IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-8, Apr 2019 E-ISSN: 2347-2693

Hijacking Spoofing Attack and Defence Strategy Based on Secured Network Protocols

B.Aravind[1*], D Murugan[2]

[1,2]Department of Computer Science and Engineering, MS University, Tirunelveli, India

Corresponding author: Aravind.gdr.cbe@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si8.6670 | Available online at: www.ijcseonline.org

***Abstract*—** Spoofing and Hijacking is a major threat in network security. Spoofing involves attacks that which are associated with the impersonation of third party to steal the credential information's from a network. Major IP spoofing attacks includes ARP spoofing attacks and DNS spoofing attack, which targets the server. This attack is also called as IP address forging which tries to take away the major information's from the organizations network systems. There are several tools available to prevent this intrusion prevention system. Some of them are snort, suricata, firewall, netfilter and IPfilter.Penetrating into the network can be prevented using be found using some testing tools like Nmap, Netcat and Hping. Certain attacks denial of service attack and man in the middle attack are more prone to these penetrating malicious threats. Therefore, it is mandatory to take necessary actions to prevent network from these attacks. Defensive strategies like filtering the packets, using an upper layer, using access control list and using a router that is encrypted in nature are encouraged to make the network secure. In this paper, various hijacking spoofing attack is analyzed and their preventive methods are mentioned to enable the network to be well secured. Certain specific protocols are encouraged to do this security measure to prevent the network attacks.

***Keywords*—** hijacking, spoofing, blindspoofing, zombie, cookie, ferret, wireshark.

I. INTRODUCTION

Session hijacking is a major threat in network security where the ongoing connection with a server will lose its connectivity for a period of time[2].The credentials like username, password and other secret information's will be steeled away by the attacker for that particular period of time. To be precise an unauthorised access is been given to a third party who acts as though he is serving from the system [3].Spoofing is an illegal trick to steel the security of the network.

Using certain strategies like ferret, hamster and Wireshark this session hijacking can be prevented. Ferret is a software tool that which checks the host to find out the vulnerabilities present in the system. It was originally designed to work on UNIX but later it was developed for windows [4]. Hamster is an external tool used by the networking devices to prevent the forgery of false and fake fingerprint readers. Wireshark is an analyser application, which uses the network protocol to analyse the traffic over the network. Major advantage of Wireshark is that this is a multi-platform supporting tool [7].

The main purpose of the contribution of this paper is that to prevent all the session hijackings like blind hijacking, hybrid hijacking, and a zombie attack on a network, cookie spoofing techniques and prevention mechanisms. Certain other strategies like fingerprint validation, session verification, innet strategy, outnet strategy are taken into consideration. On the conclusion part, we conclude by saying what steps we have taken to reduce the risk of server and other Dynamic Host Configuration Protocol (DHCP) being attacked [13].

In this research paper a detailed view of the hijacking and spoofing mechanisms are termed in detail. The corresponding defense strategy to provide security to the network protocol has also been suggested for a secured transmission of data packets. Hijacking can be termed as different types such as session hijacking, blind hijacking and hybrid hijacking.

II.VARIOUS SPOOFING AND HIJACKING ATTACKS

There are several types of network attacks among them few common attacks are IP address spoofing attack, fingerprint attack, zombie attack, and session hijacking attack.

A.IP Address spoofing attack

Spoofing in general happens at a different level more specifically in ARP Spoofing, MAC Spoofing, Blind Spoofing and Non blind spoofing. Blind spoofing is a method where the attacker can inject data into the stream of

packets without having a proper authentication itself when the connection is established at first stage. In this, the data packets are injected where the target is aware of the packets, which are got as sequence. A proper IDS (Intrusion Detection System) has to be used for security system of computer networks. This can be of Host-Based IDS and Network-Based IDS[5].Honey spots are identified at the first stage and soft spot which means the weak spot in the network has to be checked. After checking the weak soft spot, the IP address spoofing process starts. A prime example of IP address spoofing attack is given in the diagram below.

Consider an organization with the following configuration with following specifications.

