Comprehensive Security Mechanism for Defending Cyber Attacks based upon Spoofing and Poisoning

Alok Pandey[1] and **Jatinderkumar R. Saini**[2]

Submitted in April, 2016; Accepted in July, 2016

Abstract – Much attention needs to be paid to different types of security threats and related attacks in the LAN and the interconnected environment. A variety of controls and counter mechanisms covering different layers of TCP/IP protocol suite are already available. But most of them have several issues related to cost, compatibility, interoperability, manageability, effectiveness etc. and hence multiple protection devices need to be installed.

In this paper we propose a comprehensive security mechanism which can detect and guard against a variety of spoofing and sniffing based cyber attacks in the local area networks. The solution does not require any additional hardware and is fully backward compatible with existing versions of ARP as no modifications are required to the existing LAN protocols. It also provides necessary detection and mitigation mechanism for the common type of DoS, MITM attacks & provides mobility along with a consistent working environment to the users as they roam around on different networks

Index Terms – ARP Spoofing, Denial-of-Service (DoS), LAN, Man-In-The-Middle (MITM), Security

1.0 INTRODUCTION & RELATED WORKS

Although a lot of effort has been made by the research community for securing the network based communication, but still there are problems which need to be resolved. More attention needs to be paid to different types of security threats and related attacks in the LAN and the interconnected environment. Malicious users can launch different types of network attacks based upon the sniffing and spoofing techniques and gather information which could be used for penetrating further into network for thefts and damages to data.

TCP/IP protocol suite was initially developed with the prime consideration of communications and as such much attention was not paid to concerned security aspects. Attackers are exploiting some of the known weaknesses of the individual protocols like ARP, ICMP, IP, TCP and UDP etc. of the TCP / IP suite.

[1]Senior Systems Manager, Birla Institute Of Technology, Mesra, Jaipur Campus, Rajasthan, India, Email Id: alokpandey1965@yahoo.co.in

[2]Professor & I/C Director, Narmada College of Computer Application Bharuch, Gujarat, India, Email Id: saini_expert@yahoo.co

Some common attacking strategies adopted by attackers are by way of Intrusions, Denial of Services [1] (DoS and DDoS), Interception and re-routing of the communication.

In a typical LAN environment, internal user can launch different types of network attacks based upon sniffing, spoofing techniques and capture sensitive information like user name, passwords, IP addresses, port numbers and other proprietary data [2] and use it for penetrating further into network for thefts and damages to data.

Capturing and analyzing a TCP/IP packet on a network for stealing network based information is called Sniffing [3]. Another well known technique for launching attacks in network environments is Spoofing[4]. This underlines the need for reliable techniques for detection of sniffing and spoofing based activities and related attacks on the network.

Attackers craft and inject bogus packets by exploiting the feature of Raw Socket Programming which is offered by most of the programming languages today. Spoofing is the process of creating and injecting fake TCP/IP packets with some one-else's identification on networks [5] whereas in MITM the entire session is hijacked by the attacker for stealing of data.

Protocols like IP and ARP are exploited [6] for launching attacks like Port Scanning, ARP Cache Poisoning, Changing of Default gateway, ICMP redirect, DHCP poisoning, DNS poisoning etc. Based upon IP spoofing, which involves forging of IP addresses of the source device, different types of attacks can be launched [7] whereas attacks like DoS and MITM can be achieved using ARP spoofing.

Address Resolution Protocol (ARP) is used for finding out the MAC address [8] of the destination device on a LAN. ARP stores such mappings of IP addresses to MAC addresses in temporary storage called cache for future usage [9]. This cache is updated from time to time. Whenever the system has to transmit a frame it first checks its ARP cache for locating the corresponding MAC address of the receiver[10]. It uses two types of messages namely ARP request and ARP reply which are encapsulated inside an Ethernet frame. It contains MAC addresses of sending and receiving devices along with a value of 0x0806 in Ethernet type [11]. The frame also contains the IP and MAC addresses of the sender and receiver along with an operation code as part of the ARP message.

