Analysis of Network Security Spasms and Circumvention

Sangamithra A [#1] , M.P.Vani [*2]
[#]Research Scholar , Computer Science, VIT University, Vellore, Tamil Nadu
[#]sangamithraa@yahoo.com
[*]Associate Professor Computer Science ,VIT University, Vellore, Tamil Nadu
[*]mpvani@vit.ac.in

Abstract: **Network is one of the rapid growing technology in today's world. Network is attached in our life from small things to large things. Everywhere network is spreaded, where people are surrounded by network. We can get more advantage in various fields by using the network. But at the same time there is a lot of things is there to attack the security of the network. In this paper we discuss about the main common attacks in the network , about the causes of the attack and how to recover from that. So this will be helpful for the researcher to come up with the best prevention of the attacks in network.**

Keywords: Ddos , Protocols , Qos , Dos.

I. INTRODUCTION

In this modern world network has become important in all the field. Network is used by small scale industries to large scale industries. In spite of that it is also used, in education, public, and defense. Ubiquitously we are in need of the networks. As there is advancement in certain things , there will be certain drawbacks or defects taking place simultaneously. So the same thing is getting implemented even in the network field of development, like there is a lack of security which is very essential in the network environment. For example in network even large amount of fund transaction is happening and so many things , so obviously we have to concentrate on the security. We have got so many worms which will affect the network security. The figure1.representsthat there are large number of social users in the world. There by the graph below shows that the number of users gradually getting increased year by year. So in order of secure use of network in this paper we are analyzing what are the common attacks existing that attacks the network and what are the necessary measures we can take to prevent the various attack in the network.

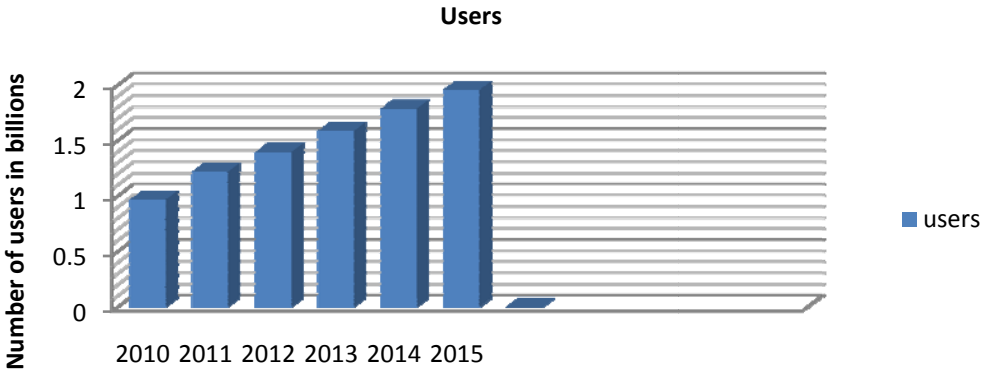

Figure:1:Social media users around the world

For instance if there are n number of attacks in the network, which will reduce the security of the network. In order to have a security usage of network, from the n number of attacks ,we consider seven common attacks which are used by the hackers to attack the network.

Now, This paper outlines the seven common attacks.[1,2,3,4] So many researchers are working to get rid of the attack but they cannot achieve it fully. So we have to concentrate more on the attack of the network to get rid of those.

II. VARIOUS TYPES OF ATTACKS

A. Denial Of Service Attacks (Dos)

DOS attack is the type of attack on the network that is designed to bring the network to its knees by flooding it with useless traffic. DOS attack attempt to make a resources such as web servers , unavailable to users. By using this attack the attacker can inject the fake broadcast packets to force sensor node to perform

expensive signature verification. [5] [9]These attack belongs to interruption and intersection security class and availability, integrity, and authenticity are main threats for this attack.

B. Ddos (Distributed Denial Of Service)

It is the type of the DOS attack which make an online service unavailable by overpowering it with traffic from multiple sources.

