iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI: http://doi.org/10.22214/ijraset.2018.2118

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Development of IDS for Detecting ARP Attack using DES Model

Shraddha Tiwari[1], Dr.Rajesh Bansode[2]
[1]*PG Student, Information Technology, Thakur College of Engineering and Technology, Mumbai, India*
[2]*Professor, Information Technology, Thakur College of Engineering and Technology, Mumbai, India*

Abstract: ***Address Resolution Protocol (ARP) is one of the important protocol in the TCP/IP suit. Address Resolution Protocol (ARP) resolves an IP address (32 bit Logical Address) to the physical address (48 bit MAC Address). Arp poisoning puts the attacker in position to intercept communications between the two computers. In ARP Spoofing, the attacker will gain all the data transferring on network. In the shared network the attacker will be able to reply to all the ARP requests which are transmitted in the network with its own MAC address and the attacker can maintain ARP table with actual addresses. Now each and every data from the host will be forwarded to the attacker. A two way communication will be maintained by the attacker by forwarding and replying to all data through itself between devices. In this paper, ARP poisoning and detection is shown. Attack is done by manipulating the IP address and MAC address. If there is any duplicate MAC address entry present in the ARP table a predefined script is launched with parameters as MAC address and IP address. And the duplicate IP address is removed from the table. In case of an attack it can also detect the real mapping of MAC to IP addresses. In ARP spoofing attacks, an attacker can pretend to be another host and gain access to sensitive information. The paper also focuses on designing a Discrete Event System (DES) based approach to detect ARP spoofed IP.***

Keywords: Address Resolution Protocol, Discrete Event System, Internet Protocol, Local Area Network, Media Access Control, Transmission Control Protocol.

I. INTRODUCTION

Networks have become an integral part of today's world. The ease of deployment, low-cost and high data rates have contributed significantly to their popularity. There are many protocols that are tailored to ease the process of establishing these networks. Nevertheless, security-wise precautions were not taken in some of them. Computer networks play a major part in this process. In recent days, it is hard to find a computer or a smart phone that is not connected to a network in some sort, whether it is directly connected to the Internet service provider (ISP) or through a local area network (LAN) alongside other devices. To facilitate this process, network engineers came up with a set of rules called protocols for message exchange between computers. These protocols maintain the connection between the connected devices within a network and allow them to work efficiently and trouble free.

II. ADDRESS RESOLUTION PROTOCOL (ARP)

Address Resolution Protocol (ARP) is one of the important protocol in the TCP/IP suit. Address Resolution Protocol (ARP) resolves an IP address (32 bit Logical Address) to the physical address (48 bit MAC Address). Arp poisoning puts the attacker in position to intercept communications between the two computers. Address Resolution Protocol (ARP) has no mechanism to authenticate ARP packets, which makes ARP Spoofing attacks a serious security threat. The host with the given IP answers back in a unicast ARP reply indicating its MAC address. The host that issued the request caches the IP, MAC pairing in a local ARP cache so that it does not have to issue the same request in the near future[1]. The information received by the destination node in ARP packet consist of its MAC address and IP address. Additionally, there is a request or reply for a MAC address to an IP address in ARP Request and ARP Reply packets. Fig 1 shows the ARP message format.

16 bits data		16 bits data
MAC Address Length	Protocol Address Length	OP Code Number
Sender MAC Address		
Sender IP Address		
Receiver MAC Address		
Receiver IP Address		

Fig 1. ARP Message Format

The remainder of the paper is organized as follows: Section II provides the Background of ARP Protocol. This section describes ARP protocol, working of ARP and short description on ARP poisoning. In section III, We discuss related works in this area, which have been proposed to manipulate the ARP spoofing attacks. Section IV illustrates Experiment results and setup required to perform the experiments. Finally, Section VI concludes the paper.

III. RELATED WORK

A centralized detection and prevention technique against ARP poisoning published in the year 2012 by the author S. Kumar and S. apaswi. This paper presents a feasible solution to the ARP cache poisoning, removing inconsistencies from all ARP tables of all hosts in the network. An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks published in the year 2007 by the author C. L. Abad and R. I. Bonilla. This paper describes the problem of ARP poisoning and ARP spoofing attacks, and have analyzed several currently available solutions, and summarized the results of the analysis.