The entries to the ARP cache can be added either statically or dynamically[12]. For supporting the DHCP enabled hosts, these entries are removed periodically form the cache. The devices update their ARP cache whenever they receive an ARP Reply even if they had not sent out the corresponding ARP request earlier as ARP is stateless protocol [13,14]. Thus,

despite its crucial importance ARP provides ground for launching ARP spoofing & ARP cache poisoning attacks [12].
For genuine communication both Ethernet and ARP headers should match. But since there is no mechanism to check consistency of these headers, attackers intentionally craft packets having different or forged values of IP-MAC addresses [15,16,17,18]. This is called ARP Cache Poisoning.
Thus attacker modifies the entry for gateway or any other genuine host with mapping of their IP Addresses and its MAC address in ARP Cache of victim system. After this a variety of attacks can be launched [14, 19] namely Denial of Service (DoS) attacks, Man in the Middle (MITM) attacks etc. The attackers craft different types of packets based upon IP, ICMP, TCP, UDP etc protocols and try to disrupt various functionalities of the network.
A variety of controls and counter mechanisms like Antivirus, Anti Spam, Anti Malware, Encryption and other related software covering different layers of TCP /IP protocol suite are already available. Some higher-end expensive hardware and software based devices like Switches, Firewalls, IDS, UTM etc. are also available for mitigating specific types of individual or group of attacks at various layers. But most of them do not cover the range of Sniffing, Spoofing, ARP Poisoning, Packet Crafting for Port Scanning and Flag Manipulation based DoS attacks actually taking place. Besides these, the issues related to cost, compatibility, interoperability, manageability, effectiveness etc. are also involved As a result multiple protection devices need to be installed.
Although solutions based upon Static ARP Cache entries to prevent ARP spoofing attacks exist yet they have some major issues like effort required for manual configuration of static entries, limited scalability and workability in static and DHCP based networks [14]. Some of the typical works done in this category include the DAPS (Dynamic ARP spoof Protection System- Cisco^{R}) technique suggested in [20] which is a solution to ARP spoofing that snoops DHCP packets. Katkar et al. [21] have proposed a light weight approach for prevention & detection of ARP Spoofing. A server based solution has been proposed by Ortega et .al. [22]. Another mechanism to prevent ARP spoofing based upon the use of static ARP entries was suggested by Ai-Zeng Qian[23]. A combination of using static ARP entries and SNORT-IDS is suggested in [24] for resolving the ARP spoofing problem.

2.0 METHODOLOGY

In this paper we propose a comprehensive security mechanism which can detect and guard against a variety of spoofing and sniffing based cyber attacks generated by exploiting some inbuilt vulnerabilities of heavily used major protocols of the TCP / IP suite such as ARP, IP, ICMP, TCP and UDP protocols from both the internal and external attackers.
The proposed solution performs cross layer inspection, identifies invalid combinations of Source and Destination IP addresses and MAC Addresses, performs Port Scanning, restores the Default gateways and helps the victim machine to recover from Spoofing and Poisoning based attacks in the Local Area Networks. The solution does not require any additional hardware and is fully backward compatible with existing versions of ARP as no modifications are required to the existing LAN protocols.
It also provides comprehensive detection and mitigation mechanism for the common type of Denial of Services attacks that are based upon IP, ICMP, TCP, UDP etc. protocols.
The proposed solution also aims to provide mobility and a consistent working environment to the users as they roam around on different sub networks of the corporate network which might be geographically dispersed. The proposed solution comprises of 4 Modules that work in the client server environment as follows:-
Module 1 focuses upon User Registration, Validation and Log on. Here the user is required to register and provide the required details as can be seen in Figure1. After the initial registration the user gets user name, password, an authentication code and location code which are used for logging on the network and getting the IP from the respective DHCP Server for that location [25].