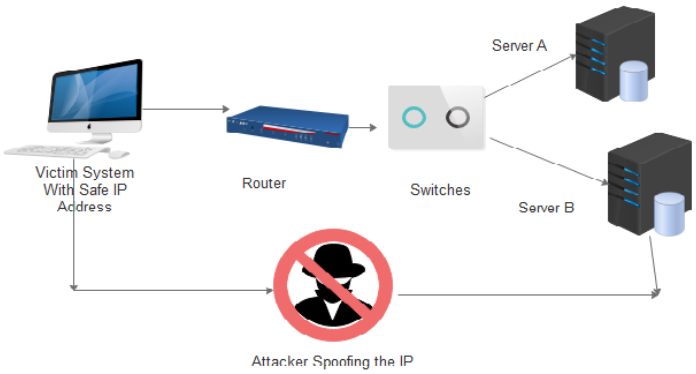

Fig 1: Representation of IP Spoofing Attack

The system to be attacked is been passed to a router and to a switch. Then it is been transmitted to two servers server A and server B.The IP address that is transmitted through the network is been attacked and spoofed by the attacker. Now the original IP address of the victims system that is the system been attacked is changed to another IP by the attacker [8]. Now the fake IP address, which is transmitted from the attacker, is been sent to servers and for users. This shows the IP been spoofed by the third party attacker.

B.Session Hijacking Attack

Hijacking a particular session of a network taking away all the credential information's from the network between client and server is termed as session hijacking attack. Denial of Service is more common to this type of attack. During session, hijacking attack an adversary sets up a fake point to access the hijackers. This attack is a mixture of DOS and man in the middle attack. A network sniffer is present in this attack. This attack leads the user to go to the fake website leading to take away all the information's like password and usernames. Cross-site scripting is used in hijacking the session of a particular network path. This stolen information's can lead to loss in integrity and confidentiality of the network systems [16]. This attack is more often in wireless network than in wired network. The session ID of victim and the fake masquerade authorized user, is the computer session been exploited. This is also termed as SHA (Session Hijacking Attack).A more detailed view of the organizations network is been given in the below system where the information of the network is been stolen and taken away by the attacker. Session hijacking leads to a major headache for networks that which are connected without a proper network throughout the organization.

Consider the following criteria happening in the below given system architecture.

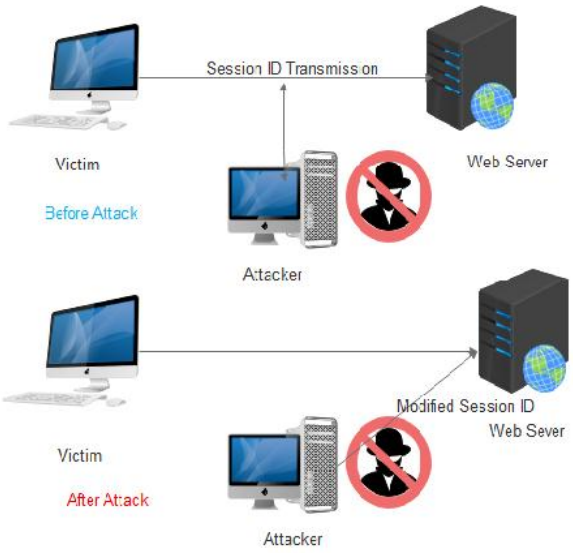

Fig 2: Representation of Session Hijacking Attack.

In the above system, the victim transmits a session ID from its end to web server. There is an attacker present illegally between two systems sniffing the session ID.This ID after been sniffed the attacker takes control of the entire system. The attacker will terminate the endpoint connection between client and the server [15]. Therefore this session is hacked and a fake session ID is been transmitted to web server which leads to sensitive information been taken away from the web server.

C. Zombie Attack

Zombies can be generally referred as spam or junk messages which are been transmitted to a particular system to make it a malicious thing. Spam zombie detection scheme blocks the emails and mail server that which transmits the junk of data. SPOT is a lightweight spam zombie detection system, which detects the intrusion detection system as required by the bothunter.Mails which are designated from various sources comes into the zombie and they all together form an attacked system, which can cause heavy damage to the system of the organization. Spam zombie algorithm is available to find out the zombie-attacked system [10]. Emails servers provide the

junk of the zombie system where enormous amount of information is been involved for the system to developed. An organization with different zombie attacked system is been given below and their functionalities are termed below. Zombies plays a vital role in network security by sending junks of data an mails throughout the system network enabling the organization to cause damage to the system and to define the problems.

Consider an organization with the following configuration with following specifications.

