Journal of Engineering and Applied Sciences 12 (24): 7494-7500, 2017
ISSN: 1816-949X

Network Security: Internal and External Attacks

Ujjwal Sharma, Princi Sharma, Vivek Rawal and Priti Narwal
Department of Computer Science and Engineering, Manav Rachna International University,
121004 Faridabad, Haryana, India

Abstract: Network security is highly needed to protect legitimate files from unauthorized access, misuse, modification, destruction or improper disclosure. Recent activities in the field of cyber world proves that network attacks can cause huge amount of loss to governments, private enterprises and the general public in terms of money, data confidentiality and reputation. There always occurs a collision between the security specialists and the attackers frequently. In this study, we present an overview of different types of network vulnerabilities and brief discussion about preventive measures from such attacks including classification of IDS and IPS.

Key words: DDOS, SQL injection, intrusion prevention system, VPN, intrusion detection system, security

INTRODUCTION

Regular growth in population and number of users over internet put a huge task in management. Network security not only secures the users from intruders, errors and other threats but also provides flexibility, ease of use with standardized sets of protocols including confidentiality and integrity management (Daya, 2013). Common serious threats that are being faced regularly these days are SPAM content as it requires very less manpower but affect millions to billions of e-Mail users around the world wide that are connected through a network. The threats may contain harmful programs that could damage the entire system, sometimes they also refer links to false advertisements. Hackers choose drive by downloading method as a medium for attacks. A computer user can be tricked or forced to download such software onto a computer that contains a malicious content. Regular analysis of static, dynamic and code on network could help in prevention from malicious programs (Verma *et al*., 2013). Network security provides rigid features of access to authorized user, maintain confidentiality and grant permission for authentication, integrity for communication and non-rejection of received entity. Current architecture of network reveals about connection over network through a set of Internet Protocol (IP) and advanced set of protocol known as Transmission Control Protocol (TCP). These protocols establish a secure connection over network to two different host systems so that they can communicate with each other for a period of time.

Vulnearbility to files: The objective of this study is to discuss several techniques used by attackers that may hamper a machine. We first discuss viruses, then worms, Trojans and phishing.

Viruses: Viruses are malicious programs that are attached to some useful programs or mails coming from anonymous sources. It may cause severe damage to the system based on nature of virus such as modifying its programs, send infections to all listed contact through mails, continuously generate copy of the unknown files. It is quite difficult to identify an infected system as it keeps running and number of time infected program opens its effect could be maximize. Example: Chernobyl virus (CIH), Kenzero, the Melissa virus, Netsky and Sasser, etc.

Worms: Worms are subtype of viruses but the only difference is that it can communicate and spread automatically. It has a unique property of self-replication and has a tendency to damage the computer throughout. Malware such as worms causes the system to stop responding, it can decrease the speed of the computer if spread to any server it is capable that it will use more overhead to internet connection or bandwidth it may also utilize more resources. Few examples are I Love You, Conficker, Daprosy, etc.

Trojans: Trojan is the combination of virus, worms and malicious software. Trojan horses are not easy to identify as it clone itself to some meaningful applications but in returns it exploit and increase vulnerability to the system. It is used to penetrate one's security as it opens a

Corresponding Author: Ujjwal Sharma, Department of Computer Science and Engineering, Manav Rachna International University, 121004 Faridabad, Haryana, India

backdoor from where one can penetrate someone's personal information or credentials that you may not share with anyone. It can damage your computer but it depends on the software whether the damage will be serious or not. It can also change the wallpaper of your computer on its own, delete some of your useful files, add some unknown tab to your window and it can also corrupt files or memory of your computer. Example, Cryptolocker, 2013, Ransomeware, Storm worm, 2007, Shamoon, 2012, etc.

Phishing: Phishing is a type of online scam in which a user is tricked into trap through a fake login web page of legitimate organization. In most of the cases crafted link is send through emails and ask user to provide credentials information, however, the information is diverted to attacker. Recently in Jan. 2012 RBI inform about attack that was point of concern for every individual. The attacker makes a phishing page of RBI bank and misguides recipient by referring a link having prize money of worth 10 lakhs within 48 h of time period. The user was asked to provide his identity pin number and saving account number along with password.

