iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.42176

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: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

A Secure Detection Framework for ARP, DHCP, and DoS Attacks on Kali Linux

Monika Dandotiya[1], Abhinandan Singh Dandotiya[2], Nidhi Dandotiya[3], Ankit Sahu[4]
[1, 2, 3, 4]*Department of Computer Science and Engineering, ITM University, M.P., India*

Abstract: ***Currently, the Internet is playing a vital role in educating students to boost industrial production. Various network components are employed to give a wide range of options and reliability for internet services. As the Internet continues to develop and expand, network security has become an issue. Many attempts to secure transmission at the application, transport, or network layers have failed because the data connection layer has not been appropriately managed. The DHCP and ARP protocols are critical to the network's ability to function correctly. They were not designed with security precautions in mind. So, they are susceptible to a variety of assaults, including the rogue DHCPS, DHCPS hunger, DHCP hijacking, host impersonation, man in the middle, and DDoS. Here, we are going to examine how Kali Linux handles the aforementioned threats. DHCP hunger and host impersonation attacks could not be prevented by the current ARP and DHCP security measures. LAN assaults may be prevented and mitigated by using a novel method to protect ARP and DHCP. ARP and DHCP communications are protected by the suggested approach, which ensures their integrity and validity. A comparison of the proposed plans' security and performance attributes is carried out and compared to those of similar schemes.***
Keywords: Cyber-attacks ARP, DHCP TCP DoS, UDP Dos, Kali Linux

I. INTRODUCTION

The rapid and ongoing evolution of security vulnerabilities is one of the most troublesome aspects of cybersecurity. Hackers are constantly improving the methods they use to infiltrate computer systems. They strike fast, necessitating the need for prompt security [1]. To begin a successful cybersecurity plan, one of the first steps is to learn about the danger. The meaning of phrases like "cyber-attack," "cyber-warfare," and "cyber-crime" is commonly misunderstood. As a result of this lack of clarity, it may be difficult to create a relevant legal remedy.

As a result, in Part I of this article, we begin by defining some basic concepts. Even though this may appear to be a simple activity, it is essential to any reform endeavour.

The term "cyberattack" is defined as "any activity designed to damage the functioning of a computer network for political or national security purposes." Aside from that, we clarify the differences between "cyber-attacks," "cyberwarfare," and "cybercrime," and outline the three most prevalent types of cyberattacks: distributed denial of service assaults, the dissemination of false information, and intrusions into a safe computer network [2].

Humans, processes, and technologies are all involved in cyber security to cover the full range of threats, vulnerabilities, deterrence, international engagements and operations, information assurance, and law enforcement in the event of a cyber-attack or other crisis. OR Network, computer, program, and data security encompasses a wide range of technologies, methods, and practices aimed at preventing intrusion, harm, or illegal access [3].

A. the Level of Cyber Risk

The threat is overestimated for several additional reasons. Cybersecurity has become a highly political topic, and official claims regarding the amount of threat must be evaluated in the context of competing bureaucratic groups for money and power. In general, this is accomplished by emphasizing the urgency of the situation and presenting the overall danger as large and escalating. There is also evidence that risk perception is heavily influenced by one's instincts and emotions, along with the judgments of experts. These "dread risks," which look uncontrolled, catastrophic, lethal, and unknowable, suit the characteristics of cyber-risks in their most severe version.

People are terrified of low probability dangers, which leads to a desire to serve an activity with all the readiness to suffer large expenses for an unknown reward. Only the most serious system attacks require the attention of the traditional national security agency [4]. Attacks that disrupt services or are only a minor inconvenience to the computer are considered attacks.

