attacks generally disrupt the normal traffic flow from sender to receiver. Tools used to mount DoS attacks at the data link layer are as summarized in Table [19]:

3.7 Physical layer attacks

The physical layer is concerned with media, i.e. cable to transfer bits from source to receiver. The layer uses 100 Base-T and 100 Base-X protocols, and hub, patch panels, and R45 jack as devices to transfer data. Attacks on physical layer include physical destruction, obstruction, manipulation and malfunctioning of physical media, which leads to its unavailability to the intended users. It requires the repair to make the physical media resources available.

IV.CONCLUSIONS

Certainly, DoS attacks pose a severe problem on the Internet and challenge its rate of growth. In this paper, we attempted to attain a clear view of the DoS attack problem, and presented an updated perspective of the problem in respect to different layers of the OSI reference model. Having, this clear view of the problem, our understanding about the problem is clarified and this way we can discover more effective solutions to the problem of DoS attacks. One big benefit of the development of DoS attack classification is that effective communication and cooperation between researchers. The effective communication and cooperation can result to identify additional weaknesses of the DoS problem. This classification necessitate be constantly updating and extending as new threats are discovered and hence their defines mechanism. Their value in achieving further research and discussion is definitely great. DoS attacks remain at the top of operational threats nowadays. Whereas, DoS attacks against infrastructure and sophisticated attacks against applications remain the top concern for 2014. DoS attacks and their variety remain a key issue, so most of the organizations demands for DoS detection/mitigation mechanisms/tools for their customers.

However, we believe that no single technology based solution alone can be effective in providing defines against a variety of DoS attacks. The comprehensive protection of an organization's from DoS attack requires a multi-faceted security strategy.

REFERENCES

1. Abliz, M.: Internet denial of service attacks and defense mechanisms. University of Pitts- burgh, Tech. Rep. TR-11-178 (2011)
2. Alam, M.F.: Application layer - ddos a practical approach & mitigation techniques. URLhttps://conference.apnic.net/data/37/l7ddos apricot- 1393257782.pdf
3. Arbor, N.: Worldwide infrastructure security report, volume ix. URLpages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
4. Chauhan, A., Mishra, G., Kumar, G.: Survey on data mining techniques in intrusion detection. Lap Lambert Academic Publ (2012)
5. Douligeris, C., Mitrokotsa, A.: Ddos attacks and defense mechanisms: classification and state-of-the-art. Computer Networks 44(5), 643–666 (2004)
6. Infosec: Layer sevenddos attacks. URL http://resources.infosecinstitute.com/layer-seven-ddos-attacks/. Accessed on 20/8/2014
7. Kumar, G., Kumar, K.: Network security - an updated perspective. Systems Science & Control Engineering: An Open Access Journal (2014). DOI 10.1080/21642583.2014.895969
8. Kumar, G., Kumar, K., Sachdeva, M.: An empirical comparative analysis of feature reduction methods for intrusion detection. International Journal of Information and Telecommunication Technology 1(1), 44–51 (2010)
9. Kumar, G., Kumar, K., Sachdeva, M.: The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review 34(4), 369–387 (2010)
10. Miller, A.: What is a layer 7 ddos attack? (2014). URLhttp://ddosattackprotection.org/blog/layer-7-ddos-attack/
11. Mirkovic, J., Reiher , P.: A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Computer Communication Review 34(2), 39–53 (2004)
12. Nsfocus: Introduction to ddos attack. URL en.nsfocus.com/.../DDoS%20FAQ/What%20is-%20DDoS%20Attack.pdf. Accessed on 28/7/2014
13. Popeskic, V.: Telnet attacks ways to compromise remote connections. URLhttp://howdoesinternetwork.com/2011/telnet-attacks. Accessed on 28/7/2014
14. Prolexic: Q1 2014 global ddos attack report (2014). URL www.prolexic.com/knowledge- center-ddos-attack-report-2014-q1.html. Accessed on 28/7/2014
15. Prolexic: Q2 2014 global ddos attack report (2014). URL http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2.html. Accessed on 28/7/2014
16. Saafan, A.: Distributed denial of service attacks: Explain nation, classification and suggested solutions. URL http://www.intelligentexploit.com/articles/DDoS-Attacks- explaination,-classification-and-suggested-solutions.pdf. Accessed on 28/7/2014
17. Schneider, D.: The state of network security. Network Security 2012(2), 14–20 (2012)
18. Verizon: - The 2013 - data breach investigations report (2013). URLwww.verizonenterprise.com/resources/reports/rp data- breach-investigations-report-2013 en xg.pdf. Accessed on Sept. 23, 2013
19. Yeung, K.H., Fung, D., Wong, K.Y.: Tools for attacking layer 2 network infrastructure.
20. In: Proceedings of the internationalmulticonference of engineers and computer scientists, vol. 2, pp. 1–6. Citeseer (2008)