THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Prevention of MITM Attack By Monitoring and Stopping Internet Browsing Service

Ravishanker[1], Dr. Sahil Verma[2], Dr. Kavita[3]

School of Computer Science & Engineering

Lovely Professional University, Phagwara, Punjab, India

[1]ravishanker@lpu.co.in, [2]sahil.21915@lpu.co.in, [3]kavita.21914@lpu.co.in

Abstract:

A MITM attack generally occurs when a third party intrudes in between the communication of multiple persons or an organization and making or showing himself as he/she was the true person whom you need to send any data or information and silently steals your all information and use it to harm the organization. This mainly happens over internet through any communication medium, such as email, social network sites, web browsing, transactions etc. An attacker can intercept not only victim's data but also they try to target all the information present in victim's devices. In the early approach the user has to manually check the ARP spoofing and based on the wrong ARP entries user have to decide that whether it was an attack or it was a false alarm. In the proposed approach a python script is created which monitor the web browser. If attacked happened it automatically filters the MAC address and check spoofed MAC request. Based on this, decision is made whether the attack is happened or not. In case attack happened, the browser automatically stops working denying any request and an alert is generated.

Keywords: MITM, ARP spoofing, attack, MAC, networks

1. INTRODUCTION

Besides all the technicalities, in simple terms the main concept of MITM can be described as, Imagine being in old days when there were no communication devices people use to communicate through mails as in letter so if there are three people jack, john and bob. Jack sends letter to John giving him greetings for his success but Bob the mailman opens up the letter and rewrite the letter and gives to John and make john hate Jack through his curse words. Due to vast growth of technology and speedy hardware the hacker silently monitors all data when user visits a website and uses their credential to

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

login. This is mostly due to ignorance of the user in context of using weak security, old operating system or using hackers created networks.

Mostly attack takes place during the time of login process or when an authentication process is going on. Connections meant to be secured by symmetric or asymmetric keys, which gives access to open the file with a unique key which will be having with each client with different combination keys and the file is encrypted so can't be opened. There are many other sites which requires login and where people keep their personal information and daily routine posted which helps the attackers to harm them either virtually or physically. If someone received an email that looks like it came from the bank in which the user is holding their current account and there's a link to login their account and if it ask for confirming user's contact information and the user believed on that fake mail clicked on the link which may ask user to enter their details. Here the user on just clicking that fake link may grab all the credentials by the attacker. This is the same as phishing but in this you attacker can grab the data and alter at a same time.

2. LITERATURE REVIEW AND RELATED STUDIES

[1] Carnut et al. suggested a technique which is based on switched networks, and this it need to be installed on the network hosts. His work has proved that it can detect ARP attacks accurately. His method shows no false alarm which means that there is no ARP attack, but the detector shows the alarm. On the other hand, their method shows that an attacker has the method to stay hidden behind during large volume of data transmission and stays unidentified for the longer time. Further, the author doesn't make their techniques to be available publicly so more information couldn't be drawn of. [2] ARP-Guard [3] ARP Defender system [4] Arpwatch are commercial products, which author has used on a sensor-based design model.. [5] Hou et al. also suggested the similar approach, they slightly improvised it by adding a detect module with Snort. [6] Belenguer et al. suggested an embedded or fixed ID which has the capability to identify and simultaneously defend against the ARP spoofing based intrusion automatically and accurately, but it needs to be connected to switch or a hub. Besides, IDSs' intelligence or capability to identify ARP spoofing is finite [7]. [8] Trabelsi et al. improvised the

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

previous method as both of their methods contains the identification or detection part runs in two phases IP routing and ARP cache poisoning.

