Volume 5, Issue 10, October-2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Overview of Attacks in the Network Security System

Manimegalai.C (M.tech IT)
Aptitude Trainer,
Maharaja Prithvi Engineering College,
Avinashi, Tamilnadu, India

Sumithra.A (M.tech IT)
Assistant Professor,
Sri Krishna Engineering and Technology,
Coimbatore, Tamilnadu, India

Abstract— Nowadays securing a network system is becoming more complicated due to attacks and malicious functions. Recently, there are enormous numbers of threats occupied in the network space. Without security in the network, the system can't able to safeguard the information. Some unauthorized person can access the data or stole the secured information. To recover these problems in the system, there is a need for network security. Network security is a tremendous and blooming platform. It aid to recognize and shelter from different threats in the system. The volatile technology broadening network pursues to redefine the act of prolonging the privacy information. It is durable and dependent for authorized users to way in their information in the network. Network security built number of constituent to perform a task to prune maintenance and upgrade security in the system. The constituents of network security frequently comprised are firewall, intrusion prevention system (IPS), virtual private networks (VPNs), etc. These constituents observe the venture between interior and exterior of the network system. Before we discover our security plan, we have to point out our potential hacker. To be aware of attacking procedure, it helps you to fix the proper security in the system. This paper is proposed for various kinds of attacks and its functions.

Keywords— Network security, Constituents of network security, Attack and its function

I. INTRODUCTION

Every developing company has to secure their confidential information for upgrading to a high standard. There are large numbers of theft helve by a person who utilize computer to reap unauthorized entry to data. These thefts strive by using two major contradictory techniques. 1) Unknown person who is skill to sabotage computer security. 2) A follower of the technology and programming division. To rescue from these theft, there essential for network security. Network security is to be consistent with strategies embraced to turn aside and track authorized information, put to wrong apply, action of change made, or denial of network resources. In other words, network security is to block any fortuitous or deliberate dropping of information in the network. The network administrator of network security has the authority for the authorization of access information in the network [9].

Network security software has one central user to change the access in the network. Desktop security software can be moves backward engineered without an intention. Desktop security is a great extent capable to virus and worms. Centralized protection will halt the hacks before they damage the data in network. The main drawback of desktop software is strongly felt along with the internet connection. Virus attackers or hackers utilize their purpose through internet only. Network security software fixes a machine in between the internet and network that monitor the information across the network.

Centralized protection will take more processing time to abolish cumulative drag. Comparing to old antivirus software, centralized protection is more compatible because old antivirus are incompatible to run the risk. Centralized protection network will update on all independent users in the network system. For updating and managing on one central location is easy to save the time in the network system. Another way to secure information in the network is firewall. The desktop security flaw can be recovered by installing firewalls in the network connection.

Firewall is the process of controlling and examining the introvert and extrovert network traffic found on security rules. Firewall can be divided into two types. 1) Network firewalls. 2) Host based firewalls. Network firewalls is application software running for the purpose of hardware or hardware based firewall application. The duty for network firewall is to filter the traffic between the networks. Host based firewalls build a number of software layers to control network traffic for a single machine. Firewall system has audit and alarms for observing security phenomenon. Firewall system is a suitable platform to run some internet functions like network address translator and network management functions. Firewall system creates virtual private network to serve for IP security [9].

Intrusion prevention system or Intrusion detection and prevention system is a network security application used to recognize and block the malicious function in the network system. The prevention methods are divided into four types. They are 1) Network based intrusion prevention system (NIPS). 2) Wireless intrusion prevention system (WIPS). 3) Network Behavior analysis (NBA). 4) Host based intrusion prevention system (HIPS). The detection methods are categorized into 3 stages. They are 1) Signature based detection. 2) Statistical anomaly based detection. 3) Stateful protocol analysis detection. IPS put effortless to control the number of attacked host in the network system. IPS has the capacity to examine an extensive domain of protocols. It is easily recognize the inside and outside attackers as well as detect them.

Honeypots is one of the computer security mechanism used to conquest strives at unauthorized manipulate of information security. It can be categorized into two types. They are 1) Production honeypots. 2) Research honeypots. Honeypots are good at data collection, reduction of false positive and false negative, design and implementation simplicity and resources.

II. VARIOUS KINDS OF ATTACKS

The reason for occurring attack in confidential data is without having security. The data examining attacks are passive attacks. The remaining attacks are active attacks which means the data is destroy or corrupt by modifying the information. A system ought to be allowed to restrict damage and repossess quickly when attacks occur. There are some attacks that listed below. An **active attack** is nothing but a hacker endeavors to construct changes to information or bypass into the secured systems. Active attacks distinction with passive attack is to reap data only and there is no modification in the information. Active attacks include some attack are masquerade, session replay, message modification, denial of service, and distributed denial of service [1].