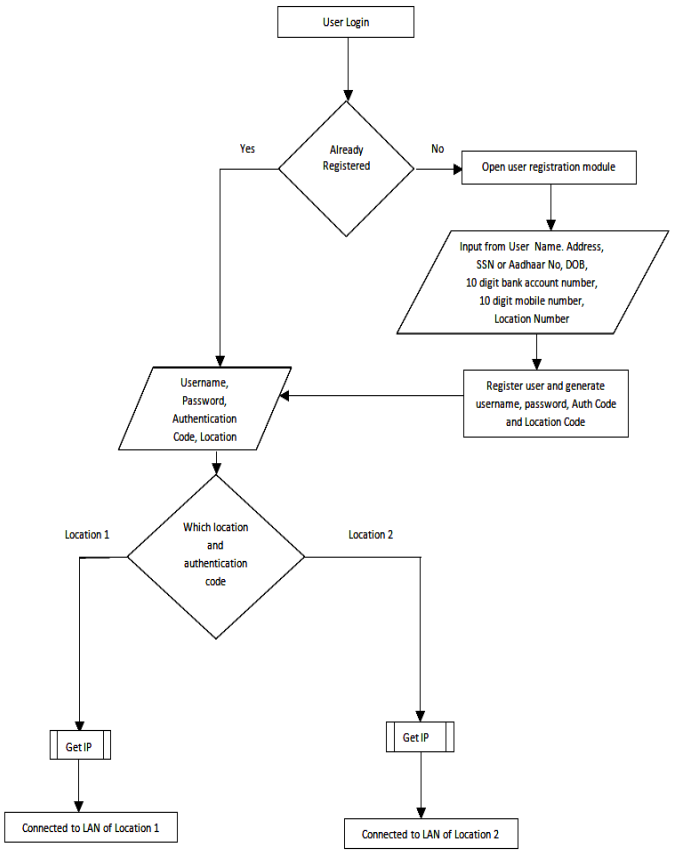

Figure 1: Client Side Flow Chart for user registration

Module 2 focuses upon the Client Side Processing. After the initial registration and verification process the client side portion takes over and provides the functionality of closing the

undesired Open Ports of the system, Restoration of Default Gateway, Discovery and Reporting of the neighbors to the server and updating of the ARP Cache with the processed contents from the server. Figure2 shows process of discovering the neighbors.Another flowchart as shown in Figure3 depicts the procedures that run and scan for open ports of the system. It then selectively closes undesired open ports based upon user confirmation. It also flushes and updates the ARP Cache of the client system based upon the authenticated updates as received from the Server side from time to time.

Module 3 focuses upon Server side Processing and performs the Genuine Host Detection, Cross Layer Verification, Final Node Detection, Updating Of Client ARP Cache, Locating and eliminating attacker etc using secure data exchange as shown in flowchart in Figure4

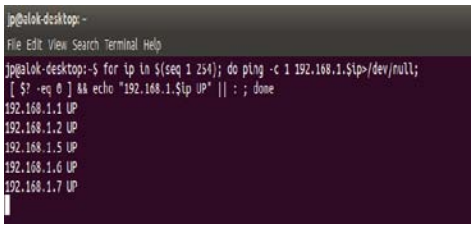

Figure 2: Client Side Scan for Active Hosts on the LAN

For detecting genuine MAC and IP Addresses of clients on the network, data regarding the active hosts on the LAN is collected using different mechanisms such as Reporting from the Clients, Lease Table of the individual location based DHCP servers for that network and Sniffing of packets on the network.

All the entries found common in all the three are recorded in the genuine host table. Other entries which are not common in all the three are recorded in the suspicious host table.

The mechanism also performs cross layer examination as seen in Figure5 and detects the invalid MAC Address – IP Address combinations by comparing the Ethernet and ARP headers [1,5,19].

If both source and/or destination MAC addresses are not identical as seen in Figure5, it means that ARP spoofing is happening on the network. The valid MAC address packets are recorded for further processing and physical node detection process.

The Final Node Detection and Cross Verification is done to verify the existence of the physical host on the network by sending ICMP ping packets to the combination of IP-MAC address pairings as recorded earlier. For the ones where no reply is received the second layer of verification is done by sending a TCP SYN packet using the details of the detected IP and MAC Address combination.

If the host is there on the LAN it will respond back with SYN / ACK or RESET packet [26]. Such entry is to be recorded in the genuine host table and passed to the client for updating its ARP Cache [27]. In case of no response then the entry is passed to the spoof alarm and counter measure mechanism for blocking the host on the network.

