EUROPEAN ACADEMIC RESEARCH
Vol. IV, Issue 12/ March 2017

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Review Paper on Network Security Attacks and Defence

ALLYSA ASHLEY M. PALAMING
College of Computer Studies
Masters in Information Technology (MIT)
Tarlac State University

Abstract:

It was also mentioned in the paper the properties of passive attacks as follows: (a) interception – the data passing through a network can be easily sniffed and thus attacking the confidentiality of the user, such as eavesdropping, "Man in the middle" attacks; (b) traffic analysis it attacks confidentiality, which include trace back on a network like a CRT radiation. In this report most of the basic information regarding network security will be outlined such as finding and closing vulnerabilities and preventing network attacks and also security measures currently being used.

The perimeter defense works in an organization that harden the network security by using tools such as hiding the network behind a firewall, separating the network from an untrusted network. There was a thorough discussion on the different types of network security are as follows: the security by obscurity, the perimeter defense, and defense in depth. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. The security by obscurity works on stealth approach.

There are numerous advancements that are being made in the field of network security both in the field of hardware and software, it's a continuous improvement between network security analyst and crackers and as the demand of internet shows no signs of decreasing its development. Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of network

security. As internet has become a huge part of the daily life, the need of network security has also increased exponentially from the last decade.

Finally, network security is being improved in two fields namely hardware and security in the following ways: The hardware development in this field is not developing very rapidly as its software counterpart but nonetheless some amazing developments are being made such as using biometric systems and smartcards which can drastically reduce the number of unauthorized access. The software developments the software field is very wide when it comes to network security. Firewalls help preventing unauthorized network traffic through an unsecured network to a private network.

Key words: network security, attack, network management, wireless sensor, network

I. INTRODUCTION

Network security refers to protecting the websites domains or servers from various forms of attack. Network security is important in every field of today's world such as military, government and even in our daily lives. Having the knowledge of how the attacks are executed we can better protect ourselves. A network consists of routers from which information can be easily stolen by the use of malwares such as a "Trojan Horses". The synchronous network consists of switches and since they do not buffer any data and hence are not required to be protected.

Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. As forecasting goes for the field of the network security it can be said that some new trends are emerging some are based on old ideas such as biometric scanning while others are completely new and revolutionary.

In this report most of the basic information regarding network security will be outlined such as finding and closing

vulnerabilities and preventing network attacks and also security measures currently being used.

II. REVIEW AND ANALYSIS

In this paper the authors discussed the different types of security attacks such as the passive attacks, active attacks and DOS attack. They describe that passive attack includes attempts to break the system using observed data. One of its examples is plain text attack, where both the plain text and cipher text are already known to the attacker. It was also mentioned in paper the properties of passive attacks as follows: (a) interception – the data passing through a network can be easily sniffed and thus attacking the confidentiality of the user, such as eavesdropping, "Man in the middle" attacks; (b) traffic analysis it attacks confidentiality, which include trace back on a network like a CRT radiation.

Furthermore, active attacks described in the paper that the attacker sends data stream to one or both the parties involved or he can also completely cut off the data stream. Its attributes are as follows: (a) interruption – which prevents an authenticated user form accessing the site. It attacks availability such as DOS attacks; (b) modification – in this the data is modified mostly during transmission. It attacks integrity; and (c) fabrication – which is the creating counterfeit items on a network without proper authorization. It attacks authentication.

Moreover, the authors explained that DOS attack today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. Many attacks are used to perform a DOS attack so as to disable service. Some of which are as follows: TCP SYN Flooding - ICMP Smurf Flooding: ICMP package is used to know whether the server is responding or not. The server replies with an ICMP echo

command. In smurf attack the attacking host forges the ICMP echo requests having victims address as the source and the broadcast address of remote networks. The UDP Flooding many networks now use TCP and ICMP protocols to prevent DOS attacks but a hacker can send large number of packages as UDP overloading the victim and preventing any new connection.

There was a thorough discussion on the different types of network security are as follows: the security by obscurity, the perimeter defense, and defense in depth. The security by obscurity works on stealth approach. Its basic working principle is that if no one knows the system exists then it won't be attacked. The perimeter defense works in an organization that harden the network security by using tools such as hiding the network behind a firewall, separating the network from an untrusted network. This method does nothing to stop an attack from inside. The defense in depth is the best way to protect the system but also very difficult to implement. In this each system is hardened and is monitored thus acting like an island and it defends itself against the attacks.