Eavesdropping is an attacker quietly listen the communication between the networks. This is the massive problem where arose in the network system. The network administrator has to countenance this problem by using cryptography concept. The concept is strongly to encrypt the data in the network system [10]. A **masquerade attack** is manipulated to realize security holes in a program like stolen login IDs and passwords. A **session replay attack,** a hacker who uses session ID to steals the authorized user's login information and to gain access and the ability to change anything in the network.

Denial of service attack is an attack that is designed for the user's not having to access through network. DOS attacks many times grip ARP spoofing to connect involving several IP addresses with a single MAC address. This creates overloading the traffic in the network [2]. **Distributed denial of service attack** is also called as Botnet or Zombie army attack. This attack utilizes large numbers of make concessions system attack to attain a single target. **Ping broadcast attack** is a DOS attack. A ping request is transmit to broadcast network address, in that source address and IP address of the computer information are attached. The ping broadcast passes information through router, all computers on the network will ping rely to the connected system. This may cause lock up the network. This attack is to chunk incoming traffic that is transmitting to a broadcast address. **Ping of death,** An enlarge Internet Control Message Protocol (ICMP) datagram be able to crash IP devices that were made earlier than 1996.

Teardrop is sending a normal packet in the network system. A second packet is dispatch which has a fragmentation counterbalance insist to be interior first fragment. This second fragment is extremely compact to enlarge the first fragment. This may induce a buffer overflow or system crash on the operating system. **Man-in-the-Middle attacks** let attackers to head off, dispatch and collect data without knowing for the outside party. The interactions capable to Man-in-the-Middle attacks are connections secured by keys and financial websites. **Side jacking attack** is an attack requires sniffer to pilfer cookies and user's session. Even the sites are secure, the cookies can hold within unencrypted login data. **Evil twin** is a dishonest network that becomes visible to be a valid network. This hacker can utilize man-in-the-middle attack for intercepting between the networks.

Sniffing requires a malicious trouper using software program to cut off information existence send from or to outwit. **DNS Spoofing or DNS cache poisoning attacks** is an attack by which information is established into a Domain Name System (DNS) rectifies cache; begin the name server to take back in fallacious IP address, reroute traffic to any other computer. Example for DNS Spoofing makes users to be managed to fallacious Email existence to unauthorized mail servers [9]. **ARP spoofing** is one type of attack the ARP falsified by malicious attacker over information in the LAN. The outcome of this ARP spoofing in the connecting of an attackers MAC address accompanied by IP address of a server on the network. By using packet filtering, avoid trust relationships, using ARP spoofing detection software, using cryptographic network protocols to preventing the ARP spoofing.

VLAN hopping is a process of attacking networked assets on a Virtual LAN for makes use of security. VLAN hopping attacks is an attacking VLAN host to acquire way in to traffic on other VLANs that would not be accessible. There are two types of VLAN hopping. They are 1) Switch spoofing 2) Double tagging. **Switch spoofing** is an attacking host emulates a system of shaft switch by speaking the tagging and ventilates protocols utilized in to keep alive a VLAN. **Double tagging attack** is an attacking host attached on an 802.1q interface adds to the beginning of two VLAN tags. The first tag cannot able to transmit packets through VLAN tag. The second tag is able to be seen to the second switch that the packet encounters.

Smurf attack is a distributed denial of service attack in which huge amount of Internet Control Message Protocol (ICMP) with the deliberate casualty spoofed source IP are live stream to a network using an IP address. **Fraggle attack** is an attacker transmits a huge numbers of UDP ports to IP address. **Compromised-key attack** is an attacker utilize compromised key to obtain entry to a secured communication without the transmitter or receiver existence conscious of the attack.

Identity attack or IP address spoofing, basically networks and operating systems utilize IP address to identify a viable entity. Sometimes in the identity spoofing, the IP address is fallacious assumed. The attackers have to create a special source to build IP packets that resembles like a valid address in the corporate intranet. After pick up the network with viable address, the attacker can change, reroute or delete your information.

Password based attack; most of the operating systems and network plans is password based access control. When the attackers identify the viable user account, the attacker has the identical as the real user. This attack creates the changes in the administration as like the user do. **Application Layer attack** affects application servers by creates culpability in a server operating system or applications. It discovers a virus program in computers and software applications to duplicate viruses in every part of network. Damage other security control to permit future attacks.

Brute force attacks: at present time, brute force attacks are 25% in the network system. Neither like other attacks rear way in, it strive and error effort to conjecture a systems password. Brute force attack bid is one in which has four network attacks. Example for Brute force attack, automated software is repeatedly utilized to guess combinations of hundred or thousand password. To resolve this problem from brute force attack is to lock account after a number of wrong attempts in login ID. **Browsing attacks**: This attack will be held while the end users to surfing in the internet. The attacks give permission to oblivious download malware concealed as a mock up of software application or update.

Shellshock attacks point out vulnerabilities discovered in bash. Its occurs in command line of Linux and Unix operating systems. Recently, this attack emerge 7% in the system. Attackers have established put to use the flaws, manipulating them to install malware and distributed denial of service attacks. **Secure Socket Layer attacks:** analyzing the entire network attacks it occupy 6% in the network system.SSL attacks attempt to cut off data that is dispatch over an encryption bond.

POODLE attack (Padding Oracle on Downgraded Legacy Encryption attack) is a Man-in-middle attack which extracts the advantage of internet or way of some browser to compromise with encryption. Attackers utilizing the vulnerability by using 256 SSL 3.0 request to disclosure the encrypted data. To rectify from this attack is to utterly debilitate SSL 3.0 on both client and server side. **Collision attacks** is to discover two input strings of hash function that make same hash value due to infinite input. Collision attacks are also called as **free start collision attacks**. Collision attacks lead to smash the whole inner layer of SHAI algorithm. **Hijacking attacks** preside over for session token that is consistent with a misuse of web session control mechanism. The session key occasionally hijacked to acquire unauthorized access to data in the network system. Session hijack is also called as **Cookie hijacking attacks.** There are four major types utilized to execute session hijacks are 1) Session fixation. 2) Session sidejacking. 3) Cross site scripting. 4) Malware.

Social Engineering attacks are also called as bugs in the human hardware. It attains the unauthorized entry to a network by overthrowing personnel information. Social engineering is one form of close-in attacks. Examples for social engineering are pretextual, phishing, interactive voice response, diversion theft, etc. **Phishing attack** is one of the examples of social engineering attack. It seeks to gain the sensitive information like username, password, and credit card details, generally for the purpose of create malicious function in an electronic communications. Phishing types are spear phishing, clone phishing, and whaling.

Exploit attack is a segment of data that lead bugs to begin not predicted behavior in the system. Pivoting is the only method to rescue from exploit attack. It can be divided into two types. They are 1) proxy pivoting. 2) VPN pivoting.

Passive attacks are required only to observe data and nothing changed in it. It is on cryptosystem which cannot able to interact with the parties. Passive attacks embrace active reconnaissance and passive reconnaissance. Active reconnaissance is an invader capture system to collect information regarding vulnerabilities. Passive reconnaissance is contrast of active reconnaissance, to collect information concerning computers and network in absence of actively in capturing with the network system. Methods of passive attacks are war driving and dumpster driving [1]. **Telephone tapping** is keep track of third party in between the conversion of telephone and internet. Legal telephone tapping is known as Lawful interception. In this two kinds of wiretapping are there. They are passive wiretapping and active wiretapping. Passive wiretapping is used to observe the network traffic and active wiretapping is used to modify on it.

Port scanner is a software application used to study about the open ports in server or host. The administration are utilized the port scan to verify the network and along hacker to distinguish services on host and vulnerabilities. **Portsweep** is to scan many hosts for listening ports. Types of scanning are TCP scanning, SYN scanning, UDP scanning, ACK scanning, Window scanning, FIN scanning and other scanning types.

Idle scan is a TCP port scan technique which is used to find available service by sending spoofed packets. This is only for perceiving the information and not for transmitting zombie system. Zombie is nothing but pretend to be another system.

III. CONCLUSIONS

Network security is required to get the assurance of information security in the network system. Network security has to recognize the threats in the network and have to fix the suitable security plan to the network computer. We should be aware of various attacks and then how to protect from them. A virtue of security plan is to phase the requirement of the administration, management and users in the network system. Here we have seen about various kinds of attacks in detail and how to rectify them by using some safeguards like intrusion prevention system, honeypots, firewall, etc. These safeguard techniques are used to enlarge the security levels in the network system.

REFERENCES

[1] Inam Mohammad, Rashi pandey, Aashiya Khatoon, "*A review of types of security attacks and malicious software in network security",* International journal of Advanced research in computer science and software engineering, vol.4, iss.5, pp.413 – 415, May 2014.

[2] www.securityweek.com/security infrastructure/ network-security.

[3] http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Network-Security-Basics.pdf

[4] William Stallings,"Cryptograpy and Network security", Vth edition.

[5] http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/\

[6] http://whatis.techtarget.com/definition/active-attack

[7] http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html?referring_site=smartnavRD

[8] https://training.apnic.net/docs/TSEC01.pdf

[9] Matt curtin, " Introduction to network security".

[10] Bhavya daya "network security : history, Importance, and future".