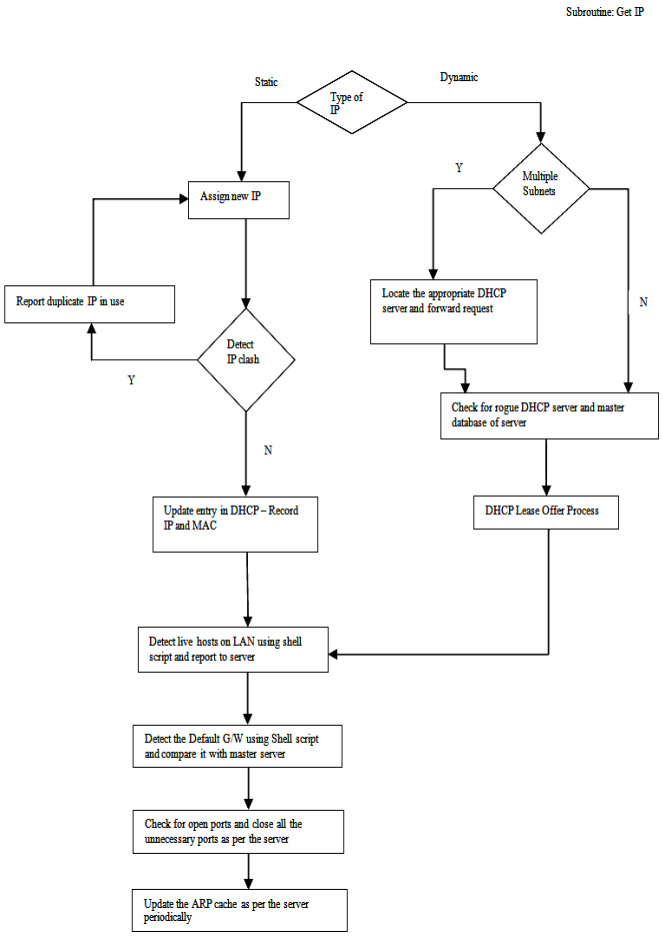

Figure 3: Client Side Flow Chart

The entries that finally pass all the tests are sent to the client for updating the respective ARP cache. The existing cache of the client is flushed out by deleting all the available entries and updating the ARP cache of individual client after a specified time period with the genuine set of valid entries as sent by server side.

Based upon the list of IP – MAC combination that failed to respond to either ICMP Ping Or SYN Scan, the administrator can eliminate such malicious hosts from the network if desired. In order to protect the inter-host communications during the entire process communications encrypted data exchange is done between the client and server portions and also for communicating with DHCP servers on the different sub networks.

Module 4 focuses upon Prevention of Common type of DoS [31] attacks that are created using abnormal packets of TCP, UDP, IP, ICMP etc. which are purposefully crafted by attackers and injected into the networks so that the existing devices like Servers, Workstations, Computers, Firewalls, IDS and other

interconnecting devices like switches, Routers, Gateways etc. and the supporting software either malfunction or crash [28]. The adversary purposefully creates the abnormality so that the filtering devices like firewalls and IDS are cheated and the packets pass through them without being blocked and ultimately result in system crashes. For the purpose of creating problems an adversary manipulates theses fields and crafts packets that are either incomplete or have wrong values.

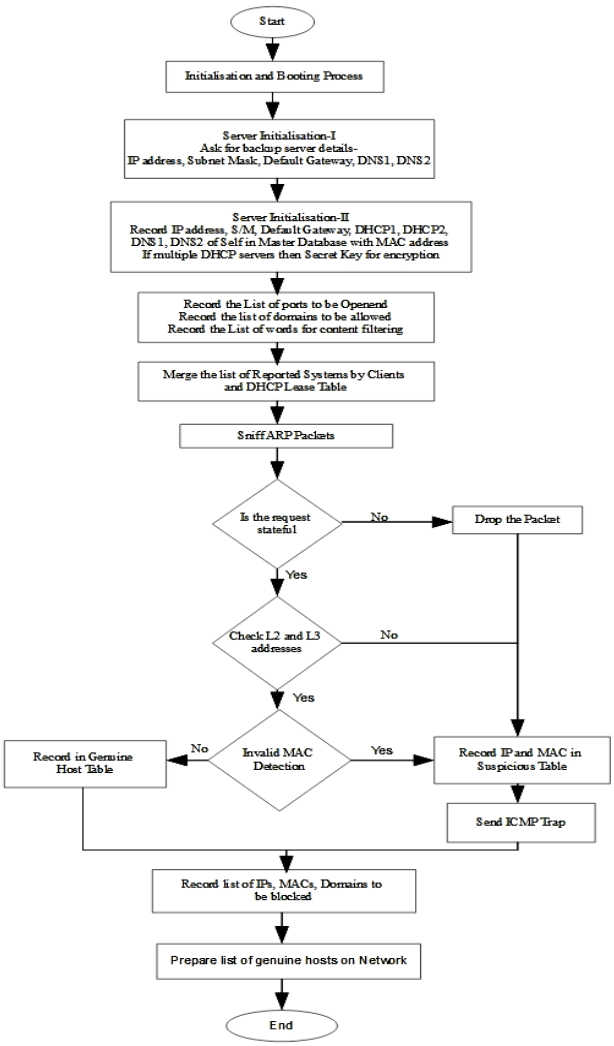

Figure 4: Server side Flow Chart

This portion filters out the abnormal packets which are deliberately crafted by the attackers to launch different types of attacks. The mechanism filters out the Abnormal IP packets which either have Unknown Protocol Type in the IP Header or are abnormally fragmented like illegal offset values, overlapping fragments, or if the first fragment is very small.