Next, we discuss about general application that can keep us safe against malware such as antivirus and firewall. Anti-virus software is designed to cure, detect and remove malicious activities like virus, worms, Trojan, etc. These programs are made to work in collaboration with various operating systems. It performs scanning method to detect malicious programs and scanning processes could be manual or automatic. It is quite difficult to attack on a system having antivirus installed on it. Antivirus company regularly bring updates after analysing vulnerability or loop hole that could cause threat (Rad *et al*., 2011). The keen feature of antivirus is to maintain health of the system and keeps safe from all virus or malware activities. Firewall is another important network security system that monitors and controls all incoming and outgoing traffic based on define set of security rules. Firewall does not monitor over internal traffic and alteration from natural flow. It is assumed that source from outside is more dangerous as compared to inside but it's a complete wrong perception. Intruders could also produce same or greater amount of impact on the computer environment. Firewall is not only single solution for the purpose of security but it is all about TCP/IP filtration. It can be implemented in both hardware and software or a combination of both. In fact firewall works on two different layers that are network layer and application layer. Network layer firewall also known by packet filter firewall is the one who works on mutual principle of incoming packet. Incoming signal could be from anywhere, it establishes barrier between legalise copy and unknown source. Application layer blocks the incoming packets when comes from an unknown source and matches with the set of restrictions that are being blocked through firewall without any acknowledge to user. As all set of rules are not be predefined at initial time so it allows Trojan programs too. Network layer filters the source IP address, source port, destination IP address or port at which communication takes place.

MATERIALS AND METHODS

Network security vulnerability: In this study, we discuss several types of network security vulnerability that may damage your computer. First, we discuss DDOS (Distributed Denial of Service) attacks, then SQL injection, XXS (Cross Site Scripting) and brute force attack.

DDoS: DDOS (Distributed Denial of Service) attacks are the type of attacks in which multiple compromised systems which are often infected with a Trojan are used to target a single system by degrading the quality of the network's connectivity. In some cases the attacks may also deplete all the resources of the victim's computer. This attack is major trouble to the availability in which the attacker can find some bug or some weakness in the implementation of the software to disrupt the service. In this the attackers scan the network to find the machines (Zombie machines) that have some vulnerability and then they are used as agents by the attacker. In most cases, the targets can be web servers, storage, CPU and the other network resources like bandwidth which is the most common way to overwhelm a website. These attempts flood a site with external requests, making the site unavailable to the user which are initiated by a network of remotely controlled, well structured and widely dispersed nodes called Zombies. Attacker use spoofed IP addresses (Zombie machines) which are obtained by eavesdropping in which the attacker spies on the network, making difficult to trace the source of the attack by compromising the security of hosts in which host is the major factor for security on the internet. The master server holds the attack by directly communicating with handler and instructs the Zombie for attack. DDoS can be further classified as bandwidth based attack and resource based attack which consume the entire bandwidth and resources of the network that are being exploited (Deshmukh and Devadkar, 2015).

Bandwidth based attacks: These attacks utilize the whole bandwidth of the victim's computer by flooding the unwanted traffic so that the legitimate traffic do not reach

the target's network. The tools like Trino are usually used to perform these types of attacks. These attacks are further classified as flood attacks and amplification attacks. In flood attacks the attacker sends a large volume to traffic to the victim by the help of the Zombies that clogs up the victim's bandwidth with IP traffic. The system that that has been victimised undergoes a saturated network bandwidth and slows down in order to prevent any legitimate traffic to access the network. This is instigated by the UDP (User Datagram Packets) and the (internet control message protocol) packets. In amplification attack the attacker sends a large number of packets to a broadcast IP address. It causes the systems in the broadcast attacks to send a reply to the victim system thereby it results in a malicious traffic. This attack exploits the broadcast address feature that is found in most of the internetworking devices like routers. This kind of DDoS attack can be launched either by the attacker directly or with help of Zombies. Smurf and Fraggle attacks are well-known attacks of this kind. These attacks can be prevented by providing a destination site router connected to a destination site locally along with internet connection. Another way is by providing connectivity between said origin and destination site routers to the internet or the other Wide Area Networks (WAN).