[9] Barbhuiya et al. used combination of digital signatures and OTP and [10] Song et al. proposed a detection method for ARP spoofing using DS-ARP that stores the ARP cache table under the inspection and verifies the changed address in the table. [11], [12] Ramachandran et al. suggested a method to identify the ARP spoofing attacks over the mismatching of ARP Request or the Response packets. [13] Carnut et al. has implemented another technique, in which he assigns the disclosure of ARP spoofing to a specially designed detection station. [14] Kalajdzic and Patel suggested a method where rather depending totally to the test host, every single host execute the detection of attack by themselves. [15] Ortega et al. proposed a server-based technique which can be used to prevent ARP spoof attacks in small companies or office's LANs. His method contains a server and a switch. Their method was based on an OpenWrt firmware which need to be installed on the host. After this the server listens to requests which are in the form of ARP in the network and replies back with an (IP, MAC) mapping from the ARP cache, and the installed firmware continuously monitor and prevents the all ARP messages.

3. PROPOSED SYSTEM

Two methods can be implemented for prevention of MITM attack - Manual monitoring and Auto-Browser stop. In the GUI we have implemented a button with the name ARP table. It will open the ARP table and shows the IP and Mac addresses and you can compare the Mac address changes before and after the attack. But, in this method you have to open the ARP table every time or periodically in order to check if there is any kind of attack.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

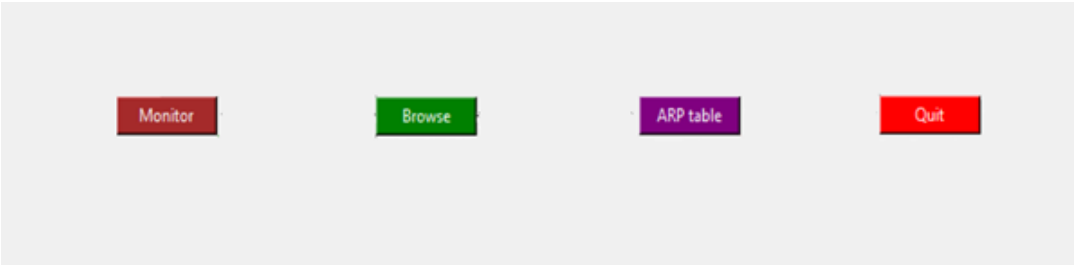
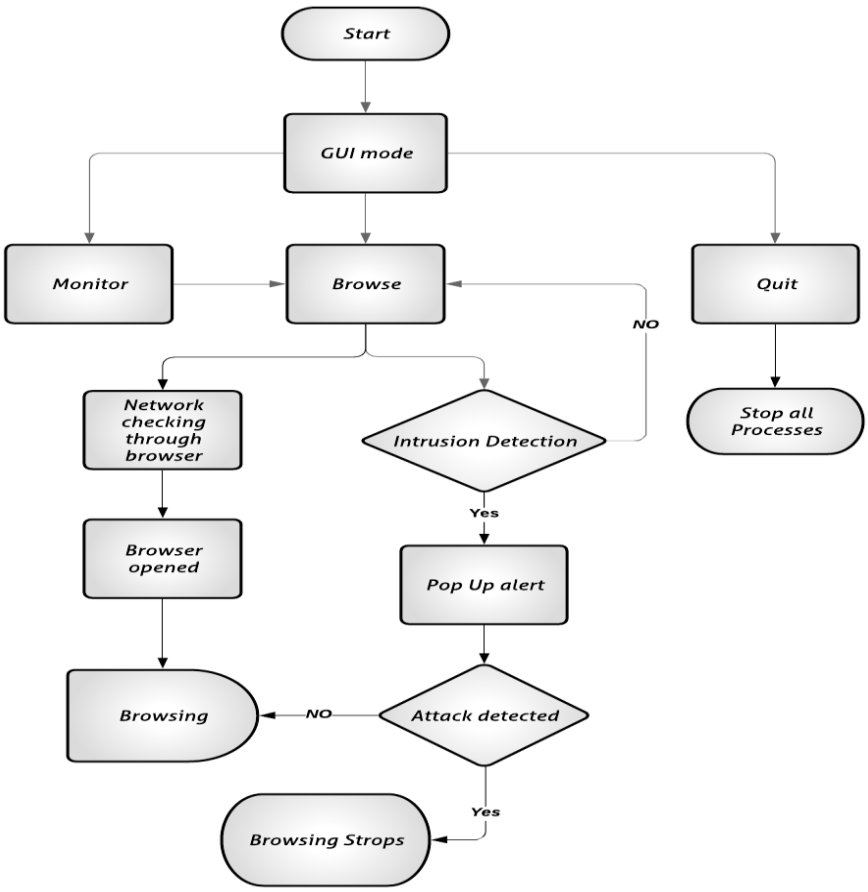