An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries published in the year 2014 by the author A.M. AbdelS alam, W.S. Elkilani, K.M. Amin. In this paper, a solution to the problem of ARP spoofing has been proposed, the solution is an automatic and scalable method of configuring static ARP entries instead of manually configuring. Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting published in the year 2005 by the author P. Arote and K. V. Arya. In this paper, a new approach for detection and prevention against ARP poisoning attack is proposed. A solution is fully based on the ICMP and Voting over centralized system.

Detection and Prevention of ARP Poisoning in Dynamic IP configuration published in the year 2016 by the author D. R. Rupal, D. Satasiya, H. Kumar and A. Agrawal. This paper demonstrates a utility which gives users the authentication as well as detection and prevention of ARP poisoning in dynamic IP configuration.

Detection of ARP Spoofing: A Command Line Execution Method published in the year 2014 by the author D. Sharma, O. Khan and N. Manchanda. This paper has a mechanism to detect IP-ARP Spoofing. The technique discussed in this paper includes a network administrator, who can monitor and easily detect the ARPSpoofing occurring in his local subnet

Preventing ARP Spoofing Attacks through Gratuitous Decision Packet published in the year 2012 by the author Haider Salim, Zhitang Li, Hao Tu, and Zhengbiao Guo. The proposed method named a Gratuitous Decision Packet System GDPS achieves a detection of suspicious ARP packets, by implementing a real-time analyzing for received ARP packets.

IV. WORKING OF ARP

ARP cache is a table of recently resolved IP addresses and their corresponding MAC addresses. The ARP cache is checked first before sending an ARP Request frame. ARP cache entries can be dynamic or static [2] .Let consider an example to have a detailed look at ARP and how it functions:

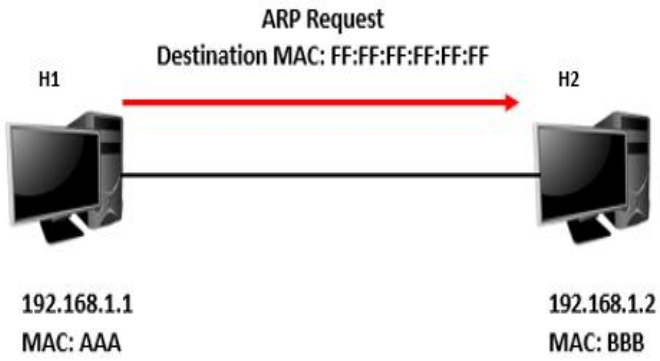


Fig 2.ARP Request (Broadcast Request)

In above fig.2, there are two computers with their respective IP address and MAC address. Computer1 i.e H1 wants to communicate with H2. It will send ping request to H2. The ARP table is empty so H1 have no clue what the MAC address of H2 is. So, H1 will send an ARP Request. This message means “Who has IP address 192.168.1.2 and what is your MAC address?” Since the system’s MAC address is not known the broadcast MAC address for the destination (FF:FF:FF:FF:FF:FF) will be used. The broadcast MAC address message will reach to all computers in the network.

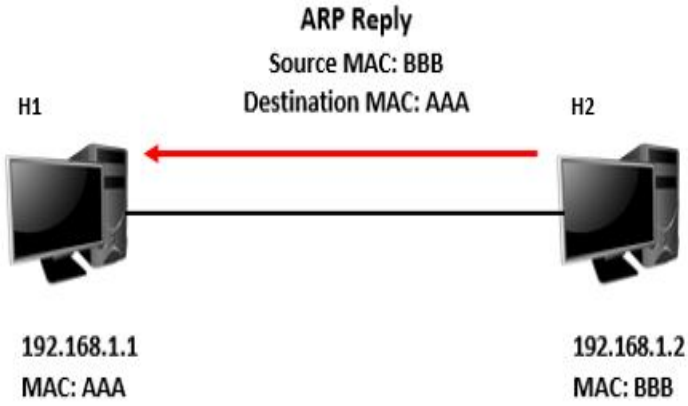


Fig 3.ARP Reply

Fig 3 describes after the broadcast message is received, the system with IP address 192.168.1.2(i.e. H2) will reply with a message ARP Reply and it basically means "that's me! "And Reply with its MAC address. After receiving H2 MAC address, H1 can now add the MAC address to its ARP table and start forwarding data to H2.

