A Study of Attack and Defense in Computer Network

Richa Pandey[1], S.P Sah[2]
[1, 2] Department of Computer Science
[1, 2] Graphic Era Hill University

Abstract- *Network Security is the way of providing security when we are using network. In today's world there is a serious need for security as many vulnerable crimes are taking place.*

So, there is a need of providing security for all the clients who are accessing internet. In this paper I want to show some light on the various types of attack and defense in network security.

Keywords- DOS attacks, Firewalls, Encryption, Port Scanning, SSL, VPN.

I. INTRODUCTION

Network security means saving the websites domains or servers from various types of attack.

Network security is very important in every field such as military, government and in surfing. If we have proper knowledge of providing security then we are able to save ourselves from attack.

The earlier architecture must change so as to provide better safety over network. Firewalls are used for providing security in systems. There are many threats in internet world for stealing the security of the user whether they are using e mail service, chatting over internet. Many defense methods are introduced over times to provide security.

II. DIFFERENT TYPES OF SECURITY ATTACKS

A. Passive Attacks

This type of attacks includes attempts to break the system using observed data. In this attack an adversary deploys a sniffer tool and waits for sensitive information to be capture.

Properties of passive attacks are as follows:

1. Interception: The data between network can be easily sniffed and the confidentiality of the user is such as eavesdropping, "Man in the middle" attacks.

2. Traffic analysis: The network can be easily observed and the packed passing can be monitored.

B. Active Attacks

In active attack the attacker sends data stream to parties involved or he can also completely cut off the data stream. In this attack the adversary does not wait for sensitive or authentication information. Its attributes are as follows:

· **Interruption:** It does not allow an authenticated user form accessing the website. It attacks availability like in DOS

· **Modification:** In modification the content is changed. It attacks integrity.

· **Fabrication:** It makes counterfeit items on a network without proper authorization. It attacks authentication.

C. DOS Attack

DOS attacks in today's world have become a major threat to network security. It can be easily done by anyone who has the knowledge of the network. The attacker can Shutdown the network by overflowing it by requests and thus affecting the availability. Trinoo is a network tool which is easily available in internet the attacker can download it and use for DOS attack.

III. DEFENSE AGAINST NETWORK ATTACKS

A system which is vulnerable to attack due to fault and faulty programming.

However this cannot prevent most of the attacks, to prevent them, the network requires configuration such as:

A. Configuration Management

For protecting a system a firewall is needed when a network setup is completed all its default logins, Ids, address must be changed as soon as possible as all these information as it is available in the internet. Anyone can use the default login to use the network for intentions which may not be good. There should not be any security holes. There are many tools available in the internet for helping in configuration management.

B. Firewalls

Firewalls are very popular tool for network security this is the wall in the form of barrier which stands between the local network and the internet and filters the traffic ads. There are three different types of firewalls depending on filtering at the IP level, Packet level or at the TCP or application level [11].Firewalls helps the user from the unauthorized access. It notifies the user when an entrusted application is requested access to the internet. It also maintains logs. This log can be very harmful in case of any hacking. Firewalls only works if they are correctly configured, if some mistake is there then hacker can easily enter the system of the user.

The best thing while configuring firewall is to deny anything that is not allowed [12].

C. Encryption

Encryption methods one can prevent the hacker to get the useful information. HTTPS or SHTTP during the transmission of data between the client and user can be use to prevent Man in the middle attack. Sniffing and eavesdropping can also be prevented. VPN can be used to encrypt all the data in the network it also helps in getting privacy. Encrypting data takes processing power from the CPU. This in turn reduces the speed at which data can be send, the stronger the encryption the more time it takes [13].

D. Defense against DOS Attacks

In DOS attack intrusion detection systems (IDSs), firewalls and enhanced routers are used. The monitoring of the connections is done. They have traffic analysis, access control, redundancy built into them [15].IDSs maintains log of both the incoming and outgoing connections.

E. Vulnerability Testing

For prevention of any attacks on the network one must know about any open vulnerability in the network and stop them. Open port, faulty and outdated software with known vulnerabilities, outdated firewall. There are different tools available which allows a user to test network security and also find vulnerabilities in a network [4]. One of the methods is using a port scanner which can be used to probe a server and find any open ports. This is used by many admits to verify policies of their servers and also can be used by attackers on a network to find exploits in them. Some of the tools which are available for free on the internet are N map, Super Scan. These tools can be downloaded by everyone and each comes with a detailed tutorial for using them [16].

IV. TOP NETWORK ATTACK IN 2015

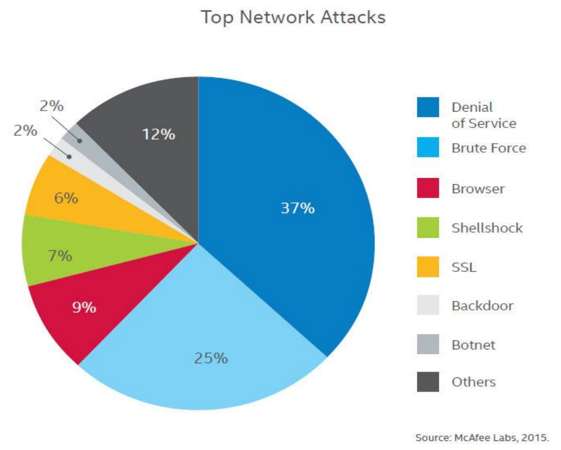

Fig: Top attacks in 2015[18]

1. Denial of service attacks – 37%

A denial of service (DOS) attack attempts to make a resource, such as a web server, unavailable to users. These attacks are very common, accounting for more than one-third of all network attacks reviewed in the report.

