An Analytical Study of Network Security Threats Through IP Spoofing

Deeksha Vashishth

B.Sc (H) CS, 6 Sem, 3rd Year
CCSIT, TMU, Moradabad
deekshavashishth0807@gmail.com

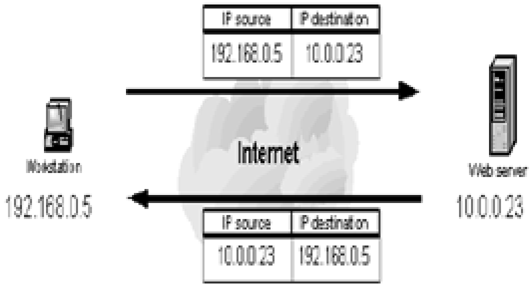
Abstract— The fact that networks are at a high rate of risk, means that the data transferred in and out of the network are being sniffed every now and then. This doesn't stop with the least secured data, as it aims at the highly secured data like the bank account, confidential passwords, and also financial data etc. The most important practice used to sniff data in a network is called a spoofing technique, which plays a wide role in helping the attacker to develop his reign in intrusion and sniffing of data in any network or a particular device. These attacks are a threat to devices connected to any particular LAN or other networks. There are techniques used for the prevention of few attacks, as spoofing doesn't end with just a few types. The latter part of this paper provides detailed survey on techniques used frequently for invading a network. A basic intrusion detection system or a firewall is sufficient to prevent primary attacks when the network is at risk. This survey paper focuses on the state of art of various spoofing and its vulnerabilities.

Keywords— Spoofing, network, attacks, intrusion detection system.

INTRODUCTION

Spoofing is a process that enables to gain access to unauthorized information in wireless network. This is a process to gain the user's private data access. Network attacks have become increasingly high, as there exists no particular cause other than theft, sport, or fraudulency in money making. This is an important aspect to be overlooked before any highly secured information is being transmitted in the network layers.

. Types of Spoofing Attacks There are several types of spoofing, and the main category is the network spoofing, which is again broadly categorized into three main types namely the IP spoofing (Internet Protocol), ARP spoofing (Address Resolution Protocol), and DNS spoofing (Domain Name System), protocol spoofing, MAC spoofing(Media Access Control). The remaining vulnerabilities of spoofing are the web spoofing, Email spoofing, and the non-technical spoofing. The vulnerabilities are elaborated below as: Network spoofing: Network spoofing is an act of spoofing the sources and information from the restricted and protected files in any network. Network spoofing is a neutral task; this can be made beneficial and hazardous as well. The main perspective behind network spoofing is to spoof the data that is least protected by faking an IP address and gain trust as a legitimate user of the network. But otherwise, network spoofing is a superficial activity that could protect data traffic in the network, as it is not easy to validate all the packets being transmitted from one user to the other, this practice is also helpful in clearing or reducing the network traffic. The network traffic is a broad sector which is further split into three main categories namely the ARP spoofing, IP spoofing, DNS spoofing, protocol spoofing, MAC spoofing. These types are elaborated as follows: ARP Spoofing: ARP spoofing is called the Address resolution protocol spoof technique which is primarily based on a practice of sending the fake ARP messages to the target user which matches the MAC address to the target's IP address there by sniffing the data which is originally intended for that IP address. There are several types of attacks possible in ARP spoofing, such as the; Denial of service attacks: This is just the basic of any ARP spoofing technique, to link multiple IP addresses to the target's MAC address. This results in redirecting the traffic to the fake user instead of the intended IP addresses. Session hijacking in general is known as cookie hijacking, this is familiarly known as the session key. But ARP session hijacking is a part of this technique which steals the session ID of the particular target and used to access private data. Man-in the- middle attack: Man in the middle attack uses this technique to create traffic in the network. IP Spoofing: IP Spoofing is an idea used frequently to sniff data in any network access. There are two types namely, (i) Traffic overloading at the target by faking an IP address in a particular network, and (ii) To sniff the target's IP address and send data to others in that address so as to gain the necessary data as response from the other users. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system. The common steps of IP spoofing are to create IP packets with a forged source, in order to gain.