A. Arp Poisoining

ARP spoofing attack is a kind of attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages over a LAN. As a result the attacker links his MAC address with the IP address of a legitimate computer (or server) on the network. If the attacker managed to link his MAC address to an authentic IP address, he will begin receiving any data that can be accessed by that IP address. ARP spoofing allows malicious attackers to intercept, modify or even stop data which is in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

V. EXPERIMENTS AND EVALUATION

In this proposed work, ARP Spoofing attack is performed and also mechanism to detect ARP poisoning attack is shown. Attack generation tools jpcap, pcap were deployed in attacker machine and several scenarios of spoofing MAC addresses were attempted. Different amounts of attack packets (up to 200) per second were injected in the LAN.

A. Experimental Setup

To implement the attack, we have taken a real network environment consisting of 2 systems. Both systems have windows operating system installed. Each system is having 2GB RAM, Intel Core i3 processor. All are connected over wired network. Port forwarding is enabled. Following IP addresses and MAC addresses of the machines are present in the network.

Table 1. Attacker and Victim machine detail

System	IP Address	MAC Address
Attacker Machine	175.175.1.153	989096d4807d
Victim Machine	175.175.3.241	74D435CBFF44

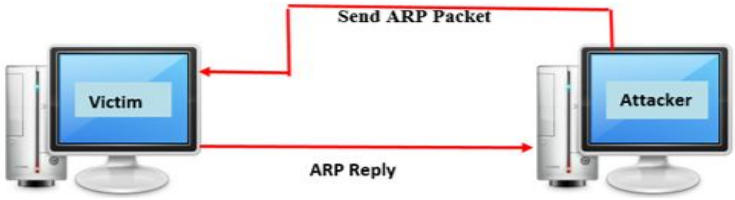


Fig.4. ARP poisoning

Fig. 4. shows detection of ARP poisoning which illustrates, first Attacker sending ARP packet to Victim, Attacker with IP address 10.0.0.3 are poisoned with same MAC address 08:00:27:26:3b:f8. Thus, ARP poisoning is detected.

A. Results

In this section, results are shown that are being developed. Jpcap is used to capture packets on the network. ARP attack and defence are performed.

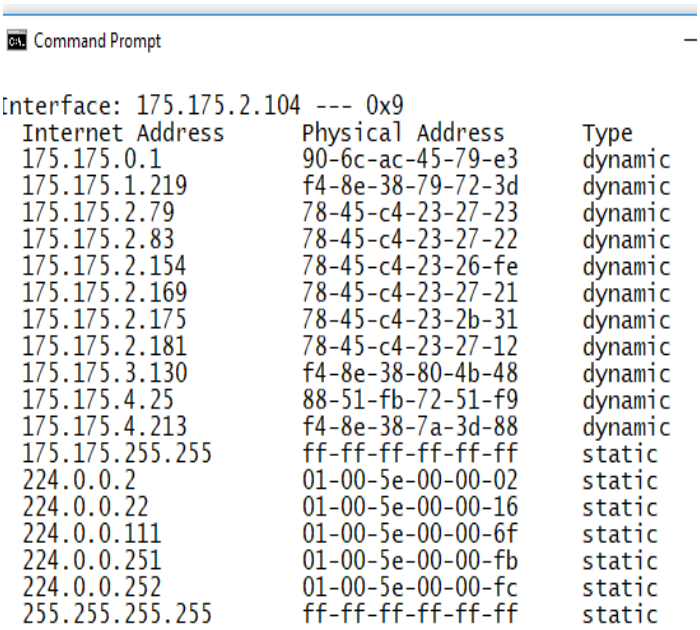


Fig 5. ARP Table

Fig .5 shows the ARP table. ARP provides a mechanism to lookup on the network. ARP table is the place used to store this lookup. This table will display all the connected host to a particular machine on the network.

