Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Network Security Analysis Based on Digital Automation and Software Installation Techniques

Deepak Shrivastava*, Vimal Shukla
Cyber Security/Cyber Forensic
KNP College of Science & Technology, Bhopal,India,
RGPV, Bhopal, India

Abstract*— Information security is an important and critical component that ensures safe and secure transmission of information through the internet network. In computer networking the term firewall is not only shows expression of a general idea, but it can also means for proper and perfect things. The firewall already keeps path of every file that was entering or leaving the network in order to sense the source of viruses and other problems that may affect the network. Network Security is an unique, efficient and beneficial part in the management of network. Mostly many organizations around the world spend millions of revenue in every year for the safety and provide security regarding valuable corporate form of data's and information. Various companies are using firewalls and encryption mechanisms as a security measure. Authors, those are working on this ensuring a base of study to sense port and Security analysis of hostile viral penetration, authentication packet, DDOS network system, terminal mobile WiBro, a HTS program etc .All these various types of analysis was in order to open by the use of the scanning process that used NetScan Tools, is to analyze, and generate Forensic form of information, regarding which Author was tried to used this, as for its criminal investigation and legal form of data.

Keywords*— Viral Perforation analysis, Criminal exploration, judicial data format, Forensic information.

I. INTRODUCTION

Due to the presence of public network, significant security threats can be beneficial and efficient form to an individual's personal part of information and also to the resources of companies and government. It is Providing security in terms of confidential system, maintaining integrity and assuring the opportunity of correct format of data or information that is the primary objective of the security system.These threats are basically generated at present due to the [1]ignorance shown by the users, weak and low based form technology and poor design of the network. Sometimes there are many network services that are activated in its own by default in a personal computer or a router. Out of which many services are either not be important or beneficial and may be used by an striker for information gathering. So it is the better option to de-active these unneccesary services to protect them from hackers and strikers. [2]More importantly,this thing not only need to be concerned regarding the security at each point of the network rather than the focus should be on securing the entire network.

Computer security is an indestructible form of problem. Security on the network based computers is much also in an indestructible form.But if the machine is connected to a network system , the situation is becoming much complicated and the network security is in the network information security [3-7]. Wireless Sensor Network (WSN) is a novel idea that deploys large scale of sensor nodes into present environments and use RF to communicate and collect information from nodes.There are various applications of WSN that include monitoring, tracking, and position controlling[8].Basically,RSSI (Received Signal Strength Indicator) values are directly proportional to the distance between badge and beacons, the greatest value of RSSI should be received from the nearest beacon, without any interference.Hence,the location of beacon with maximum RSSI value can be assigned as the location of the badge and user. However, the interferences can takes place from devices, surrounding environment, and others RF signals are unreliabilities in positioning.[9-11]Some regulations are also used for obtaining stable RSSI values have to apply in proper position algorithm to ensure accurate performance of positioning results. The regulations are created by practical measurement and testing processes, after all devices have been located.

Academic and commercial research [13-15]efforts can be done in the field of network security is leading towards the development of an appropriate secure technology. The structure of the Internet itself, has not been used without any fault, presenting a security threats not only from external, but also from within the network.Typical network strike consists of eavesdropping, Denial-of-Service, buffer overflow and Injection of Structured Query Language.These type of strikes may results in a simple identity theft to misplacement of lives.Many companies are using encryption mechanisms and firewalls as a security measure to ensure security. There are various types of firewalls and encryption mechanisms are available in the market. Out of them only some of them are suitable for small companies such as the Small and Medium Enterprises (SMEs). For SMEs, these type of applications might be an overkill, both financially as well as functionally. As such, this study aims to propose the design of a network security based tool on an open-source applications for