Types of DDos attack

i. Volumetric Attacks

To flood the network layer these attacks uses the multiple infected systems which are often part of the botnet. Because of this attack the network consumes excessive amount of bandwidth. There are variety of forms in volumetric attack like, UDP floods:[11,10] Random ports on a server flooded with the UDP packets, causing the server to repeatedly check for and respond to non-existent applications at the ports. ICMP floods: Where the server is flooded with ICMP echo requests from multiple spoofed IP addresses.

ii. Application – Layer Attacks

They target web application packets in order to disrupt the transmission of data between hosts.

iii. State – Exhaustion Attacks

It is also known as the protocol attack which target the connection tables in firewalls, web application servers, and other infrastructure components.

C.Brute Force Attacks

In network some attacks look for a back way in , but a brute force attack tries to kick down the front door. The main motivation of brute force attack is to decode an encrypted data such as a system's password or data encryption standard key. Brute force will mostly attack the network layer.

D. Browser Attack

This attack target the end user who are browsing the internet. It will encourage user to download malware disguised as a fake software update or application. When a person browses the web, their computer is normally protected from attack by a firewall, that filters out suspect messages. But researchers at SPI Dynamics, based in Georgia, US, have found that certain JavaScript code embedded in web page can be used to bypass the firewall. JavaScript is a simple browser-based programming language that is widely used to make web pages interactive.

When a user visits such a page, the code is able to automatically probe the local network to which the user's machine is connected. [6]Once this has identified the computers and other devices on the network, the same method could be used to send commands to crash or control them.

Fyodor Vaskovich, a respected security expert and creator of the network mapping tool NMAP, says the technique poses a dilemma for web developers.[8] This is because blocking the relevant JavaScript functionality at the browser level would also disable many normal websites.

E. Shellshock Attacks

Shellshock also known as Bashdoor , is a family of security bugs in the widely used unix bash shell , the first of which was discovered on 24 September 2014.It is a serious vulnerability affecting Linux, UNIX and OS computers, is making life difficult for IT admins, as vendors rush out patches to stay ahead of the cybercriminals trying to exploit this bug. The attacker can exploit shellshock by injecting malicious commands into a website to compromise a server. Once the server is under the cybercriminals control , they can drop malware on the server to steal data , compromise other computers , or launch DDoS attack.

F. Ssl Attack

SSL attacks aim to intercept data that is sent over an encrypted connection. A successful attack enables access to the unencrypted information. Hackers hide malicious code in SSL packets to bypass on-premises inspection engines and crash web servers. In some cases, hackers insert code into the encrypted communications channel between two parties to stage man-in-the-middle attacks. Even simple attacks gain new life when delivered over SSL connections that can't be inspected.

G. Backdoor Attack

A back door is a means of access to a computer program that bypasses security mechanisms. According to Trend Micro's report, "Backdoor Use in Targeted Attacks," applications that allow for remote access to computers known as backdoors are often used for targeted attacks. In these types of breaches, hackers leverage backdoor programs to access the victim's network. The benefit of this attack vector is that the backdoor itself can help cybercriminals break into the infrastructure without being discovered[12].

Backdoors not only provide a disguised point of entry for hackers, but can also offer a number of strategies for intrusion [13]. Trend Micro's report noted that these include

i. *Port binding:* Utilized before firewalls were commonplace, port binding involves specific information configurations to reveal where and how messages are transmitted and delivered within the network.

ii. *Connect-back:* Once firewalls were put in place on many networks, hackers began using the connect-back approach, where backdoors are leveraged to connect the targeted systems to cybercriminals' C&C server systems. This also allows for a reverse connection from the servers to the victim platform through ports not under firewall protection.

iii. *Connect availability use:* This strategy involves the use of several malware samples to not only breach the network, but remain there undetected for long periods of time. [10]This extends the window hackers have to steal sensitive data from the target. The first malware, or "first-line backdoor," serves as a platform to download the second sample, the "second-line backdoor," which performs the actual theft of information.

iv. *Legitimate platform abuse:* The report noted that abusing legitimate platforms has become more common especially as hackers must now work harder to side-step security systems. Within this strategy, cybercriminals abuse a valid platform – like a blog, for example – and utilize it to for the storage of C&C server data.