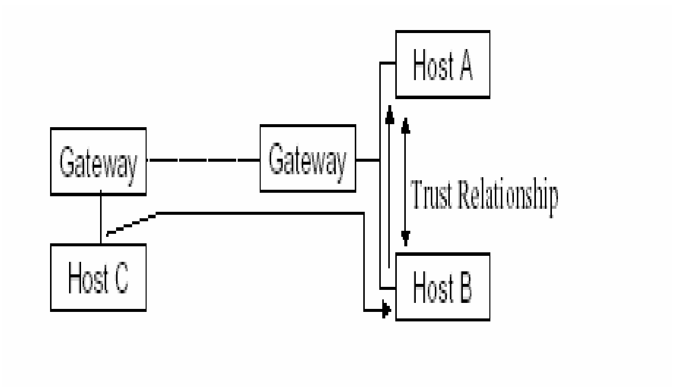


. *Journal of Chemical and Pharmaceutical Sciences ISSN: 0974-2115*

fake identity. And deny the access of the original user. Create data traffic or overloading to the target user so that the network security is damaged. IP spoofing is again categorized into four main categories as Blind IP spoofing, Non-Blind Spoofing, DenialOf service attack, Man –in –the Middle attacks etc.

1.Blind Spoofing

□ Blind spoofing is generally based on the sample sequence numbers, the hacker more often sends a few packets to the target machine keeping in mind the end goal to test succession numbers, which is possible in more established days. This technique is to compromise the sequence numbers in order to sniff the data.

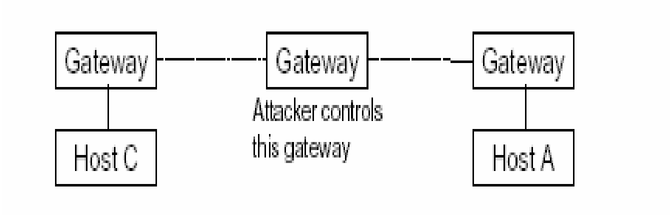


2.Non-Blind Spoofing

□ Non–blind spoofing is commonly referred to as session hijacking, where the attacker becomes a trusted user of the target through authentication. All this is possible only if the target and the attacker are said to be in the subnet. This is a comparatively easy task than blind spoofing.

3.Man-in the Middle Attack

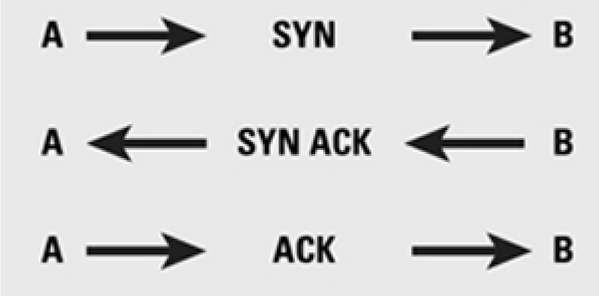
□ Man-in the Middle attack is just an eavesdropping attack, where there is an undisturbed conversation between two end target users, and this attacker has a high note on all the data that is being transferred between both of them.



Progress of a man-in-the-middle attack

4. Denial-of-Service Attack

□ Denial-of –service attack is a direct hit on the large network administrations, where the server or the main access point is being hacked and the information from it to the targets are spoofed at denial of permission. DNS Spoofing: This technique is to bring an associate the domain name of any system to the IP address of the hacker. DNS is a system which is base to resolve URL's, email addresses of any computer that depends on internet or other networks for data transfer. There are different types of DNS spoofing:



DNS cache poisoning: DNS server is not self-sufficient with the memory to store all the addresses or the domain names/IP addresses of its own network, instead it uses the DNS cache, and this instead stores the information about that particular network. DNS server has a restriction to communicate only with its own server, in order to communicate to a different server it has to request for the permission to access data to access from the other DNS server. This process used to but the attacker to fake a different IP address and access or get data with authentication is called the DNS cache poisoning. DNS ID spoofing: This technique is mainly based on the communication between a particular network where the former and the latter system communicates with the help of the ID authentication. This occurs as a request which is given by the former system to the DNS server. This DNS server compromises only depending on the pseudo random number which is assigned to the former system, after which it provides the IP address of the later system to which it has to communicate. This DNS ID spoofing can be done by faking a pseudo random number or the ID number in order to gain authentication of that network or server. MAC Spoofing: MAC (Media Access Control) address is a factory assigned address given for any device which could connect itself to a network for any data transfer. This is conventionally considered that it is coded and could not be changed. But there are possibilities to change the MAC address of a device. This process of masking the original masking address of the device is called the MAC spoofing. There are two types of MAC spoofing techniques:

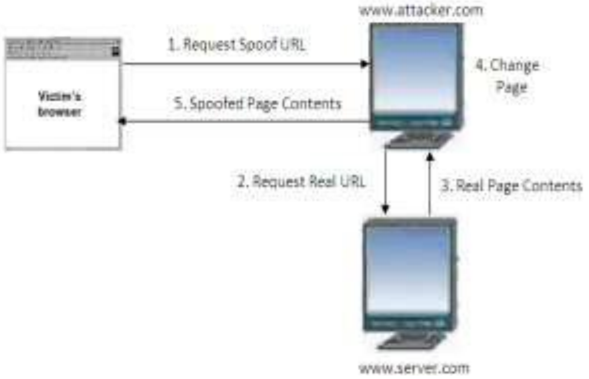
□ The primary technique is for security and privacy policy. The user prefers a technique called identity masking which is to hide the user's private MAC address in order to safe guard the data transmission when connected in a private LAN or Wi-Fi connection. This prevents sniffing of data as the original MAC ID of the user remains hidden.

□ This is the second technique in which every device connected to a network has its own MAC address. When it requires an internet connection, the service provider registers its MAC address and then provides the connectivity. Supposing it requires a dual connection, there exists another fake system which projects this registered MAC address and gains access to the internet connectivity in the name of the original system. Protocol spoofing: PROTOCOL is a set of rules. Every network has its own protocol like the Transmission Control Protocol (TCP). These types of protocol is to set up a network, maintain the data transfer in and around the network, also used abruptly to cut down or breakdown the data transfer in the network. The primary procedure to connect a computer or a device to a network is to send request, which is analyzed by the check data of this protocol. This process is a little hectic as it could also create data traffic. This could change the sequence numbers or the produce changes in the data being transferred. Here spoofing acts as a plan to interpret as a gateway which again sends requests and replies to the TCP messages, thereby gaining access to that particular network.

Types of spoofing attacks E-mail address spoofing: E-MAIL spoofing is the most efficient and easiest technique to gain the target access. This requires a forged email header which resembles the original email ID. This is a process that is enabled by using a Simple Mail Transfer Protocol (SMTP). This protocol is a simple mechanism which does not require any authentication from the network or the device. This is considered to be the easiest method used to invade into any network and use it to send messages, provided if there is no proper precaution. With this protocol it is now made simple to write or send an email from anyone and anywhere pretending to appear like the original sender. E-mail spoofing has various purposes like collecting very confidential sensitive data like that of the bank account information, passwords etc, to the very least secured data, which could be simply accessed by using a fake e-mail address of the most important official, which might look real. There are three main E-mail threats: Phishing: This is a simple technique that is used by most of the growing hackers to sniff data creating an e-mail that looks exact and similar as a business e-mail. These attacks are not intended to have a specific target or a particular victim. These e-mails are broadly created and sent to many people, the more the e-mails are sent, the more it is generated, the more is the possibility to sneak people's password, bank account number and other confidential details. Spear phishing: This type of phishing is more specific. The target is initially identified and then the e-mails are sent, this is a threat to many people who are using e-mails as the main media of information and business transactions. The attackers tend to gather the information and personal details to create a fake e-mail that looks very similar as the original to gain private data of the target. E-mail spoofing: E-mail spoofing is a technique that uses the SMTP protocol to sniff data. This technique is simple and could be detected if the target has a firewall or an intrusion detection system (IDS) in the device.

Web spoofing:

Web spoofing is a practice that permits somebody to see and change all website pages sent to a victim or the target user, through this method any forms of data entering and leaving the device can be monitored, for example, addresses, changes in card numbers, mail passwords etc. This technique can be done utilizing JavaScript and Web server modules, and works in two sections. To begin with, the attacker causes a program window to be made on the target's machine, which appears normal but has minor changes and links that could redirect all the information to the attacker. These attacks are simply produced using a JavaScript or plug-ins. These do not require huge initiate by the target as it is enough even if the target visits a malicious website, or reads a malicious e-mail.



Literature Review:

Amit Kumar Tyagi (2014), A Novel Approach to Detect and Defence against Address Resolution Protocol (ARP) Spoofing Attack. This method uses detection and a defence mechanism. The detection mechanism used here is the (IDS) Intrusion Detection System. The defence mechanism used here is monitoring the sniffer thread using winpcap. This uses active probing technique to reduce the ARP traffic through the defence mechanism. This detection mechanism is efficient and self-operating as it does not require any external hardware application. This work does not serve the purpose to cure the complete ARP cache poisoning attack and it is a window OS based mechanism.