Distributed denial of service (D Dos) attacks is popular today. This approach uses automation for distributing the task to a number of computers. The computers are flooded with messages without the knowledge of the owner. These network attacks are spreading very rapidly every year and some send more than 100 G bps at peak.

2. Brute force attacks – 25%

Brute force attack is a trial-and-error attempt to guess a system’s password. One in four network attacks is a brute-force attempt. Automated software is often used to guess hundreds or thousands of password combinations. For prevention of attack one of the simplest methods is to lock accounts after a number of login attempts. Blocking IP addresses after multiple login failures is another. The user can restrict login access to certain IP addresses.

3. Browser attacks – 9%

Browser-based attacks target end users who are using the internet. The attacker can attract the user for downloading the software which is malicious.

One of the best ways to avoid browser-based network attacks is to regularly update web browsers and browser-related services such as Java and Flash...

4. Shellshock attacks – 7%

“Shellshock” refers to vulnerabilities found in Bash, a common command-line shell for Linux and UNIX systems. When security researchers disclose shellock in Sept. 2014, millions of systems and appliances – from web servers to thermostats – were vulnerable. Attackers have since started exploiting the errors using them to install malware that sends spam campaigns and DDoS attacks. As, many systems are never updated the vulnerabilities are present across the Web..

5. SSL attacks – 6%

SSL attacks aim to intercept data that is sent over an encrypted connection SSL attacks were more popular in late 2014, but they remain prominent today, accounting for 6% of all network attacks analyzed.

A certain rise in SSL attacks followed the disclosure last year of several security vulnerabilities in SSL and TLS, including the POODLE attack.

All versions of SSL (1.0 – 3.0) and TLS 1.0 encryption protocols are considered to be vulnerable to attack and should be avoided.

6. Backdoor attacks – 2%

A backdoor is a type of attack that bypasses normal authentication to allow remote access. Backdoors may be present in software by design.

7. Botnet attacks – 2%

A botnet is a group of hijacked computers that are controlled remotely by one or more malicious actors. Launching DDoS attacks, to sending out spam email, to practicing click-fraud, attackers use botnets for their dirty work.

V. RECENT ADVANCES IN NETWORK SECURITY

Earlier when the internet became popular and common, intrusion detection means detection of an unauthorized access in the system but this meaning reformed with the advent of Covered worm and its variants in the year 2001. These were 1st generation worm they had high spread in the sys A real-time and an automated system These worms generated high traffic especially on Port 80, so there was a need for finding the approach to correct it. Network security is Being improved in two fields namely hardware and security in the following ways:

A. Hardware Development

The field of hardware development is not growing in comparison to software development. Biometric systems and smartcards have lesser the number of unauthorized accesses. Biometric is very useful in the field of the network security, Biometric scanner attached to a workstation can be used as an authentication mechanism which can be used as a login to the system, since two persons cannot have the same biometrics as the both persons, it is a full proof mechanism of login [1].Users tend to forget their passwords it can be easily avoided by the use of biometrics

B. Software Developments

The software field is very vast when it comes to network security. It includes firewall, antivirus, VPN, intrusion detection, and many much more. There are still many areas for improvement. When new virus is introduced the new ways for detection and corrections are also found.

Currently research is being focused on neural networks for face recognition software. Most current algorithms require substantial processing power. This power cannot be available in small devices like sensors. Therefore, one must develop light weight Algorithms to counter this problem [1].

Antivirus works on a very simple principle, they scan a file, matches its digital signature against the known malwares. If the signature is match in the database it reports it, delete it or even disinfect it depending on the user’s setting. This system is easy but more vulnerable to attack as the former antivirus does not know about the new virus. To prevent this antivirus companies introduced a new system called cloud scanning this way not only wills the digital signature be scanned across the database but also across millions of computers and servers across the world.

VI. FUTURE RELEVENCE

For the betterment of the safety purpose in the network security the antivirus must be update and there configuration must be more dynamic. In case of firewall the new definitions must b taken into consideration as attackers have new techniques for attacking the system.

The client must be sure about the confidentiality of the information that they are sharing on the internet. Network security is very crucial in day to day life.

VII. CONCLUSION

In the today's world most of the work is done on internet, so there is a need for user to know about the attacks in the network security and the way of prevention. The attackers use different techniques for attacking the security of the users. The main aspects such as intregity, authentication, and availability must be ensured for the client. There are latest developments in the security area which must be updates. As attackers are ready with the new techniques the defending techniques should also get completed.

REFERENCES

[1] B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[2] Li CHEN, Web Security: Theory and Applications, School of Software, Sun Yat-sen University, China.

[3] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

[4] A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

[5] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009

[6] M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.

[7] R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.

[8] Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.

[9] M. A. Shibli, "MagicNET: Human Immune System & Network Security," IJCSNS International Journal of Computer Science and Network Security, Vol.9 No.1, January 2009.

[10] M. Silva, "Virtual Forensics: Social Network Security Solutions," Proceedings of Student Research Day, CSIS, Pace University, 2009.

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

[12] S. Alabady, "Design and Implementation of a Network Security," Technology, Vol. 1, p. 11, 2009.

[13] B. Preneel, "Cryptography for Network Security," Katholieke Universities Leuven and IBBT, 2009.

[14] M. Kassim, "An Analysis on Bandwidth Utilization and Traffic Pattern," IACSIT Press, 2011.

[15] M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology, 2011.

[16] D. Acemoglu, "Network Security and Contagion," NATIONAL BUREAU OF ECONOMIC RESEARCH, 2013.

[17] S. Shaji, "Anti Phishing Approach Using Visual Cryptography and Iris Recogn No. 3pp. 88-92, 2014.

[18] http://www.calyptix.com