These are just a few attack strategies that can be carried out with backdoors. Trend Micro noted that other approaches include common services protocol or file header abuse, protocol or port listening, custom DNS lookup use and port reuse.

H.Botnet Attack

A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals. They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.

The word Botnet is formed from the words 'robot' and 'network'.[16] [14] Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage.

Often, the cybercriminal will seek to infect and control thousands, tens of thousands, or even millions of computers so that the cybercriminal can act as the master of a large 'zombie network' or 'bot-network' that is capable of delivering a Distributed Denial of Service (DDoS) attack, a large-scale spam campaign, or other types of cyber-attack.

In some cases, cybercriminals will establish a large network of zombie machines and then sell access to the zombie network to other criminals either on a rental basis or as an outright sale. Spammers may rent or buy a network in order to operate a large-scale spam campaign.

III. PERCENTAGE OF COMMON ATTACKS

In this paper we have discussed about the some of the common attacks in network. Figure 2 depicts that percentage comparison of all the common attacks in today's world network technology

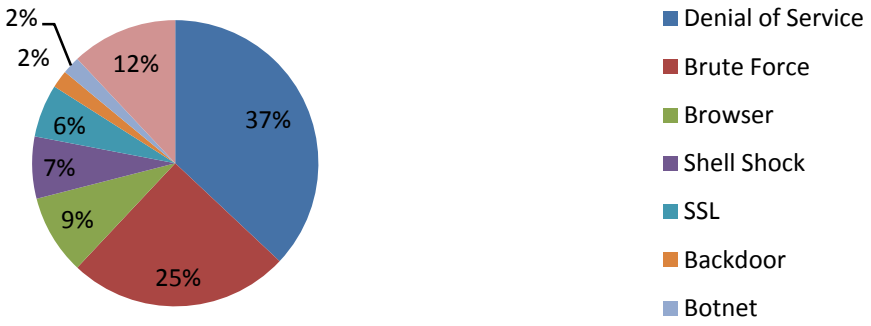

Figure:2: Common Network Attacks

Table:1: Representation of Common Seven Attacks

Name of the Attack	Risk	Protocols	Prevention
DdOS	Network Bandwidth Server Memory CPU Usage Hard Disk Space Data Base Space Data Base Connection Tool	NTP,UDP	Dot Defender Web Application Firewall :dot Defender's unique security approach eliminates the need to learn the specific threats that exist on each web application. The software that runs dot Defender focuses on analyzing the request and the impact it has on the application. Effective web application security is based on three powerful web application security engines
Browser Attack	Spoofing Eavesdropping MITM Spyware Malicious Scripting Cookies	TCP,UDP,DCCP, SCTP, RSVP	Blueprint that Web developers can insert between user-generated pages and the browser. The researchers designed Blueprint to work with eight major browsers, which make up more than 96 percent of current market share, and tested the system against 94 types of cross-site scripting attacks taken from an Internet repository called the XSS Cheat Sheet.
Shellshock Attack	Attacker can inject malicious commands into a website to compromise a server.	DHCP , SMTP , SIP , CUPS	Sophos Antivirus Web Application Firewall Intrusion Prevention System Advanced threat protection.
SSL Attack	Attack mostly communication in network.	TCP , IP	VPN proxy server with data encryption secure shell tunneling.
Backdoor Attack	It cause a security risk because there are always crackers out there looking for any vulnerability to exploit.	TCP	Installing firewall which can block entry points from all but authorized users. Cloud security- Fortified robust network use to monitor particularly of any open source based programme.
Botnet Attack	This attack will spread all types of malware and send spam emails with viruses attached.	TCP , HTTP	Installing effective anti-malware software will help to protect your computer against Trojans and other threats.