Fig. 3.1 GUI interface for attack detection

In auto-prevention mode user does not require observing the ARP table all the time as it detects automatically whenever there is an attack. A simulation tool is designed in Python having a button with the name Browse and when user click, it opens an interface or separate browser to browse a web page. Whenever there is any kind of attack possibility the browser will automatically disconnect.



ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Figure 3.2 Working procedure of the proposed work

In proposed method there is a button with name Monitor in which detection and pop-up code has been applied so, whenever there is any kind of attack these codes will be called. First step is to open the browser for the browsing and data transmission purpose and later steps is to perform a ARP spoofing attack and when the attack has done on the victims machine, the detection code which were running in the background and monitors for the intrusions if finds any intrusion then it will alert the users with a pop-up on the screen and the browser will be disconnected from the internet and in the security tab it will show the connection is not secure. Finally the data cannot be theft because the transmission will be stopped after the detection. Step by step procedure is as followed:

Terminal 1: **root@kali#** ifconfig

This command in the Linux terminal helps to know about the IP address and to which interface the machine is connected to, the ethernet or to wlan0 and gather the default gateway, broadcast address.

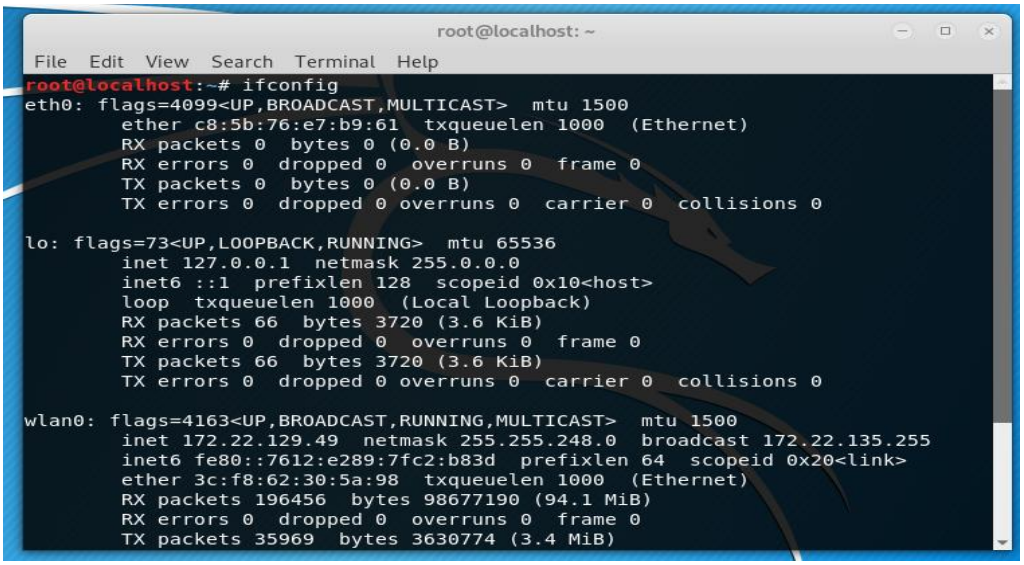


Figure 3.3 To know current IP address of the host

Terminal 2: **root@kali#** arpspoof -i wlan0 -t <IPaddress Victims> <default gateway>

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

This command helps the attacker to attack on the router and takes routers IP address and shows him as a router ip address to the user and then send request to the victim to tell him/her that he is the router and send the data to him/her (attacker).