Resource based attacks: This attack targets to exhaust or consume the victim computer system's resources, so that, the legitimate users could not use the services. This attack can be further classified as protocol vulnerability exploitation and malformed packet. In protocol vulnerability exploitation the main aim is to consume a large amount of resources from the victim by exploiting the specific feature of the protocol that is installed in the victim. TCP SYN attacks are the best example of this type. Malformed packet attack refers to the packet that is wrapped with malicious information or data. The attacker sends these packets to crash it. This can be done in two ways IP address attack and IP packet options attack. These attacks can be prevented by using a firewall, an antivirus or intrusion prevention system.

Prevention of DDoS: The best way to overcome this attack is a technique called filtering. The ingress filtering stops the incoming packets with a not legitimate source address. Routers are used for this purpose. Another type of filtering called the Egress filtering uses the outbound filter. This technique allows the packets that have vivid IP address in the network to leave the network. Another way to overcome this attack is CAPTCHA (Acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge response test used incomputingto determine whether or not the user is human or not. CAPTCHA prevents bots from regular attempt in authorisation access. Intrusion detection system is used to detect DDoS attack. Other prevention techniques includes disabling unused services, applying security patches, changing IP address, disabling IP broadcasts, load balancing and honeypots.

SQL injection: SQL (Structured Query Language) always works and responds to the queries that have to execute in the database. Malicious code is injected into the semantics and syntaxes frame of the database query that directs controls of web application's database server (also commonly referred to as a Relational Database Management System RDBMS). Suitably crafted code helps attacker to enter into the database where the administration password is stored and gets the username and password which gives authorize access to the legitimate website. SQL injection attacks are executed statically and dynamically to hack websites. Injection of code is done via. user input, cookies, server variables and second order injection. Intruder detection system and firewall is also not effective in stopping these attacks. The vulnerabilities in a web application of a particular system can be exploited to implement this attack. Such vulnerabilities may include insufficient connection of variables, lack in data verification, etc. SQL injection attacks are divided into order based on its nature. In first order attack the attackers write some type of malicious queries that causes the code to execute immediately and in second order, attacker modifies the contents of the database system by using the SQL statements like insert and delete. An attack is then forcefully executed by another action. Third order attack plays with the implicit functions.

Resolving SQL injection: Various detection techniques have been developed to detect such vulnerability. WAVES which is generally known as a black box technique (Huang *et al*., 2003) is efficient to test web applications for SQL vulnerabilities. It finds or identifies all the loop holes or points that can be easily found to inject SQLIAs. During the attack phase WAVES targets certain vulnerabilities as well as keeps a check on the web application by machine learning (Huang *et al*., 2003). Two recent approaches, SQL DOM (Halfond *et al*., 2006), safe query objects (Cook and Rai, 2005) for monitoring application response are also used that provide a secure environment to access database.

Cross-Site Scripting (XSS): Cross site scripting enables the attackers toinjectmalicious code at client-site through

mails, links on web pages that seems to be of legitimate and harmless. When a user put any credential to such links it bypassaccess controls in the hand of attacker. Attacker can also steal web browser cookies which alternatively used in session hijacking or personal data. Sometimes users are directed to move into a specially crafted link that may alter the user's choice (non-persistent attack) or by being anonymously by simply visiting a web page embedded with malicious code (persistent attack) (Grossman, 2006). There are two general methods for injecting malicious code into the web page, first is stored XSS in which the attacker persistently stores the malicious code in a resource that is managed by the web application such as a database. The actual attack is carried out in a later time when the victim requests a dynamic page that is made from the contents of this resource. The second method is called reflected XSS, the attack script is not persistently stored but instead it is immediately reflected back to the user. It may be temporary and permanent attack based on its nature. In temporary attack, few sessions are hijacked and on the other hand, permanent attack session hijacking is done to get confidential data of an admin of the website. The optimal approach to prevent XSS attack is eliminating all the possible vulnerabilities in the affected web applications. A web application must validate all the inputs properly and remove malicious scripts. Example, Samy worm 1.