SMEs. Recently a financial transaction value which leads to the carrying Internet which uses WiBro networks is activated for the government ,the security company and the bank ,financial institution etc. There must be a inevitably which will be analyzing the security vulnerability due to which the financial transactions which leads WiBro carrying Internet and it prepares in financial accident. The security vulnerability of mobile stock trading from WiBro, it must analyze forensic fundamental data that must created and the stability and a security characteristic measure of financial transactions from the carrying Internet can be approach later on. It should secure the reliability and security stability could be guaranteed in our country finance IT ,which is an Information Technology super high speed Internet used for the robust country. From the author point of view ,importance and objective with the scope of WiBro research carrying Internet networks, mobile HTS, it also enquire mobile HTS utilized for transactions analyzes, WiBro mobile HTS programs. The financial transaction hackings and phishing presenting conditions of recent times. Author analyzes experimental surrounding environments and stock trading network and susceptibility stock trading contents and WiBro mobile stocks vulnerabilities from WiBro mobile HTS vulnerability analysis experiments. Author analyzes on strike and forensic information lifestyle rime,it stands in about Wibro mobile stock trading systems and also present in virus diffuse throughout attack and authentication packet. HTS is groove trading with home trading system. The investor goes to the security company, or, it does not use a transformation not to be, it is a system which puts out the
direct stockjobbing order to use the computer from the family or job.On-line leads in single word and it is a system stockjobbing. HTS programs in PDA and the screen which it executes it made. WiBro networks it leads and the stock trading whole aspect PDA it leads and market conditions, quotient,securities news and quick time etc. securities pertinent information as a real-time it confirms and the users are safe and conveniently, one card it does not stand it uses an user authentication function and a annexed service.

KT login of separate way without the current price and information confirmation are possible with WiBro whole aspect terminals. There is a stockjobbing function and a CMA variant function and the quick upload speed and service charge are cheap. The service possible area is the Seoul former area, the capital region and the condition part area, service use method login of separate way without the current price and information confirmation are possible with KT WiBro whole aspect terminals [8]. According to National Intelligence Service 2006 phishing instance 1226th case middle bank and theinsurance company etc. financial relation agency 871st case, the transactions sites which go round with 68.8% are becoming target of hacking. The electronic transaction enterprise one phishing degree 380th case (30%) it rises in the object.The National Intelligence Service in order to close phishing damage presented a real site and the imitation site distinction law. The normal site payment account input is not a necessity and when login doing, the separate way screen floats and when pressing the inquiry button, becomes the balance indication and it is to be a normal site (phishing sites the balance inquiry being not right)[13].It used a connection system above gateway system and WiBro base stations were located within 200m and within the building from WiBro repeaters from within 1~2m scopes above reception rate 90% upload 1Mbps, they experimented from the place it will be able to maintain the speed of download 2.5~2.8Mbps. A project, called Active Campus, is done at University of California, San Diego, which provides an infrastructure that focuses on integrating location based on the services for academic communities.[5].The study provides an outdoor kid's safety care context based architecture using space oriented concepts and contexts.House_n [7] at Massachusetts Institute of Technology (MIT) explores to design Home and its relevant technologies, products, and services to evolve and to meet the challenging opportunities of the future.Smart homes [8] generates a numerous demonstrations for elders or people with health problems, providing assistive technologies and safety aids such as video-intercom system and motion sensors are used for lighting control, and emergency buttons for elders. So, we have try to locate information into the community to provide extra services and benefits which makes the scenario a complete profile.

II. LITERATURE REVIEW

[1]Anupriya Shrivastava, M A Rizvi, "RESEARCH ARTICLE Network Security Analysis Based on Authentication Techniques ". The target of Network security not only requires ensuring the security of end systems but of the whole entire network. Authentication is one of the most primary and commonly ways of ascertaining and ensuring security in the network. An attempt has been made by the author to analyze the various authentication techniques such as Knowledge-based, Token- based and Biometric-based etc. The user has to be use authentication technique depending as per requirement. Password based technique is best one, if you have to remember a single password. But the problem takes place ,when we have to remember many passwords ,in that case we use those passwords that are easy to remember or keep in mind easily. Token based techniques provide added features such as security against denial of service (DoS) attacks. In comparison of above two, techniques biometric cannot be stolen easily, hence it provides stronger protection.