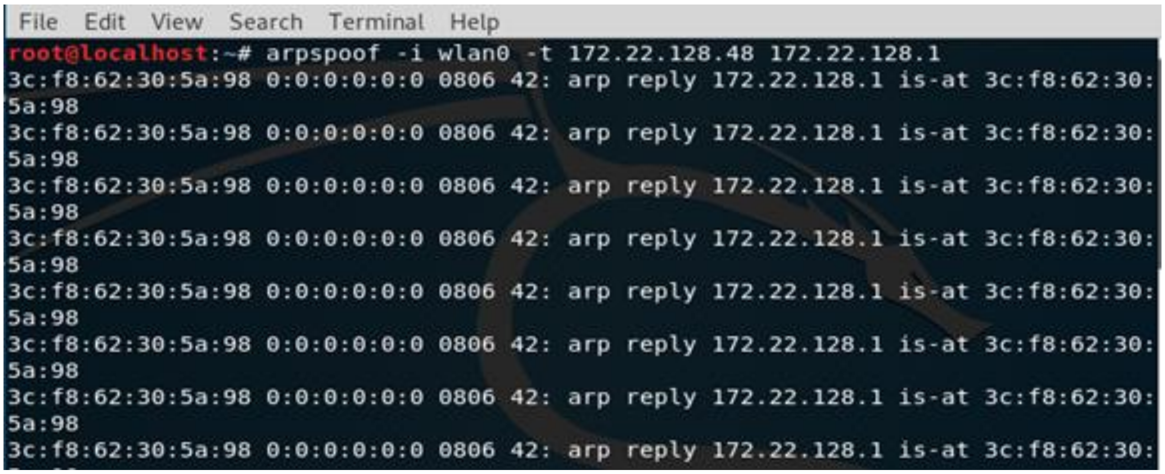


Figure 3.4 ARP Spoofing data visualization

Terminal 3: **root@kali#** arpspoof -i wlan0 -t <default gateway> <IP address Victim’s>

Reverse spoofing is done in order to not get suspicious by the host. So it is needed to send some data or reply to the victim so that attacker machine can act as genuine router. This command sends fake packets to the user from the router side and user can’t get suspicious of it and the targeted host can send the data freely thinking it as a router, but the data goes to the attacker. After this step the spoofing attack has been successfully done.

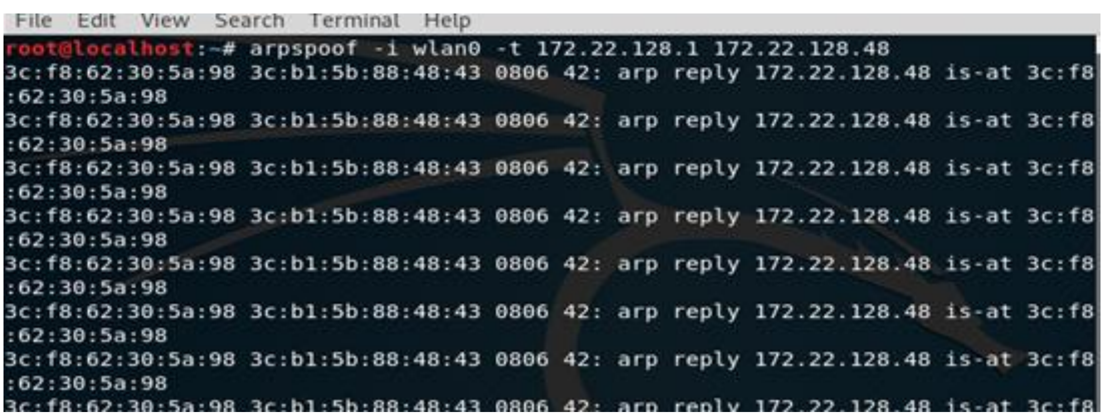


Figure 3.5 Reverse ARP Spoofing

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

The below steps are additional if attacker wants the data in a real-time. For example if the user or victim is accessing or sending some data, at the same time the information is received on the attacker machine also. It helps attackers to fetch data from the victim's activity on a particular website on which an attacker had already made a fake URL link and sent to him. For example cloning a website and make a fake URL which redirects the user to the cloned website and when user enters their login details then the details are received on the attacker machine.