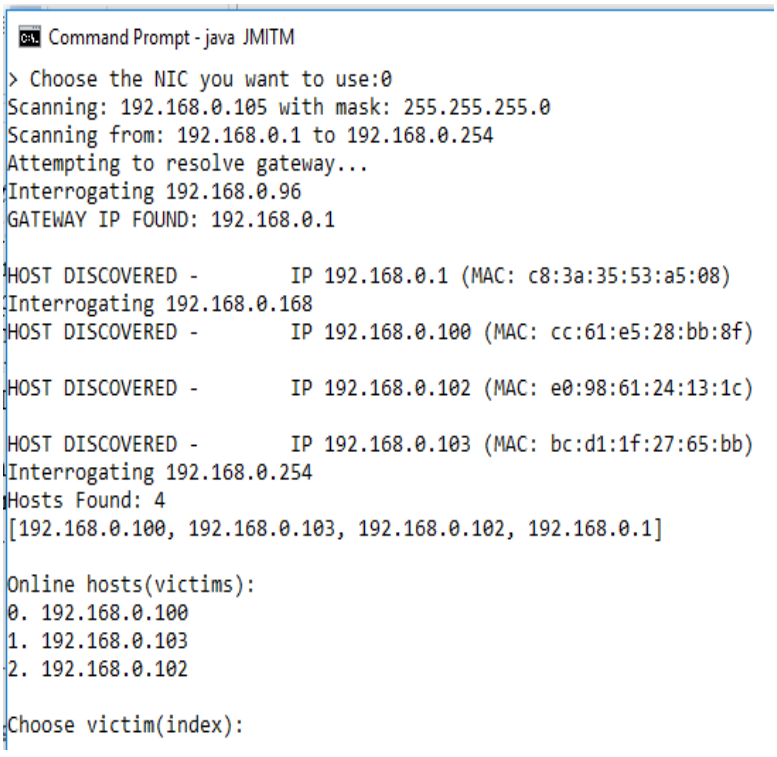


Fig. 6 Analyzing ARP packets

Fig 6 shows the number of online host that are connected to the victim and attacker machine on the same network. The attacker scans the entire network and discovers the host on which attack is to be performed. The IP range is scanned and only those host IP are displayed that are online. Gateway IP of particular interface is fetched and entire network is searched for attacking purpose. IP and MAC address of the host are displayed. The attacker can select any victim of which he needs to sniff the network. Jpcap sets a filter and displays only online host which can send and receive packets. For performing attack, jpcap asks to choose a victim from the filtered host IP address. It is shown that the attacker selects any one victim among the listed host on which sniffing is to be done.