Brute force attack: Every individual choose their password according to own concern. Hackers may choose hit and trial method to get into others privacy. Brute force attack is similar to dictionary attack. In both attacks, random passwords are tried so as to break security per unit time. Dictionary attack comprises of word list of potential passwords but not on user's perception but on the other hand in brute force attack, a set of passwords that could be anything or any combination, tried on the page at one time. It works on mathematical possibility of permutation and combinations. There is another type of attack called reverse brute-force attack in which the attacker chooses a single password for multiple usernames and encrypted files. This process can be repeated for selected few passwords. In this type of strategy the attacker does not targets a specific user. Reverse brute-force attacks can be prevented by establishing a policy regarding the passwords that disallows common passwords.

Handling Brute force attacks: Since, no specific logic can be applied in these Brute-force attacks except for hit and trial technique in which different combinations of characters are tried out for the secretion of a password, the prevention technique is quite basic and simple. You should use a strong password or complex master password that should contain certain important characteristics. Such combination must be of minimum 8-10 characters and consist of an uppercase letter, one numeral, special character or symbol.

RESULTS AND DISCUSSION

Intrusion prevention system: IPS (Intrusion Prevention System) is a complete solution for network security as it detects any known and unknown attacks and responds accordingly. IPS is considered as better to detect any loop hole in an organisation or home. Different types of IPS has been introduced in different fields to solve the issue and these are inline network intrusion detection system, application-based firewalls/IDS, layer seven switches, network-based application IDSs, deceptive applications (Desai, 2003). It aims to monitor traffic and work similar in function to a firewall but it is considered to be better than firewall. It detects signature of incoming traffic along with TCP connection and protocol validation (Desai, 2003). It provides an advance environment where user gets a complete knowledge of unwanted incoming traffic source and blocks vulnerability for future prevention. Three basic categories of solution have been available to deal with an attack, Network IPS Solutions (NIPS), Host IPS Solutions (HIPS) and Wireless Intrusion Prevention System (WIPS). HIPS is considered to block unwanted application at the host and also refer to as last line of defence whereas NIPS blocks any critical or unwanted source on the first line of defence. WIPS checks for unauthorised access to the network. As any other system IPS has also least cons like it sometimes make unveil of useful data due to its abnormal traffic movement in the network and investment requirement in implementing, it is somehow high. NIPS consist of two component matching engine and a complementary packet classification engine. NIPS are designed to work in-line (Weinsberg *et al*., 2006). IPS are having some tools that are mainly used to deal with the detected vulnerability over network.

Snort's database: Snort is an open source de-facto standard for NIPS. Snort contains database rule book of several thousand of attack signature. It is having a header file that contains packet identifier and several content part having pattern. Packet identifier checks IPs and port whereas patterns checks for several possible correlation along it. It uses a variant of the Boyer-Moore algorithm to search pattern (Weinsberg *et al*., 2006).

Parallel bloom filters: In study of Dharmapurikar *et al.* (2004) describes parallel bloom filters is an algorithm that uses a bloom filter for each pattern length. It generally uses several hash functions that are capable of reducing the potential patterns space that may match the search window. In this each different pattern length requires a separate bloom filter which is its major limiting factor when dealing with long virus definitions that are several bytes long.

Network processor pattern matching: The research of Liu *et al.* uses a network processor with a hashing engine that is memory based. It uses a prefix sliding window of length w which shifts from the leftmost byte to the rightmost byte of the text. Their algorithm supports only simple patterns with no correlations of patterns. The algorithm uses a shift table (of size (21) w) that includes all possible w bytes combinations.

TCAM pattern matching: Yu *et al.* (2004) proposes TCAM pattern matching an advanced memory chip having three bit zero, one and "don't care". This algorithm minimise the pattern matching time. In the study Yu *et al.* (2004), it is stated suppose the packet length is n the algorithm requires n TCAM lookups. If a single TCAM lookup takes 4 ns, this brute force algorithm yields a matching speed of $8\times n\ [Bytes]/^{4n[ns]} = 2$ Gbps (denoted as Naive Scan rate) (Weinsberg *et al.*, 2006).