Terminal 4: (1) **root@kali#** service apache2 start

Apache is one of the popular open-source which means it is free for all and it is a cross-platform web server. The Apache web server has modules which add more functions to its software and helps us to gather information in further process. Start the apache server in order to provide permission to host any website.

Terminal 5: (2) **root@kali#** setoolkit

The following step helps attacker to create a fake PHP page. The Social-Engineer Toolkit (SET) is made to do the high end attacks to the users data and their accounts credentials. These steps help attacker to create a clone website and generate a PHP link and if an attacker has send that link to anyone and the victim opened it and enter his personal details then on your terminal the details are displayed simultaneously. SET contains following types of attacks: 1. Social Engineering, 2. Website attack Vectors, 3. Credentials harvesting, 4. Site cloning,-> provide our ip address-> url to clone the site.

Terminal 5: The below command helps to create a text file with attackers IP address and the cloned PHP link in order to use it directly for DNS spoofing.

i. **root@kali#** Pico attack.txt
ii. <Attackers IP address> <URL>

Terminal 6: In the below command executes the DNS spoof using the text file which was created in the above step and used as listener on the particular ports.

root@kali# dnsspoof -i wlan0 -f test.txt

4. RESULTS AND CONCLUSION

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

In the browse mode the victim is simply accessing any URL. This is the situation where an attacker has not performed any MITM attack.

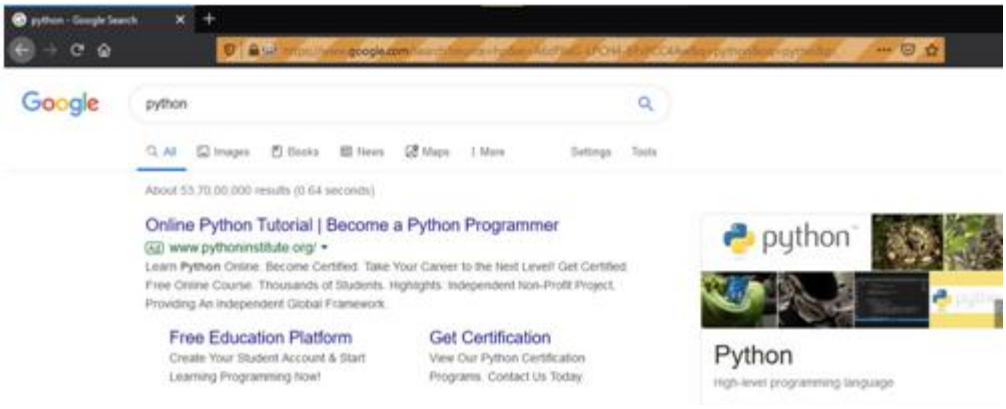


Figure 4.1 Browse mode where no attack is done and browser working as normal

In Figure 4.2 the attacker has already performed ARP Spoofing and performed MITM attack. The browser stopped working and site become unsecure.