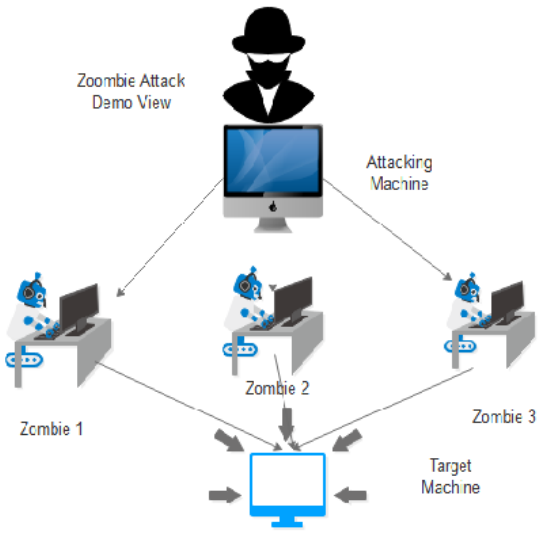

Fig 3: Representation of Zombie Attacked System

The attacker has assigned three systems to act as zombie to attack the main system. After getting all the junk messages and emails from across all the sections the zombies just passes the information's from one system to another. The attacking machine on receiving information to be theft from the system gives the zombie system with each task. The targeted machine will then be attacked by the various junk messages to jam the main system. This is working of zombie attack.

III. STRATEGIES TO PREVENT NETWORK ATTACKS

There are plenty of methods and techniques to prevent network attacks. Some of the network attacks are mentioned in this paper with their diagrammatic representation. Some common methods are using Wireshark tool, in network strategy, out network strategy been implemented.

A. Wireshark Tool

Wireshark is a network protocol application to analyse the data packets been transferred from one section to the other. This is a multi-platform supportive tool, which supports Linux, Mac OS and BSD platforms as well. This tool can be used to prevent the system from being been affected by the external internet traffic. When huge traffic comes to a webserver intented to attack a network Wireshark will provide as a supportive tool to the operating system with the traffic been not affected by the network. Wireshark can capture the data and include PROFINET by using a capability to discovering the topology of network to work on the required spots. Network experts use Wireshark as a troubleshooting tool and for analysing the security issues [7]. Protocols such as TCP/IP, MAC, IP datagram and the data transmission of PDU can be seen and analysed using the Wireshark tool. Hence, this tool is a good analyser and security tool for making the network connections more secure.

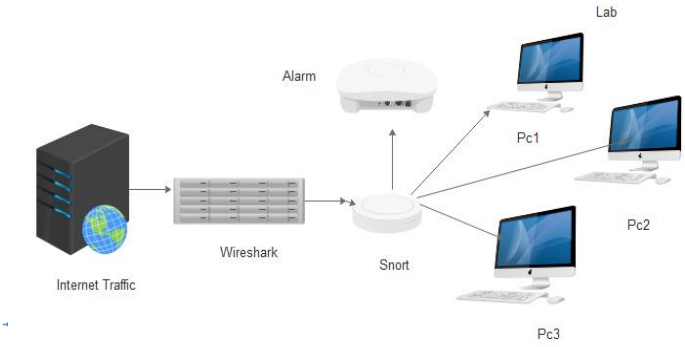

Fig 4: Representation of a system that is protected by Wireshark

In this system architecture a system with heavy internet traffic is been sent to jam a network system. A Wireshark is present in-between the network. Snort and an alarm is kept for analysing and sending alarm to inform the incoming internet traffic. It analysis and divides the traffic according to the organisations needs and splits up into various parts. The snort will be then divided into different PCs.Hence Wireshark provides, as a block between the networks been not being damaged. It analysis the traffic and sends the needed data and blocks the unwanted data as an integral part of a network.

B. In network Strategy

This is a unique method of preventing network security where there will be two firewalls one on the outer and one on the inner firewall. The organisation is double protected with the firewalls on both the sides before exposing the network to the internet exposure. This serves as the double-blinded system.

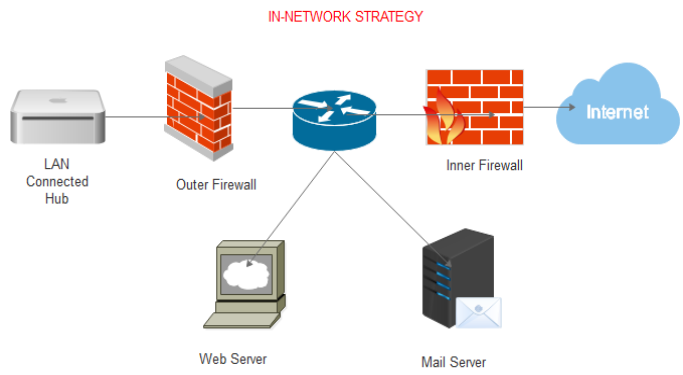

Fig 5: In network Strategy Representation

In the above system, the Router is present in-between two firewalls thus providing which access to be given to the required system. The router sends the data to web server and to mail server. Hence it is provided between two walls whereas the data integrity is been protected by having the double protection. This strategy is followed in many of the companies and organization, which handles very confidential data like bank and government websites.