Intrusion Detection System (IDS): Primary area of concern for any attack is to detect a prevention that can only be followed when a proper citation of any attack is identified. IDS primarily focuses on all possible suspicious incidents, logging information and any attempt in the direction of security threat. It monitors and analyses configuration and abnormal pattern that can produce anomalous and malicious activity. Detection is being followed on two different approaches that is signature based and anomaly based. Signature based approach look up for particular pattern or identification mark whereas anomaly based detection recognise abnormal behaviour of any pattern. Intrusion detection system follows two different approaches for its implementation, software that is deployed on server or host and next implementation is hardware in the form of product. A different approach has been concluded to detect an attack. One of them is Bayesian approach which aims to find out possibility of attack by analysis of previous statics. Detection is verified on two different categories that is network based and host based. Network based checks for entire setup monitoring and components. It takes care of every process and command that is processed on the network. Host based takes care for every status and monitors at the terminal or server.

Attack could be perform based on two different methodologies, first is multi-connection attack and second is single connection attack. Multi-connection is for more number of intruder to a network at a time whereas single connection approach is having single intruder to the network. Attacker may use more than one attempt and more number of technique to enter into the network by manipulating large amount of traffic. IDS have to detect the pattern in real time and behavioural change of each data flow in the network. Anomaly detection pattern is considered to be more accurate in identifying types of intruder and source. Anomaly detection technique uses different techniques to detect intruder such as related work, outlier detection, mining outliers using distance to the k-th nearest neighbour, Nearest Neighbour (NN) approach, Mahalanobis-distance based outlier detection, density based Local Outliers (LOF approach). Another approach has been considered that is EMERALD system (Javitz and Valdes, 1994) that compares historical data with newly obtained data. Outlier technique is based on pick up the odd or outlier one. It checks for data or pattern that has not been previously reported. Recent advancement can also consider multidimensional distribution of data (Knox and Ng, 1998; Ramaswamy *et al.*, 2000).

After concluding detection techniques, IDS perform some basic function to keep away safe from any type of threat. IDS collects information from data mining, generate security alert to the security administrator, produce reports underlying all security concern and blocks all detected vulnerability.

Network security advancement: Network security got attention when a crime committed by Kevin Mitnick had 80 million dollars loss in the US intellectual property and the source code from many companies. Since then, information security came into spotlight (Zalavadia, 2014). Network security attacks have become easier to use. Today, everything is connected to internet from simple shopping to defence secrets as a result there is huge need of network security. Now a days, the network security is continuing the same route. The same techniques of security are used with the addition of the biometric identification which provides a better method of authentication rather than passwords. New technology such as smart card is also surfacing in the research of network security. Constantly, new firewalls and encryption schemes are also being implemented. In future, the embedded security of the new internet protocol IPv6

may provide benefits to the internet users. The IPv6 internet protocol seems to evade many current popular attacks. The IPv6 and the security tools such as firewalls, intrusion detection and authentication mechanisms will prove effective in securing intellectual property in the near future.

CONCLUSION

Internet is a blessing to our lifestyle. We all depend on it directly or indirectly now a days. Various steps are being taken to prevent the privacy of either individual or an organisation. Almost all activities whether they are of daily use or professional use are defined through internet. Several types of attacks have been identified and some of them are outlined in the study. Some are minor and some causes severe damage. We should understand the depth of security and utilise it's prevention in our system. Risks are always there, new advancement are yet to be done along with modification in existing application and across the world find new methods to prevent them. White hat security gives a threat classification with Web Security (WASC) is the standard to prevent from malicious programs. Firewall, VPN and intrusion detection system are some of the few tricks to get away from it but they do not guarantee full proof security. Somehow TOR browser will be a better solution. This study deals with some basics and random attacks on network, more area needs to be dealt. We must have proper knowledge of various prevention to implement as per requirement and safety in our daily life.