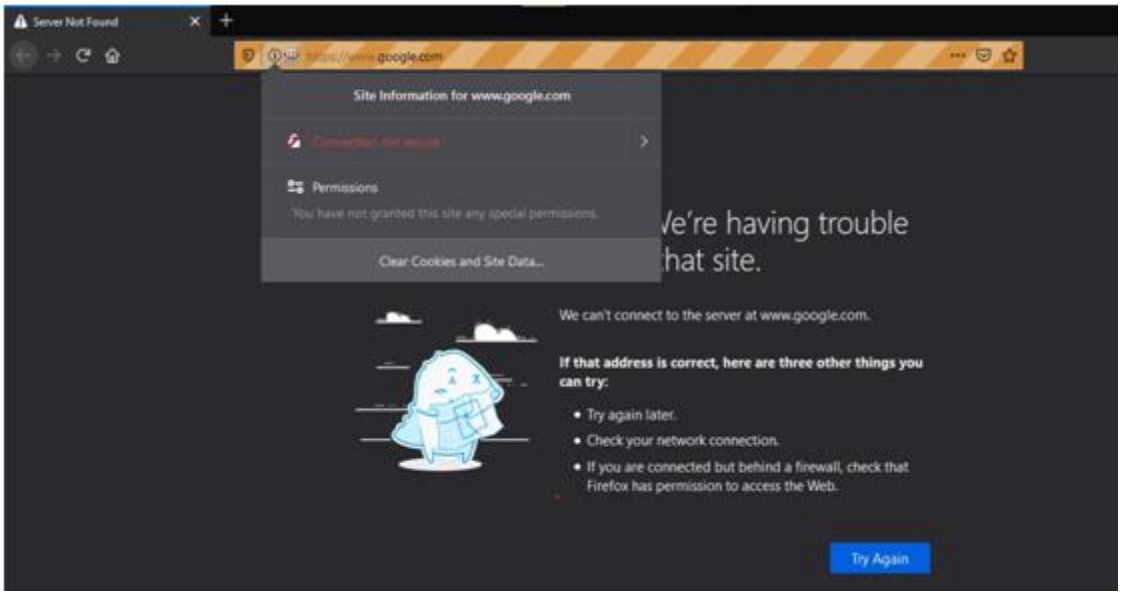


Figure 4.2 Browse mode where attack is executed and browser stopped working

From this point of time if the victim use the proposed Python script running in the background monitoring the network and browser, it automatically generates a popup alert showing spoofed MAC address using MITM attack by the attacker.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