C. Outnetwork Strategy

Out network strategy is a method of giving out the internet sources to outer systems that which are present in the environment in an open account to be accessed by the individual users controlled system. The below picture shows the representation of out network strategy of networking system.

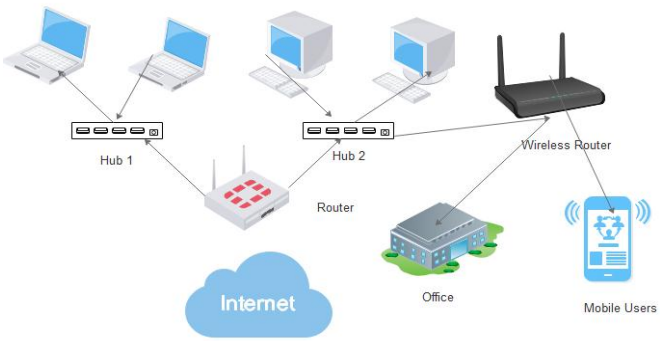

Fig 6: Out Network Strategy Representation

A massive amount of internet is been provided by the internet provider to the router at initial stage. After it gets give, the internet from the provider the router divides the network into for hubs. The hubs transfer's data for the systems present in the organisation. In extend to this a wireless router is present which provides access to the Wi-Fi enabled zone such as mobile users and office providers. This method is followed in organisations where the architecture of the system is well formed without leaking any confidential information's from the source to destination. This is the overview of the out network strategy of the system.

D: Other Techniques to provide defence strategy for network protocols.

Apart from the above-mentioned techniques, there are other strategies to prevent the network attacks by using a proper filter to avoid the proxy, using ferret and hamster strategies. Using proper filter is a good technique that which can be applied in order to provide a good security for networks. Filtering the data packets based on the nature of the source whether it contains any harmful contents or malicious natured codes to threaten the network system to be collapsed. Ferret is another technique, which can be analyzed to choose what type of attacks to be caused by individual networks. Hamster is another network security-providing tool, which helps in finding the network faultering.This tool uniquely provides the entire network from to be being accessed by an illegal third party attacker.

IV.RESULTS AND DISCUSSION

The main features and findings of this paper includes

1. *Intimating the Hijacking*, which includes whether the incident happened, is a hijack or not. More common Problem first faced is the suspicious activity is an attack or any ordinary network cracks.
2. *Identifying what has happened* in the network is the next factor of the work that which has been carried out. It is necessary to analyse what sort of attack has happened in the network and the need is must to be fulfilled.
3. *Find out whether the thing happened is an attack* is another foremost thing, which has been carried out because not every single activity can be termed as attack.
4. *Amount of detection been found* is another major role because the security has to be preserved well enough in order to give the attackers a solution.
5. *Respected solution for attacks*, which has happened, is the next thing, which has been studied in this paper. This has resulted in providing multiclient with the feature of providing a well-supervised material to execute the attacks, which has happened. We do not want to use big firewalls to get a secured network authentication. Just these preventive actions will do a great doing for the given organisation. Almost 65*/* of detection is increased because of the system that we have proposed. This also provides and supports multiclients, which prevents zombie attack. Detection rate can be improved by using the server broadcasts that which we can use some secured data mechanism such as, DHCP (Dynamic Host Configuration Protocol) where the management of network usually gets to use to assign dynamically the Internet protocol address to any device or any node or any particular network for which the security needs to be provided

V.CONCLUSION AND FUTURE SCOPE

.Future scope of the networkingincludesDHCP.Dora (Discovery, offer, request, acknowledgement) process, which exists in this paper for a future work to be discovered. Dora is a process of handling the servers that which distributes dynamically the network configuration parameters such as IP addresses interface methods and their services. This is been standardized by following network protocols used in the network communication. Discovery includes the network sub netting that is followed by destination address.DHCP offer provides a DHCPDISCOVER message from a client where it receives the IP address that is to lease the request from the server[15].DHCP request is followed up with a client server connection thus leading to a well secured authentication scheme. Acknowledgement includes the receipts to be involved in the system to enable the data packets to be included in the duration and other configurations. The final IP configuration can be done in this system.

REFERENCES

[1] Abdullah H. Alqahtani, Mohsin Iftikhar,"*International Journal of Science and Modern Engineering",* Volume-1, Issue-10**,** September 2013.

[2] Saurabh Jha, Shabir Ali, *"Mobile Agent Based Architecture to Prevent Session Hijacking Attacks in IEEE 802.11 WLAN*" International Conference on Computer and Communication Technology,2014.