Like-wise the proposed solution is capable of filtering out the abnormal TCP Packets also. TCP uses a combination of six flags to indicate specific functionality or meaning of the current packet and its contents. Each flag is of one bit and has a specific meaning or functionality associated with it for example some TCP segments carry data while others are used for acknowledgements of the received data.

Figure 5: For cross layer examination

Out of these flags the most popular flags are the "SYN", "ACK" and "FIN", which are used for establishing connections, acknowledging and terminate connections. A SYN packet (Synchronization) is used for initiating a TCP connection whereas an ACK indicates that contents have been received and the device is ready to accept further packets. The 3-way handshake mechanism is based upon these packets and is used to ensure that both the sender and the receiver are ready to communicate before the actual transmission of data is done from either side.The detailed functional specifications for TCP are defined in RFC 793. Packets with other flag combination should be treated as suspicious. The attacker can use such illegal combination to identify the operating system at the victims system and then exploit some of its known vulnerabilities to further penetrate into the system. Sometimes such illegal combinations may go undetected through firewalls and intrusion detection systems or may crash the victim target device.

Some of the commonly seen invalid combinations for TCP may include packets with TCP Headers having both SYN and FIN Flags Set or having SYN, FIN and PSH Flags Set or SYN FIN RST Flags Set or SYN FIN RST PSH Flags Set or having only FIN Flag without ACK Flag Set or ALL Flags Set or no Flags Set at-all or SYN Flags set but containing data. Other illegal forms may include the Source or Destination Port Numbers set to 0 or packets having ACK Flag set but the Ack Number set to 0 etc. [5, 12, 17]

The proposed solution is capable of filtering the abnormally crafted UDP packets. UDP is another Protocol that is available at the transport layer. It is a connectionless protocol with very little services. It is also available in the standard deployment of the TCP IP protocol suite. Both TCP and UDP have source and destination ports. Protocols like DHCP, SNTP, DNS and TFTP use UDP as a transport mechanism [17,29,30]. The abnormal UDP packets may contain zero as either source or destination port numbers or the packet may be illegally fragmented or attacker may flood victim devices by sending multiple UDP packets with same IP address or same port numbers. [5,12,17] .

Similarly the proposed solution is also capable of filtering out the Abnormal ICMP packets, which are fragmented or redirect everything to itself or larger than 65,535 bytes or echo request packet containing data or multiple ICMP packets with same Destination IP Address [5, 12, 17, 29, 30].The communication between the client and server portions is encrypted using the encryption key which may be generated using government / authenticated individual identifications like driving license, passport number or other related information provided by the user at the time of initial registration.

3.0 EXPERIMENTAL SETUP & RESULTS

The test network consists of a network of three computers. We have used a system with two LAN cards to provide the functionality of a Router, DHCP Server and testing of the conditions. One of the machines acts as an attacker machine and is loaded with packet crafting software for generating malicious packets and injecting in the network. Wireshark was used for verification of the successful injection of such in the network..

Different types of ARP, IP, TCP, UDP and ICMP packets were crafted and injected in the network by the attacker system. Several packets with invalid source MAC Address, Destination MAC Address, Source and Destination Port Numbers, illegal flag combinations, were generated and injected in the network. Proper filter conditions to filter out such bogus packets were implemented at the Routing system.. Screenshots were taken before and after implementing the filter conditions at the victim machine. Wireshark was also run at the victim to capture and display the packets. Some of the screen shots are included herein. Figure6 shows that Packet with SYN, FIN, PSH, RST has been dropped at the Filtering System after applying the filter conditions.Figure7 shows that UDP Packet with destination port having 0 value was dropped by filter system after applying filter conditions. It can be observed that the crafted packets with illegal or invalid parameters by the attacker system are being filtered out and thus the victim system is protected against different types of DoS and MITM attacks.