However this cannot prevent most of the attacks, and to prevent them, the network requires configurations such as: configuration management it is as important as having a descent firewall to protect the system. As soon as a network setup is completed all its default logins, ids, address must be changed as soon as possible as all these information is available on the internet for anyone to view. The firewalls it is the most widely sold and available network security tool available in the market. This is the wall which stands between the local network and the internet and filters the traffic ad prevents most of the network attacks. There are three different types of firewalls depending on filtering at the IP level, Packet level or at the TCP or application level.

Firewalls help preventing unauthorized network traffic through an unsecured network to a private network. Firewalls

only work if they are correctly configured, if somebody makes a mistake while configuring the firewall, it may allow unauthorized to enter or leave the system. Firewall also reduces the speed of network performance as it examines both incoming and outgoing traffic. Firewall does not manage any internal traffic where most of the attacks come from. Many companies are under false assumptions, that by just using a firewall they are safe, but the truth is they are not, firewall can be easily be circumvented. In the encryption methods one can prevent hacker listening onto the data because without the right key it will just be garbage to them. Different encryption method such as using HTTPS or SHTTP during the transmission of data between the client and user, will prevent Man in the middle attack (MIM), this will also prevent any sniffing of data and thus any eavesdropping.

In defense against DOS attacks there are many technologies have been developed such as intrusion detection systems (IDSs), firewalls, and enhanced routers. These things are used between the internet and servers. They monitor incoming connections as well as outgoing connections and automatically take steps to protect the network. They have traffic analysis, access control, redundancy built into them.

In the vulnerability testing one must find any open vulnerabilities in the network and close them, these may include open ports and also faulty and outdated software with known vulnerabilities, outdated firewall rules.

For the sake of privacy, confidentiality and availability the communications on the web should always be encrypted this reduces the number of attacks and prevents anyone to view the ongoing transmissions. Using this mechanism can spread resources and prevent dependent on one system. The secure sockets layer it uses both asymmetric and symmetric keys encryption transfer data in a secure mode over a network. When SSL is used in a browser it established a secure connection between the browser and the server. The secure

HTTP (SHTTP) it is an alternative to HTTPS, it has the same working as HTTPS and is designed to secure web pages and their messages. There are differences between SHTTP and SSL protocol such as SSl is a connection oriented protocol and it works it transport level by providing a secure tunnel for transmission whereas SHTTP works on application level and each message is encrypted separately, but secure tunnel is created. The VPN (Virtual Private Network) is a way to transport traffic on an unsecured network. It uses a combination of encrypting, authentication and tunnelling. The most known and used protocols are as follows: (a) point-to-point tunnelling, (b) protocol (PPTP), (c) layer 2 tunnelling protocol (L2TP), (d) internet protocol security (IPsec) and (e) SOCKS.

The e-mail security as both the sender and receiver of the email one must be concerned about the sensitivity of the information in the mail, it being viewed by unauthorized users, being modified in the middle or in the storage. Email can be easily counterfeit therefore one must always authenticate its source. E-mail can also be used as a delivery mechanism for viruses.

Finally, network security is being improved in two fields namely hardware and security in the following ways: The hardware development in this field is not developing very rapidly as its software counterpart but nonetheless some amazing developments are being made such as using biometric systems and smartcards which can drastically reduce the number of unauthorized access. The software developments the software field is very wide when it comes to network security. It includes firewall, antivirus, VPN, intrusion detection, and many much more. The improvement of network security is basically still the same. When new viruses are found virus definitions are updated, it's the same for firewalls instead their rules are updated.

III. RECAPITULATION AND CONCLUSION

As internet has become a huge part of our daily life, the need of network security has also increased exponentially from the last decade. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of network security. Most of the attacks can be easily prevented, by following many simply methods as outlined by the authors in this paper. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them. There are numerous advancements that are being made in the field of network security both in the field of hardware and software, it's a continuous improvement between network security analyst and crackers and as the demand of internet shows no signs of decreasing its development.

IV. 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 Universiteit 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 Recognition. No. 3pp. 88-92, 2014.