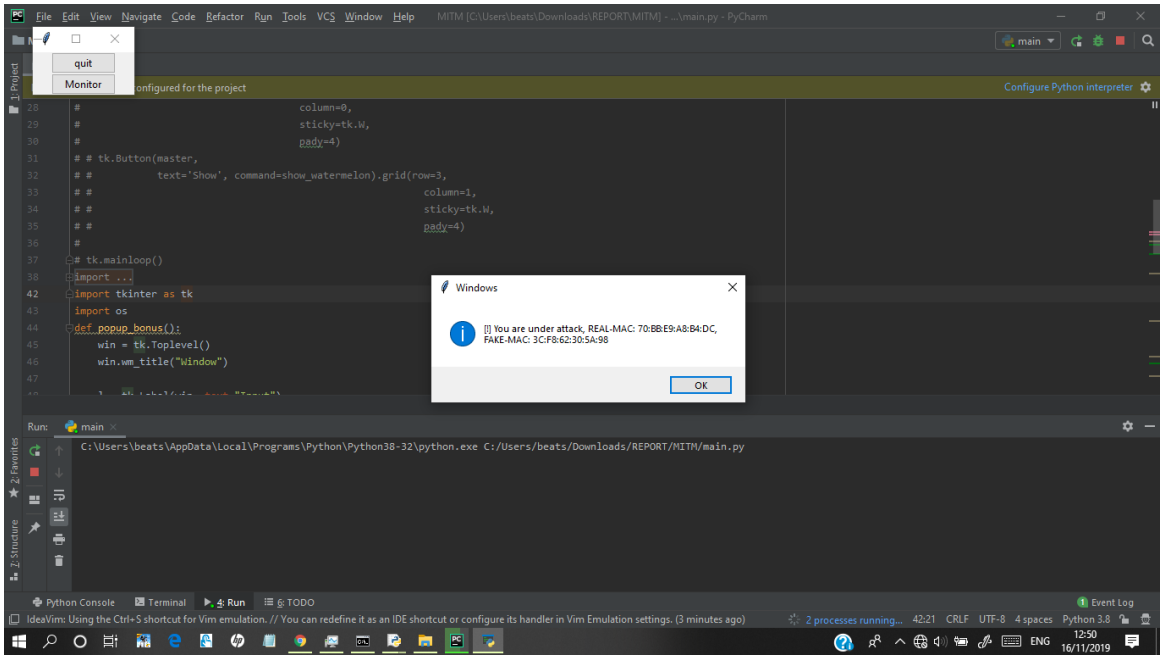


Figure 4.3 Browse mode where attack is executed and Pop-up Alert displayed

Figure 4.4 Pop-up Alert displayed

Proposed techniques alerts the victim with the following output if executed on the terminal. It's the output of the detection running in the background.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Figure 4.4 Alert generated with original MAC address and Spoofed MAC address

Finally the proposed approach will monitor the web browser service. If any attack is done then it automatically filters the MAC address and check spoofed MAC request. The script continuously monitors the current IP mapped with its MAC address and if any deviation of mapped address is done then decision is made whether the attack is happened or not. In case attack happened, the browser automatically stops working denying any request and an alert is generated. There are so many techniques already available but this method specially helps used to prevent him from MITM attack as well as phishing. Future work includes controlling of tunneled application and system using network address translation.

5. REFERENCES

[1] Carnut, M., and J. Gondim. "ARP spoofing detection on switched Ethernet networks: A feasibility study." *Proceedings of the 5th Simposio Seguranca em Informatica*. 2003.

[2] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, *18*(3), 2027-2051.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[3] Bhushan, Bharat, G. Sahoo, and Amit Kumar Rai. "Man-in-the-middle attack in wireless and computer networking—A review." *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017.

[4] LNR Group. "arpwatch, the Ethernet monitor program; for keeping track of ethernet/ip address pairings." *Last accessed September* 17 (2016).

[5] Hou, Xiangning, Zhiping Jiang, and Xinli Tian. "The detection and prevention for ARP Spoofing based on Snort." *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*. Vol. 5. IEEE, 2010.

[6] Belenguer, Jorge, and Carlos T. Calafate. "A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments." *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*. IEEE, 2007.

[7] Sato, Tomoaki, and Masa-aki Fukase. "Reconfigurable hardware implementation of host-based IDS." *9th Asia-Pacific Conference on Communications (IEEE Cat. No. 03EX732)*. Vol. 2. IEEE, 2003.

[8] Trabelsi, Zouheir, and Khaled Shuaib. "NIS04-4: Man in the middle intrusion detection." *IEEE Globecom 2006*. IEEE, 2006.

[9] Barbhuiya, Ferdous A., et al. "An active host-based detection mechanism for ARP-related attacks." *International Conference on Computer Science and Information Technology*. Springer, Berlin, Heidelberg, 2011.

[10] Song, M. S., Lee, J. D., Jeong, Y. S., Jeong, H. Y., & Park, J. H. (2014). DS-ARP: a new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments. *The Scientific World Journal*, *2014*.

[11] V. Ramachandran, S. Nandi, "Detecting ARP spoofing: An active technique" in Information Systems Security, New York, NY, USA: Springer, pp. 239-250, 2005.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[12] Hubballi, Neminath, et al. "An active intrusion detection system for LAN specific attacks." *Advances in Computer Science and Information Technology*. Springer, Berlin, Heidelberg, 2010. 129-142.

[13] Carnut, M., and J. Gondim. "ARP spoofing detection on switched Ethernet networks: A feasibility study." *Proceedings of the 5th Simposio Seguranca em Informatica*. 2003.

[14] Kalajdzic, K., and A. Patel. "Active detection and prevention of sophisticated ARP-poisoning man-in-the-middle attacks on switched Ethernet LANs." *Proc. of 6th International Workshop on Digital Forensics & Incident Analysis*. 2011.

[15] Ortega, Andre P., et al. "Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt." *2009 Latin American Network Operations and Management Symposium*. IEEE, 2009.