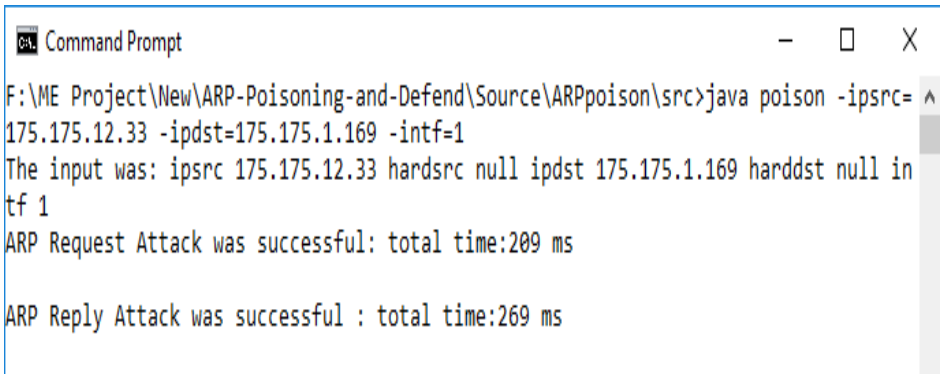


Fig. 7 ARP Attack Performed

Fig.7 shows the DES model used for ARP Poison. DES model shows the time taken by attacker to perform attack and sniff victim's machine. It provides better mechanism to detect the attack performed by the attacker.

```
C:\WINDOWS\system32>F:

F:\ME Project\New\ARP-Poisoning-and-Defend\Source\ARPDefend\src>java de
fend -intf=0 -timeout=120
Defending started
ARP REQUEST 00:50:56:c0:00:08(/192.168.239.1) -> 00:00:00:00:00:00(/192
.168.239.2)
        Entry was added to the list 192.168.239.1
        ARP Request is sent to: 192.168.239.1
ARP REQUEST 00:50:56:c0:00:08(/254.128.0.0) -> 00:00:00:00:00:00(/192.1
68.239.1)
        Entry was added to the list 254.128.0.0
        ARP Request is sent to: 254.128.0.0
ARP REQUEST 00:50:56:c0:00:08(/192.168.239.1) -> 00:00:00:00:00:00(/192
.168.239.2)
        192.168.239.1 already exists in database
```

Fig 8. Defending Window

Fig.8 shows defending window. The detection is done on victim's machine. It shows that defending of attack is being started. It captures all the IP address from the ARP table of the system and determines which IP address is newly added. Any new added IP address is stored in ARP table of system. The figure shows two new IP address that are added to the ARP table.
It also shows detection of spoofed IP. The fig describes that an ARP request is sent to the specified IP address from the ARP table with IP address and MAC address. If the systems IP address is already stored in the system's ARP table a message as particular IP address already exist. The defending system searches for MAC address. If ARP table has two same MAC address entry then the encountered IP address is spoofed IP address and thus ARP spoofing is detected as shown in figure. Thus the defending system will remove the IP address which has same MAC address as of other.

VI. CONCLUSION

ARP protocol is a stateless protocol has very dangerous consequences. An attacker could manipulate the connection of the users, steal their data, and even redirect their traffic to different websites than the ones they requested. Network administrators should become more aware of these attacks and take countermeasures against them. Users should also become more aware of them and use security solutions to prevent getting their data stolen.

Packet sniffer is a program which monitors network traffic which passes through victim's machine. A packet sniffer which runs on your PC connected to the internet using a modem, can tell you your current IP address as well as the IP addresses of the web servers whose sites you are visiting. Most networks use what is known as broadcast technology, meaning that every message transmitted by one computer on a network can be read by any other computer on that network.

The proposed scheme for ARP-Spoofing detection has following points:

1. Network security enhancement
2. Works with dynamic IP Addresses
3. No network congestion

REFERENCES

[1] C. L. Abad and R. I. Bonilla "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks,"2007 Distributed Computing Systems Workshops,. ICDCSW '07. 27th International Conference, Toronto, pp. 60-60.doi: 10.1109/ICDCSW.2007.19

[2] M.Al-Hemairy, S. Amin, and Z. Trabelsi, "Towards More Sophisticated ARP Spoofing Detection/ Prevention Systems in LAN Networks," 2009 International Conference on the Current Trends in Information Technology (CTIT), pp.1-6, Dec-2009.

[3] S. Kumar and S. Tapaswi, "A centralized detection and prevention technique against ARP poisoning," 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpu, pp. 259-264.doi: 10.1109/CyberSec.2012.6246087