IV. CONCLUSION

In this paper we outlined some of the common attacks in network. In our daily life the network has become a huge part , so the need of security also increases. From small business to large business everything is running through network only. Even though there are certain attacks plays a vital role , like sending and receiving of email , transmission of packets using TCP and UDP in client server environment and tracing the acknowledgement of packet reaching the source and destination can be done efficiently and effectively using network security. In today's world if network security did not exists the transaction in the real time also affects lot like large amount of fund transactions also takes place in the network, it should be secured. The small vulnerabilities in the network will make a disaster effect. This computer network security is complicated issues, even though we have so many solutions to overcome this problem but also we cannot achieve the full result. In order to increase a secure way of networking we have to find a new method which will solve the security problem.

REFERRENCES

[1] Kartikey Agarwal, Dr. Sanjay Kumar Dubey .,August 2014 ,Network Security : Attacks and Defenc ,International Journal of Advance Foundation and Research in Science & Engineering 1(3).

[2] JaykumarShantilal Patel1 , Vijaykumar M. Chavda., 2014 , Security Vulnerability and Robust Security Requirements using Key Management in Sensor Network, International Journal of Grid Distribution Computing.7(3),pp.23-28

[3] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and KashifNaseer Qureshi, 2014, Security Issues and Attacks in Wireless Sensor Network ,World Applied Sciences Journal 30 (10), 1224-1227

[4] Chang-Su Moon1and Sun-Hyung Kim Dept. of Information & Communication Eng., Graduate Soonchunhyang Univ., Chungna, 2014, A Study on the Integrated Security System based Real-time Network Packet Deep Inspection, International Journal of Security and Its Applications ,8(1) ,pp.113-122.

[5] Sujata Tambat, VaibhavNarkhede, Buldana, Overview on Network Security, International Journal of Advent Research in Computer and Electronics , Special Issue National Conference "CONVERGENCE 2015", 28 March 2015

[6] Rajesh Pant1, CN Khairnar, April 2014, A Cumulative Security Metric for an Information Network, International Journal of Application or Innovation in Engineering & Management ,3(4),

[7] Ailin Zeng Shunde Polytechnic, Foshan, Guangdong, China , 2014, Discussion and research of computer network security, Journal of Chemical and Pharmaceutical Research, , 6(7), pp.780-783

[8] Priyanka Goyal, Gaurav Sharma and Shivpratap Singh Kushwah , 2015 ,Network Security: A Survey Paper on Playfair Cipher and its Variants, International Journal of Urban Design for Ubiquitous Computing,3(1)

[9] .L.Devi,.S.P.Shantharajah,"A survey on authentication and security maintenance in wireless sensor network, Available Online at www.ijcsmc.com International Journal of Computer Science and Mobile Computing ,4(5),pg.53 – 70

[10] Y.M.Wara D. Singh. June 2015,A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN) , 8(2)

[11] Jing Li College of Information Engineering, Qingdao University, Qingdao Shandong 266071, China ,The Research and Application of Multi-Firewall Technology in Enterprise Network Security, International Journal of Security and Its Applications, 9(5)pp. 153-162

[12] XiangdongCai Harbin University of Science and Technology, Harbin, 2015,Network Security Threat Situation Evaluation Based on Fusion Decision and Spread Analysis, International Journal of Security and Its Applications 9(3) ,pp. 383-388

[13] D. Acemoglu, 2013,Network Security And Contagion, National Bureau Of Economic Research,

[14] R. K. Khalil, 2010 ,A Study of Network Security Systems, International Journal of Computer Science and Network Security,

[15] D. Martins and H. Guyennet,2010 Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey, 13th International Conference on Network-Based Information Systems.

[16] A. Cooper , E.Llans, 2012, Adoption of Traffic Sniffing Standard Fans WCIT Flames, Center for Democracy & Technology.