ACKNOWLEDGEMENTS

Researchers are thankful to the Editor, Associate Editor and anonymous reviewers for several constructive suggestions. We also would like to express our sincere gratitude to Dr. Sukhdev Singh, Accendere Knowledge Management Services Pvt. Ltd., for his valuable comments that led to substantial improvements on an earlier version of this manuscript.

REFERENCES

Cook, W.R. and S. Rai, 2005. Safe query objects: Statically typed objects as remotely executable queries. Proceedings of the 27th International Conference on Software Engineering, May 15-21, 2005, ACM, St. Louis, Missouri, ISBN:1-58113-963-2, pp: 97-106.

Daya, B., 2013. Network security: History, importance and future. University of Florida: Electrical and Computer Engineering, Gainesville, Florida. http://www.alphawireless.co.za/ wp-content/ uploads/2013/01/Network-Security-article.pdf.

Desai, N., 2003. Intrusion prevention systems: The next step in the evolution of IDS. Symantec, Mountain View, California.https://www.symantec. com/connect /articles/intrusion-prevention-systems-next-step-evolution-ids

Deshmukh, R.V. and K.K. Devadkar, 2015. Understanding ddos attack and its effect in cloud environment. Procedia Comput. Sci., 49: 202-210.

Dharmapurikar, S., P. Krishnamurthy, T. Sproull and J.W. Lockwood, 2004. Deep packet inspection using parallel bloom filters. IEEE Microbiol., 24: 52-61.

Grossman, J., 2006. Cross-site scripting worms and viruses. White hat, Pasay, Philippines. http://s3.amazonaws.com/academia.edu.documents /6784491/wp5css0607.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1493814150&Signature=6XMAEfAlwRW62wDo6mbu7pm3wDw%3D&response-content-disposition=inline%3B%20filename%3DCross

Halfond, W.G., J. Viegas and A. Orso, 2006. A classification of SQL-injection attacks and countermeasures. Proceedings of the IEEE International Symposium on Secure Software Engineering, March 13-15, 2006, Washington, DC., USA.

Huang, Y.W., S.K. Huang, T.P. Lin and C.H. Tsai, 2003. Web application security assessment by fault injection and behavior monitoring. Proceedings of the 12th International Conference on World Wide Web, May 20-24, 2003, ACM, Budapest, Hungary, ISBN:1-58113-680-3, pp: 148-159.

Javitz, H.S. and A. Valdes, 1994. The NIDES statistical component: Description and justifi-cation. Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California.

Knox, E.M. and R.T. Ng, 1998. Algorithms for mining distancebased outliers in large datasets. Proceedings of the 24th VLDB International Conference on Very Large Data Bases, August 24-27, 1998, VLDB, New York, USA., pp: 392-403.

Rad, B.B., M. Masrom and S. Ibrahim, 2011. Evolution of computer virus concealment and anti-virus techniques: A short survey. Int. J. Comput. Sci. Issues, 8: 113-121.

Ramaswamy, S., R. Rastogi and K. Shim, 2000. Efficient algorithms for mining outliers from large data sets. Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data Vol. 29, May 15-18, 2000, ACM, Dallas, Texas, ISBN:1-58113-217-4, pp: 427-438.

Verma, A., M.S. Rao, A.K. Gupta, W. Jeberson and V. Singh, 2013. A literature review on malware and its analysis. Intl. J. Current Res. Rev., 5: 71-71.

Weinsberg, Y., S.T. David, D. Dolev and T. Anker, 2006. High performance string matching algorithm for a Network Intrusion Prevention System (NIPS). Proceedings of the 2006 Workshop on High Performance Switching and Routing, June 7-9, 2006, IEEE, Jerusalem, Israel, ISBN:0-7803-9569-7, pp: 1-7.

Yu, F., R.H. Katz and T.V. Lakshman, 2004. Gigabit rate packet pattern-matching using TCAM. Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP 2004), October 8, 2004, IEEE, Berkeley, California, ISBN:0-7695-2161-4, pp: 174-183.

Zalavadia, B., 2014. Network security issues and solutions. Intl. J. Comput. Sci. Eng. Technol., 5: 621-624.