[2].Miss. Shwetambari G. Pundkar, Prof. Dr. G. R. Bamnote, "RESEARCH ARTICLE ANALYSIS OF FIREWALL TECHNOLOGY IN COMPUTER NETWORK SECURITY". Design of Network Security Tool presents a design for Network Defender, specially a network security tool. Network Defender is consist of four components namely Firewall, Network Intrusion Detection, Vulnerability Scanner and Exploit Tool. Firewall is a software or hardware-based network security system that controls incoming and outgoing traffic by analyzing data packets. Firewall determines which traffic should be allowed to pass or rejected, based on a set of rules that must be follow properly. It also creates a barrier between a trusted and secure, internal network and other outer networks. Network Intrusion Detection System (NIDS) is a system that attempts to discover unauthorized access to a computer network by analyzing traffic for signs of malicious activity ("Network Intrusion Detection System," 2013). Vulnerability Scanner is a computer program designed to assess computers, systems, networks or applications for its weaknesses. There are several types of scanners found in literature, based on focus and particular targets. While their function varies for different types of scanners, they share a common,

core purpose of enumerating vulnerabilities in one or more targets. Exploit Tool is used for developing and executing exploit code against a remote target .[13-17].T Yamakami, T ACCESS, "MobileWeb 2.0: Lessons from Web 2.0 and Past Mobile Internet Development," By the Use WiBro, from mobile stock trading which networks VM from mobile communication terminals, downloading transactions stock company name and account number, after putting the account information of account ID and account password etc. from web, mobile communication terminal crossroad, it transmits and also stores in account DB of mobile communication terminals the phase which it passesd by. In the Mobile stock trading system terminals AccessPoint lead from communication phase and with wired-network connection, scanning it under they lead and AccessPoint hishing .Data fishing pulls out the general Email dispatch,it is the first phase private with intention. Phishing Mail the users approach with a social engineering methodology which 'Change the password, When answer back within 24 hours, the account stands still.' etc. and is linked in Email the internet address which to under click they make. [3-10]. Real Secure uses SSH connection and provides inspection against incoming network traffic. It has a powerful log monitoring capability, due to which it can scans the log files and search for known text patterns or rules ("IBM Internet Security Systems," 2013). Once a proper possible attack is detected, it sends out an alert message either to an individual or another system, such that problem can be cleared out in short period of time. Real Secure Server Sensor pre-emotively combats threats and addresses vulnerabilities at the network level while performing security compliance auditing. Real Secure Server Sensor protects against network vector attacks including worms, boot worms, Trojans and Denial-of-Service attacks through a local firewall and inline vulnerability-centric intrusion prevention. This system has two main components: a) Network Intrusion Detection b) Firewall. Adware's Attack Mitigation System (AMS) is a real-time network and application attack mitigation that protects the application infrastructure against network and application downtime, application vulnerability exploitation, malware spread, regarding information theft, web service attacks and web defacement ("Radware," 2013). This system includes four basic components: Network Behavioral Analysis, Intrusion Prevention System, Reputation Engine and Web Application Firewall, which can be classified as Firewall and Netwok Intrusion Detection.

III. METHOD

Several methods has used,some of them are listed below:

[A]. AUTHENTICATION TECHNIQUES: Under this authentication technique, privacy should be maintained properly.Password-based authentication techniques are used such that password policies are offering a set of rules that also have major aspect in deciding how to admin password in the systems. There are multiple policies supported by directory servers. „Default‟ and „Specialized‟ are the two of them. The default password policy is a part of the configuration for the instance, if once it was modified, it cannot be replicated again.

[B].TOKEN BASED TECHNIQUE: This is a physical form of device that performs authentication and therefore can be called as object based process. Tokens can be compared with physical keys to houses that are used as a token but in digital tokens many other factors are also present to provide information safety. In digital world, security tokens are used. Tokens themselves have password such that even if they are lost, the hackers are not able to modify the vital information. Bank cards, smart cards are fallen into the category of security token storage devices with passwords and pass codes. Pass codes are same as password except that the former are generated by machine and stored also. There exist one time security tokens and smartcards [1] can be confidentialy maintained up to some extent and proper security should be maintained by the hackers by use of the Mechanism for OTP method.

[C]. BIOMETRIC BASED: [2]This is the process of verifying if a user is whom he is claiming to be, by the use of digitized biological signatures of the user. Biometric authentication can be classified into two groups: physiological and behavioral. In the process of physiological authentication, iris, retina follow, faces, finger prints, hands. And in the case of behavioral, voice prints, signatures and keystrokes are to be used. This technique can call as ID based.

[D]. WORKING OF FIREWALL IN PC: There are several different methods in which firewalls use to filter out data, and some are used in combined form also. These methods work at not similar layers of a network, which determines how specific the filtering options can be used. Firewalls can be used up in a number of ways to add protection to your home or business. Big and large form of organizations or corporations often has very complex firewalls in place to secure their networks. On the other hand, firewalls can be configured to avoid employees from sending certain types of mails or transmitting confidential data outside of the network. A company might have to choose and select a single computer on the network for file sharing and all other computers could be controlled through it.