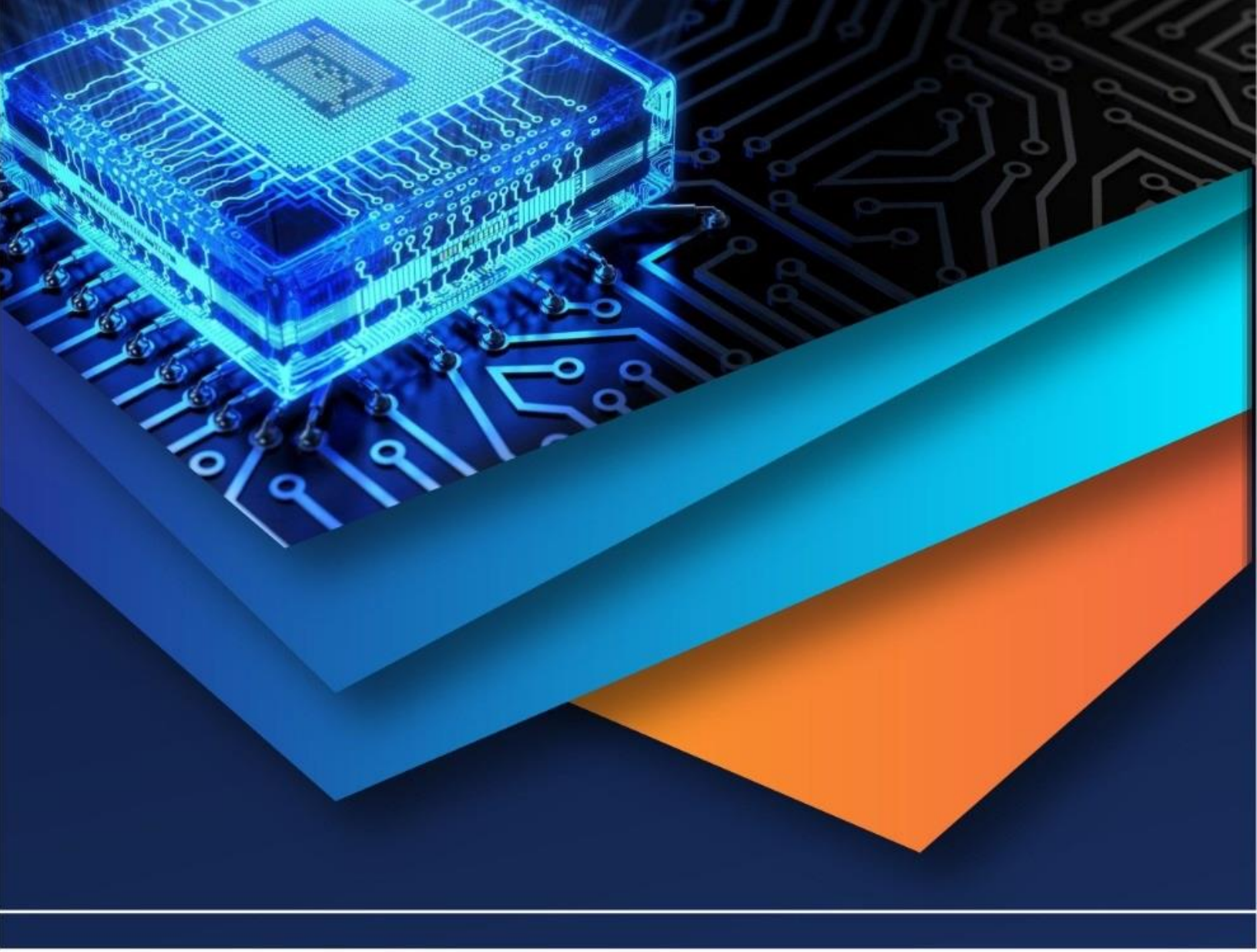
[4] A.M.AbdelSalam, W.S.Elkilani, K.M.Amin "An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries" (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 5, pp. 105-112, 2014

[5] P. Arote and K. V. Arya, "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting," 2015 International Conference on Computational Intelligence and Networks, Bhubaneshwar,pp. 136-141.doi: 10.1109/CINE.2015.34

[6] D. R. Rupal, D. Satasiya, H. Kumar and A. Agrawal, "Detection and prevention of ARP poisoning in dynamic IP configuration," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, pp. 1240-1244.doi:10.1109/RTEICT.2016.7808030

[7] D. Sharma, O. Khan and N. Manchanda, "Detection of ARP Spoofing: A command line execution method," 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 861-864.doi: 10.1109/IndiaCom.2014.6828085

[8] H. Salim, Z. Li, H. Tu and Z. Guo, "Preventing ARP Spoofing Attacks through Gratuitous Decision Packet," 2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science, Guilin, pp. 295-300.doi: 10.1109/DCABES.2012.71



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY