Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

USING ENCRYPTION FOR NETWORK SECURITY

Saba Zaidi[1]
[1]Research Scholar, Department of computer Science & Engineering
Al-Falah School of Engineering and Technology,Dhauj -121004(Haryana), India

Abstract: Network Security is very important in today's world. It is used in military, government& our daily life's. As a result different type of methods is adopted to bypass it. Network security refers to protecting the websites domains or servers from various forms of attack. There are many type of security attack such as passive attack, active attack & DOS attack. Network administrators should to keep up with the latest advancements in both the hardware and software fields. This paper outlines different attack methods which are used, as well as different defence method against them.
Key Words: DOS attacks, Firewalls, Encryption, Port Scanning, SSL.

I. INTRODUCTION

Network security plays an important role to protect the website domain or server from different type of attacks. Network security is used in every field such as military, government & in our daily life. If we have knowledge of how attacks are executed, so we can protect ourselves. Several industries used firewall to protect themselves. It is very field in today's world .If we understand the current research we must understand the background & knowledge of working of internet .Internet is now commonly used in our houses, in our work places, mobile and almost every place is connected with internet.

Synchronous network are the network which consist of switches& so they do not buffer any data hence protection is not required .It is mainly focus on data network which are link to internet As forecasting goes for field .Email is mostly used by every person in day to day life .It is a fault that there is no system of authentication of sending and receiving the emails so authentication should be there on sending and receiving the emails .SPAM is a serious security threat it only required very less manpower but it affects million of email users

II. DIFFERENT TYPES OF SECURITY ATTACKS

There are many types of security attacks such as Active attack, Passive attack and DOS attack.

a) ACTIVE ATTACK : In this type of attack the attacker send data stream to one or both the parties who are involved in it or totally cut of the data stream.

b) PASIVE ATTACK: This kind of attack it is used to break the system using observed data. Example: plain text attack in which plain text and cipher text known to attacker

c) DOS ATTACK: DOS attack is one of the major threats of network security in today's world .This type of attack can launched easily. Anybody can launch it with basic knowledge of network security.

It doesn't require much time and any kind of planning. They are cheap and efficient method of attacking networks with the help of Trinoo that is easily downloaded by the internet.

A. Different Types of DOS Attacks:

For disable services many attacks perform DOS attack .Whenever client want to connect the server, firstly client send SYN message to the server .server than respond to the client by sending SYN – ACK message to the client .Then again client complete the connection by sending an ACK message. Now connection is established now data can be easily transferred .When connection is half open

problem occurs then server waits for client to ACK message .Server will wait till expiry date .When person exploiting the server will never send ACK message so they keep on sending new connection demand ,till the server is overloaded thus cannot provide to access.

d) Type of network security:

The Different type of network security is as follow:

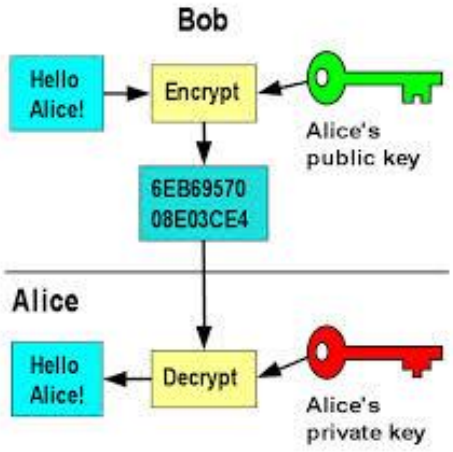
1] Security by obscurity
2] Perimeter Defence
3] Defence in depth

III. DEFENCE AGAINST NETWORK ATTACKS

Configuration management

Configuration management is a crucial part of defence against network attack. It is as much important as decent firewall to protect the system .so when the network setup is completed its default login, address; Id's is changed as soon as possible all information is available on the internet so any one can view.

Encryption:



"Figure 1.Encryption"

It is a method in which data is first written in plain text then it is converted in a cipher text then again it is converted in a plain text .In this process encoded information or message can read only by authorised party. There are two type of encryption first is symmetric key encryption second one is asymmetric key encryption

Firewall: Firewall is a wall that is lie between local network and internet & filters the traffic. It helps in preventing not authorised network traffic from unsecure network to private network .Firewall is most popular security tool in the market There are three different type of firewall IP level, Packet level or at TCP or at Application level .All these are depend on filtering. It always remind the user when some un trusted application is requested access to the internet. They minimise the speed of network performance because it examine both incoming and outgoing traffic.

IV. ENCRYPTING THE WORLD WIDE WEB (WWW)

Privacy is a important part in world wide web. Encryption is used in web to reduce the number of attacks .The important way of encryption is SSL protocol.

Secure socket layer: A secure connection is established between browser and server when SSL is used in a browser. It is like a tunnel in which data can flow easily in a secure manner. The session starts with asymmetric encryption. The server then sends the client its public key. After the

asymmetric connection both the sides switches to a symmetric connection. Asymmetric algorithms much slow and uses much more CPU power than symmetric ones. In symmetric encryption, CPU load is high; servers can only handle a fraction of connections as compared to servers with no encryption.

V. CONCLUSION

Internet is very useful part of our daily life, so network security also very important issue in today's world .Now a day's more users and criminals connect to internet .Many transaction are done over internet .A single mistake can affect a company .If company records are leaked ,user data such as banking details and credit card details are at risk. Many different type of software such as intrusion detection can prevent these attacks but sometimes it is due to human mistake so these attacks can occur some attacks can be easily prevented. Researcher across the world is finding new methods to prevent them.

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] Simmonds, A; Sandilands, P; van Ekert, L (2004). *"An Ontology for Network Security Attacks"*. *Lecture Notes* in Computer Science. Lecture Notes in Computer Science 3285: 317–323.doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.
[6]A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco
[7]DaveDittrich, Network /Intrusion Detection Systems (IDS), University of Washington.
[8].Honeypots.net.2007-05-26. Retrieved 2011-12-09.
[9]Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
[10] 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