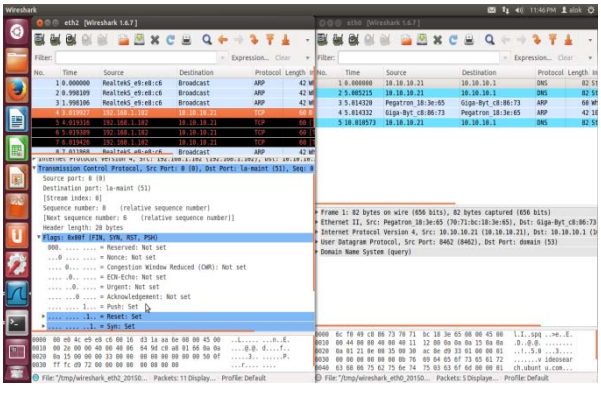

Figure 6: Packet with SYN, FIN, PSH, RST has been dropped after applying the filter conditions

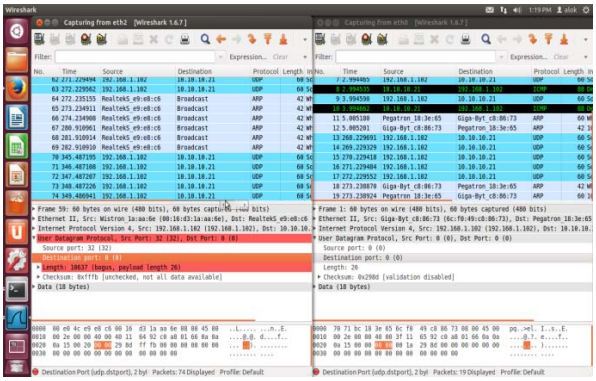

Figure 7: UDP Packet with d-port 0 value are dropped by filter system after applying filter conditions

4.0 CONCLUSION

In this paper we have highlighted the security based issues of Local Area Network and shown how some of the known vulnerabilities of the basic protocols of TCP / IP protocol suite can be exploited to launch different types of attacks. The proposed solution incorporates cross layer inspection, identifies invalid combinations of source and destination IP addresses and MAC addresses, port scanning, restoring of default gateways and helps the victim machine to recover from Spoofing and Poisoning based attacks in the Local Area Networks. The proposed solution does not require any additional hardware and is fully backward compatible with existing versions of ARP as no modifications are required to the existing LAN protocols.

The aim of this paper is purely academic research and to spread awareness amongst the network administrators and other related persons who manage, maintain and guard the networks against such attacks in LAN and WAN environments. Though highlighted, we do not intend to promote attack mechanisms nor defame any proprietary or open-source network defense tools already existing in market, we acknowledge all of them.

REFERENCES

[1] Kilari N.&Sridaran R .- *"The Performance Analysis of N-S Architecture to Mitigate DDoS Attack in Cloud Environment"* INDIACom-2016; IEEE Conference, BVICAM, New Delhi

[2] Pandey A., Saini J. R. "*Study of Emerging Trends of Cyber Attacks in Indian Cyber space and their Countermeasures"*International Journal of Computer Science & Communication Networks 2249-5789

[3] Nagpal B. & Sharma P. – *"DDoS Tools: Classification, Analysis and Comparison "* , INDIACom-2015; IEEE Conference, BVICAM, New Delhi

[4] El-Hajj, Zouheir Trabelsi and Wassim, *"On investigating ARP Spoofing Security Solutions"*, International. Journal of Internet Protocol Technology, Inrscience Enterprises Ltd., 2010, Vol. 5.

[5] S. G. Bhirud. "Light weight approach for IP-ARP spoofing detection and prevention", 2011 Second Asian Himalayas International Conference on Internet (AH-ICI), 11/2011

[6] Vidya S., Gowri N. and Bhaskaran R. – *"ARP Traffic and Network Vulnerability "* , Proceedings of INDIACom-2011; IEEE Conference, BVICAM, New Delhi (INDIA)

[7] Mateti, Prabhakar. [Online] http://cecs.wright.edu/~pmateti /Courses/4420/Probing/index.html [Accessed: November 2012]

[8] Sharma D., Khan O. andManchanda N. – *" Detection of ARP Spoofing: A Command Line Execution Method"*Proceedings of INDIACom-2014; IEEE Conference, BVICAM, New Delhi

[9] Khaled Shuaib. "NIS04-4: Man in the Middle Intrusion Detection", IEEE Globecom 2006, 11/2006

[10] F. A. Barbhuiya. "An Active Host-Based Detection Mechanism for ARP-Related Attacks", Communications in Computer and Information Science, 2011

[11] Kumar, Sumit, and ShashikalaTapaswi. "A centralized detection and prevention technique against ARP poisoning", Proceedings Title 2012 International Conference on Cyber Security Cyber Warfare and Digital Forensic (CyberSec), 2012

[12] Mohamed Al-Hemairy, Saad Amin, and Zouheir Trabelsi."*Towards More Sophisticated ARP Spoofing Detection/ Prevention Systems in LAN Networks"* : CTIT, December 2009.