[3] Vanajakshi, Srikanth Prabhu, "*An Effective Method for Preventing SQL Injection Attack and Session Hijacking"* IEEE International Conference On Recent Trends in Electronics Information & Communication Technology 2017.

[4] Nitin Anand, Anil Sharma, *"Ferret: A Host Vulnerability Checking Tool",* Proceedings of the 10th IEEE Pacific Rim International Symposium on Dependable Computing, 2004.

[5] Matin Tamizi, Matt Weinstein, *"Automated Checking for Windows Host Vulnerabilities",* Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering.

[6] Resul Das, Gurkan Tuna*,"Packet Tracing and Analysis of Network Cameras with Wireshark*",IEEE,2017.

[7] Shaoqiang Wang, DongSheng Xu,"*Analysis and Application of Wireshark in TCP/IP Protocol Teaching",*International Conference on E-Health Networking, Digital Ecosystems and Technologies, IEEE 2010.

[8] Auttapon Pomsathit, *"Effective of Unicast And Multicast IP Address Attack Over Intrusion Detection System with Honeypot"* U.S. Government work not protected by U.S. copyright.

[9] Pooja Sharma, Sanjeev Kumar**, "***BotMAD: Botnet Malicious Activity Detector Based on DNS Traffic Analysis",* 2nd International Conference on Next Generation Computing Technologies, 2016.

[10] Zhenhai Duan, Peng Chen, Fernando Sanchez, *"Detecting Spam Zombies by Monitoring Outgoing Messages"*,IEEE.

[11] Thawatchai Chomsiri, *"Sniffing Packets on LAN without ARP Spoofing*" Third 2008 International Conference on Convergence and Hybrid Information Technology,472-477.

[12] S .Raguvaran,"*Spoofing Attack: Preventing in Wireless Networks*" International Conference on Communication and Signal Processing, April 3-5, 2014,117-121.

[13] Nikhil Tripathi, "*Neminath Hubballi Exploiting DHCP Server-side IP Address Conflict Detection: A DHCP Starvation Attack*".

[14] Yongle Wang/s, JunZHang CHen/s," *Hijacking spoofing attack and defense strategy based on Internet TCP sessions*", 2013 IEEE 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation,507-509.

[15] Enos LETSOALO, Prof Sunday OJO,*"Session Hijacking Attacks in Wireless Networks: A Review of Existing Mitigation Techniques*" IIMC International Information Management Corporation, 2017.

[16] Jeffrey Cashion and Mostafa Bassiouni *"Protocol for Mitigating the Risk of Hijacking Social Networking Sites"* International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, Florida, USA, October 15-18,2017.

[17] *Veysel Harun "TOPOLOGY DISCOVERY OF PROFINET NETWORKS USING WIRESHARK"* 2013 IEEE.

[18] Pedro R. M. In´acio, Paulo P. Monteiro,*" Zombie Identification Port"* The Third International Conference on Internet Monitoring and Protection,67-73.

[19] Zhenhai Duan, Peng Chen, Fernando Sanchez,*"Detecting Spam Zombies by Monitoring Outgoing Messages",* IEEE INFOCOM 2009 proceedings.

[20] Feng Luo, *"Method and Implementation of Building ForCES Protocol Dissector Based on Wireshark"* 2010 IEEE.

Authors Profile

Mr.B.Aravind M.E(PhD) is a full time research sholar in MS University Tirunelveli.He did his BE and ME in Computer Science and Engineering in Sri Krishna College Of Engineering and Technology,Coimbatore.He started his carrier as programming trainee and software tester in DCPL software private limited Trichy.He then worked as Assistant Professor in Department of Computer Science and Engineering in CSI College of Engineering,Ooty for Four Years.He also served as Data admin in chinmaya central mission trust for one year.He is a Life time member of ISTE.His area of interest includes Network Security.He is currently pursuing his PhD degree in the area of network security.Having a rich experience in Networking and software testing domain he has delivered many guest lecturers and nurtured many students towards success.

Dr.D.Murugan is currently serving as Professor and Head in Department of Computer science and engineering in MS University Tirunelveli.He has more than 24 years of rich teaching experience.He has published 12 papers in national and international journals.He has published more than 20 papers in national and international conferences.He has also published 3 books which are indexed to springer.He has received a grant of 24 lakh from UGC major project and DST-SERB which has been successfully completed.He holds a number of positions in general bodies such as coordinator for ICTACT,Syndicate member of university and integral part of inspection committee in various colleges.He plays an integral part in the development of students and staff community.