[E]. PEOPLE TRACKING SERVICE (PTS): People Tracking Service (PTS) provides an actual-time tracking system of the particular person wearing a badge. This service is provided for the use of family members only. On the other hand,for private issue this process can not be is in use. The exact reason behind this is that security guard in control center cannot keep its path to the information of other people other than their family members.

IV. CONCLUSIONS

All the techniques have their merit and demerits. Author have to show his smartness to choose an appropriate technique as per requirement of security of networks and information by keeping economic consideration also. The

firewall also has its own drawbacks, which does not undergo firewall's process; The protection that firewalls ensures is as good as the rule they are configured for execution. But firewall strategies are user-friendly to the network security,so that the user can handle and work easily by its beneficial way. [3-9] Canghong Zhang, Based on nework security firewall technology, Information technology, Chinese new technology new product, 2009.The system, Smart Community Security System (SCSS), provides more active and easier development than traditional community providing security monitoring services.The Centralized form of database and SMS alerts used for better equipped Network Defending against Hacker attacks. It is analyzed that the study has provided a cheaper alternative measure to SMEs in securing their network researches from the carrying Internet WiBro which is used at that time for securing the stability and efficiency that possess a characteristic measure for security method and financial transactions among users.

REFERENCES

[1] Anupriya Shrivastava, M A Rizvi, "RESEARCH ARTICLE Network Security Analysis Based on Authentication Techniques ". A Monthly Journal of Computer Science and Information Technology .ISSN 2320–088X ,IJCSMC, Vol. 3, Issue. 6, June 2014, pg.11 – 18. A Monthly Journal of Computer Science and Information Technology.

[2] Miss. Shwetambari G. Pundkar, Prof. Dr. G. R. Bamnote, "RESEARCH ARTICLE ANALYSIS OF FIREWALL TECHNOLOGY IN COMPUTER NETWORK SECURITY" .ISSN 2320–088X ,IJCSMC, Vol. 3, Issue. 4, April 2014, pg.841 – 846.

[3] A. Wool, "A quantitative study of firewall configuration errors," Computer, vol. no. 6,2004.

[4] Wireless Sensor Network at WiKi, http://en.wikipedia.org/wiki/Wireless_sensor_network .

[5] ZigBee at Wiki, http://en.wikipedia.org/wiki/ZigBee

[6] ZigBee Alliance. http://www.zigbee.org/

[7] III AMTC ZigBee, http://zigbee.iii.org.tw/en/IZSSC.php

[8] Canghong Zhang, Based on nework security firewall technology,Information technology,Chinese new technology new product, 2009.

[9] [Online]Available: http://www.duosecurity.com.

[10] [Online]Available:http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication%2 0Technique.pdf.

[11] N. Akhyari, , Teluk Kalong, " Design of a Network Security Tool Using Open-Source Applications" .Australian Journal of Basic and Applied Science, 8(4) Special 2014, Pages: 40-46 AENSI Journals Australian Journal of Basic and Applied Sciences ISSN:1991-8178.

[12] http://web.mit.edu/~bdaya/www/Network%20Security.pdf. BSD Perimeter LLC, 2004-2011.

[13] PfSense.http://www.PfSense.org/. Firewall (computing), 2013.

[14] Woo-Sung Chun† and Dea-Woo Park†† ,"Security Vulnerability Analysis and Forensic Data Research to Attacks on Mobile Stock Trading System in WiBro Network ". Journal of Computer Science and Network Security, VOL.9 No.12, December 2009.

[15] Ki-Hwan Kim, Dea-Woo Park, "A Study on Extraction of Mobile Forensic Data and Integrity Proof", KSCI, Journal of KSCI, Vol. 12. No. 6. pp. 177-185, December 2007.

[16] W Han, Y Wang, Y Cao, J Zhou, L Wang, "Anti-Phishing by Smart Mobile Device," IFIP International Conference, Network and Parallel Computing Workshops, 2007.

[17] T Yamakami, T ACCESS, "MobileWeb 2.0: Lessons from Web 2.0 and Past Mobile Internet Development," Multimedia and Ubiquitous Engineering, 2007.