[13] Barbhuiya, Ferdous A., Santosh Biswas, NeminathHubballi, and Sukumar Nandi. "A host based DES approach for detecting ARP spoofing", 2011 IEEE Symposium CICS, 2011

[14] M., Ahmed, Wail S. Elkilani, and Khalid M. Amin. "An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries", International Journal of Advanced Computer Science and Applications, 2014.

[15] J.C.Gondim, Marco Antonio Carnut & Joao., *"Arp Spoofing Detection on Swtched Ethernet Networks:A Feasibility Study"*: Symposium on Security in Information Practices, Nov. 2003

[16] Mohamed Al-Hemairy. "Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks", 2009 CTIT, 12/2009

[17] Trabelsi, Zouheir. "Hands-on lab exercises implementation of DoS and MiM attacks using ARP cache poisoning", Proceedings of the 2011 Information Security Curriculum Development Conference on - InfoSecCD 11

[18] Pandey A., Saini J. R. *" Counter Measures to Combat Misuses of MAC address Spoofing Techniques"* IJANA Vol. 03, Issue 05, 0975-0282

[19] I.Bonilla, Christina L.Abad and Rafael"*An Analysis on the schemes for Detecting and Preventing ARP cache Poisoning Attacks"*, 27th International Conference on distributed Computing system Workshops, June 2007. ICDCSW'07

[20] Masuai, Soumnuk Puangpronpitag & Narongit."*An Efficient and Feasible Solution to ARP Spoof Problem"*, 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology , 2009. (ECTI-CON 2009)

[21] Katkar, Dr. S. G. Bhirud and Vijay."*Light Weight Approach for IP-ARP Spoofing Detection and Prevention"*: Second Asian Himalayas International Conference on Internet , November 2011. (AH-ICI)

[22] Andre P. Ortega, Xavier E. Marcos, Luis D. Chiang and Cristina L. Abad."*Preventing ARP Cache Pisoning Attacks: A proof of concept using OpenWrt"*.: Latin American Network Operations and Management Symposium, October 2009. (LANOMS)

[23] Qian, Ai-Zeng.*The Automatic Prevention and Control Research of ARP Deception and Implementation"*. : WRI World Congress on Computer Science and Information Engineering, April 2009

[24] Boughrara, A. and Mammar, S."*Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack"*. : 6th International Conference on Sciences of Electronics Technologies of Information and Telecommunications, March 2012. (SETIT)

[25] Pandey A., Saini J. R. *"Centralised Web based allocation and management approach towards IP addressing for providing Mobility and Security"*International Journal Of Emerging Trends & Technology in Computer Science, Vol-3, Issue-3, 2278-6856

[26] Sanguankotchakorn, Teerapat, and ThanatornDechasawatwong. "*Automatic attack detection and correction system development"*, 2011 13th Asia-Pacific Network Operations and Management Symposium, 2011

[27] Pandey A., Saini J. R. *"A Simplified Defense Mechanism Against Man in the Middle Attack"* IJEIR ,Jan 2014 Vol 1, Issue 5, 2277-5668

[28] Pandey A., Saini J. R.*"Attacks Defense Mechanisms for TCP/IP based Protocols"* IJEIR ,Jan 2014 Vol3, Issue 1, 2277-5668

[29] JUNIPER. 2006. *DDoS Secure* [Online]. Available: http://www.juniper.net/techpubs/software/management/ddos/ddos5.13.1/ ddos-secure-1200-quick-start-guide.pdf

[30] http://www.symantec.com/security_response/definitions.jsp

[31] Sharma N., Singh M. &Misra A. – *"Prevention against DDOS Attack on Cloud Systems using Triple Filter: An Algorithmic Approach"* INDIACom-2016; IEEE Conference BVICAM, New Delhi