Non-technical spoofing:

Non-Technical spoofing is simply called spoofing which is not necessarily a computer based technique. This is just an idea through which the attacker finds an idea to steal the private or personal information of the victim. This technique on a broad perspective could even be as simple as calling a person and speaks to him pretending as a friend or someone who knew his personal secrets and tries gathering all his information. This when computer based becomes complicated as it could track all the details that the victim enters in his keyboard could be sniffed all under a protocol or an application that could either be web based, internet based or simply connected to any network with a DNS server.

E-Commerce Attacks:

E-Commerce is the major source of money making business which doesn't not involves money transaction as it is; instead it is done through banking. This is a method of creating a fake shopping site to sniff bank or card details including the card number and secret pin, further used for fraudulency and money making. This technique is a technique which involves fake URL's.

Ghazi Al Sukkar (2016), this method uses an attack module and defence module. Primarily the attack module uses a GUI interface for MITM attack, and then the defence attack has a protection tool for MITM attack. This attack is capable of identifying all IP addresses in the nearby vicinity connected in the particular network. The defence mechanism is facilitated efficiently to identify if the user is a victim of any attacker. This mechanism is restricted to one particular attack only eg: MITM or DoS attack. This could not simultaneously process two set of commands. Roopam & Bandana Sharma (2014), is a review paper on Prevention of DNS Spoofing. This method uses a 1024 public key, and its URL is generated, along with a generator, which is used to generate the public key for security purposes. This method has a highly secured key to prevent from man in the middle attack, eavesdropping attack etc. Security is as same as in 2048 public key size. Generating a in a large public key size is a tedious process. Sneha (2012), proposed an IP Spoofing Attack Detection using Route Based Information. This method uses a TTL mechanism for detection, which uses two values called the hop count (Hc) and hop count value (Hs), if equal the packet is legitimate, if else it is spoofed. Further the prevention technique uses a probabilistic marking technique, after the random number is generated; it is compared with the marking, if small the router sends it to the end address fields. The advantage here is that these routers could easily track the hash value of IP address of both 16- bit address and 32- bit address. It can only trace traffic of high volume, due to its probabilistic nature. Mridu Sahu & Rainey C. Lal (2012), developed a method for controlling ip spoofing through packet filtering. This method uses a prevention technique to prevent forge spoofing attacks, like the route based Distributed Packet Filtering Method to identify the attack and blowfish algorithm for the encryption and decryption in order to prevent IP spoofing. Blowfish algorithm uses sub keys which are used to cipher and decipher the text before and after the transmission and reception for high security. It is not easy to track or retrace the route as the packets are divided into left and right. This proposed method used blowfish algorithm which used too many sub keys that needs to be computed before every encryption and decryption process. Arumugam & Venkatesh (2012), proposed a Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm. The method proposed here is to detect the web spoofing attack using a traceback algorithm, which is an ant algorithm, which ensures the source and destination address requests, and changes the TTL values by decrementing the hop count value by one for every router. This uses a pheromone intensity check, and selects.

. CONCLUSION-

Network security plays an important role in deciding the efficiency of transmission in any network. There are several network threats like the spoofing attacks and its different types. Generally these spoofing attacks are simply directed to any one device connected in a network eg: man in the middle attack, worm hole attack, cache poisoning attack etc. but denial of service is the most vulnerable of all as it could be directed to a huge infrastructure at several ends. Network security to its very basic levels as the firewall and IDS technique are not sufficient enough to build in a secured wall against such attacks. Thus to be more clear about the security threats, this paper enables in understanding the various types of spoofing attacks and its techniques used.

REFERENCES-

Amit Kumar Tyagi, Surendra Kumar Tyagi, Prafull Kumar Singh, A Novel Approach to Detect and Defence against Address Resolution Protocol (ARP) Spoofing Attack, International Journal of Advanced Research in Computer Science and Software Engineering, 4 (2), 2014.

Arumugam N, Venkatesh C, A Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm, OSR Journal of Engineering, 2 (10), 2012, 09-16.

Bao Ho, Toan Tai Vu, IP Spoofing -A study on attacks and counter-measures, CS265 – Security Engineering, Spring 2003, San Jose State University, 2003. Brett Stone-Gross, Ryan Stevens, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna, Apostolis Zarras, Understanding Fraudulent Activities in Online Ad Exchanges, IMC '11 Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, ACM New York, NY, USA, 2011. Chris Sanders, Understanding Man-In-The-Middle Attacks, Part 4, SSL Hijacking, 9, 2010. Eric Hines Jamie Gamble, Non blind IP Spoofing and Session Hijacking, A Diary From the Garden of Good and Evil, 2002. Ghazi Al Sukkar, Ramzi Saifan, Sufian Khwaldeh, Mahmoud Maqableh, Iyad Jafar, Address Resolution Protocol (ARP), Spoofing Attack and Proposed Defense, Communications and Network, 8, 2016, 118-130.

Ghazi Al Sukkar, Ramzi Saifan, Sufian Khwaldeh, Mahmoud Maqableh4, Iyad Jafar, Address Resolution Protocol (ARP), spoofing attack and proposed defence, Communications and Network, Sci Res, 8, 2016, 118-130. Gori Mohamed J, Mohammed Mohideen M, Shahira Banu N, E-mail spoofing- An open threat to everyone, International Journal of Scientific and Research Publications, 4 (2), 2014.

Himani Grewal, Shivani, A Study of Ethical and Social Issues in E-Commerce, International Journal of Advanced Research in Computer Science and Software Engineering, 2 (7), 2012. Justin Ma, Lawrence K, Saul, Stefan Savage, Geoffrey M, Voelker, Identifying Suspicious URLs, An Application of Large-Scale Online Learning, Proceedings of the 26th Annual International Conference on Machine Learning, ACM New York, NY, USA, 2009.

Jyoti Chhikara, Ritu Dahiya, Neha Garg, Monika Rani, Phishing & Anti-Phishing Techniques, Case Study, International Journal of Advanced Research in Computer Science and Software Engineering, 3 (5), 2013. Kunal Pandove, Amandeep Jindal, Rajinder Kumar, Email Spoofing, International Journal of Computer Applications, 5 (1), 2010, 27–30. Mark Lin, An Overview of Session Hijacking at the Network and Application Levels, Date Submitted, GSEC Practical Assignment v1.4c (Option 1), SANS Institute InfoSec Reading Room, 2005. Mridu Sahu, Rainey Lal C, Controlling Ip Spoofing Through Packet Filtering, Rainey C Lal, Int J Computer Techology & Applications, 3 (1), 2012, 155-159. Niluka Jayamali N.Y, Munasinghe M.G.C.M, Ariyawansha I.C, Kumarathilake Y.A, Gunathilaka W.S.N, Perera R.D.G, Dhishan Dhammearatchi, Internet Protocol Spoofing in VOIP, Imperial Journal of Interdisciplinary Research, 2 (5), 2016. Pooja Kalola, Sachin Patel, Chirag Jagani, Web Spoofing For User Security Awareness, International Journal of Computer Applications & Information Technology, 3 (1), 2013.

Journal of Chemical and Pharmaceutical SciencesISSN: 0974-2115

JCHPS Special Issue 6: November 2016 www.jchps.com Page 34

Pratibha Thakre, Jaiswal A.N, Karale S.J, A study on various spoofing attacks and attackers on wireless networks, International Journal of Engineering Research & Technology, 3 (1), 2014. Rahul Rajaram Kandekar, Amol A, Phatak, A Review of Computer and Network Security, Novateur Publications, International Journal of Innovations in Engineering Research and Technology, 2 (5), 2015. Ramesh Babu P, Lalitha Bhaskari D, Satyanarayana CH, A Comprehensive Analysis of Spoofing, International Journal of Advanced Computer Science and Applications, 1 (6), 2010. Rengarajan Alwar, Sugumar Rajendran, Saravanakumar Selvaraj, Optimization Of Blind Spoofing Using Discrete Model, International Journal of Advanced Research in Computer and Communication Engineering, 1 (2), 2012. Robert Wagner, Jeff Bryner, Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks, Practical Assignment GSEC Version 1.2f, CISSP, GCIH-Gold, GCFA-Gold, SANS Institute Info Sec Reading Room, 2001. Roopam, Bandana Sharma, Review Paper on Prevention of DNS Spoofing, International Journal of Engineering and Management Research, 4 (3), 2014. Roopam, Bandana Sharma, Review Paper on Prevention of DNS Spoofing, International Journal of Engineering and Management Research, 4 (3), 2014, 164-170. Sanjeev Kumar, Orifiel Gomez, Denial of Service Due to Direct and Indirect ARP Storm Attacks in LAN Environment, Journal of Information Security, 1, 2010, 88-94.

Sneha S, Rana T.M, Bansod, IP Spoofing Attack Detection using Route Based Information, International Journal of Advanced Research in Computer Engineering & Technology, 1 (4), 2012. Srishti Gupta, Kirti, Jaya Chaudhary, A Review on Media Access Control Spoofing, International Journal of Engineering and Computer Science, 4 (4), 2015, 11301-11305. Steven H, Bass, Spoofed IP Address Distributed Denial of Service Attacks, Defense-in-Depth, SANS Institute.