B. Attack In Cyber Security

Among the most prevalent sorts of attacks, researchers have found, are denial-of-service (DoS), destructive programming (virtually infectious agents like viruses and worms), malware (malicious insiders), stolen devices (phishing and social engineering), and web-based attacks. There are four possible classifications for the findings: cybercrime, cyber espionage, cyberwar, and hacktivism [5]. The following are the primary targets of our attention:

C. Arp Spoofing

Sophisticated attacks on the ARP (Address Resolution Protocol) protocol are known as ARP spoofing, and they are carried out by hostile actors. For example, this means that an attacker can be linked to an IP address on the network with the MAC address of a genuine device or server [6]. To begin receiving data, the attacker's MAC address must be associated with a known-good IP address. To modify or interrupt the flow of data in transit, a malicious actor can use ARP spoofing. ARP spoofing attacks are feasible on local area networks using the ARP. For enterprises, ARP spoofing attacks have the potential to cause serious problems. A simple ARP spoofing attack may be used to steal sensitive data. ARP spoofing attacks typically follow a similar progression [7-9].

D. DHCP Starvation Attack

It is possible to attack DHCP servers with a malign digital assault called a "DHCP starvation attack." By sending an endless stream of fake "DISCOVER" packets, an attacker may quickly deplete the IP address pool of an unsuspecting DHCP server. This allows the attacker to deny legitimate network users service or provide an alternate connection that leads to an attack known MITM [10]; and Acknowledgement. When it comes to DHCP, all four of these fundamental (DORA) packets are critical but DISCOVER packets will be our primary focus. An exploit known as DHCP Starvation occurs when a malicious actor floods a DHCP server with fake DISCOVER packets until the latter believes it has exhausted its available resources.

E. Denial of Service Attack (DoS)

If a system or network is targeted by a Denial-of-Service (DoS) assault, it will be rendered unreachable to its intended users. For example, a DoS attack might overwhelm a target with traffic or convey information that causes it to go down. At the same time, the DoS attack denies the expected service or resource to legitimate users (such as staff members, members, or account holders). In the majority of DoS assaults, high-profile businesses such as financial institutions, government agencies and media corporations are targeted. DoS assaults, despite the fact that they do not often result in the theft or loss of major information or other assets, are very time- and money-consuming for the victim. Flooding or crashing services are two of the most common techniques of DoS attacks. Whenever the server is overloaded with requests, a flood assault occurs. This slows down and finally stops the system from responding. The following are common flood attacks [11].

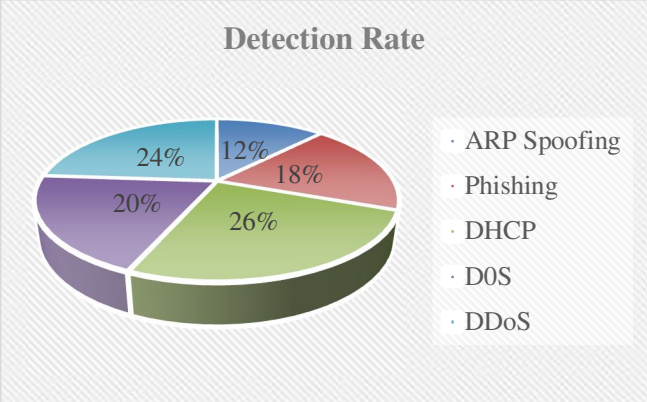


Figure. 1 Detection rate of different attacks

Sensitivity and detection rate (DR) are interchangeable terms (the proportion of affected individuals with a positive test result). In analytical biochemistry, the term "sensitivity" has a different connotation, therefore the term "DR" prevents any mistake. the detection of intruder assaults using a network security technique. There are a lot of low-level alerts generated, which makes it tough to analyze, especially when it comes to constructing attack scenarios. Construction of attack scenarios using Alert Correlation (AC) is critical for revealing the tactics of the attacker [12].

II. LITERATURE REVIEW

A survey study by [13] showed that social media, cloud computing, smartphones, and other auxiliary technologies were experiencing new trends and risks. There were vulnerabilities in hardware, software, and network architecture that were discovered throughout the research. Traditional ways to cyber security are effective against well-known dangers, and new hot research issues for the future include unique identity and trace-back techniques. The most recent approach to cyber threats may be summarized by looking at the following state-of-the-art metrics.

For ACPS detection and defence against sensor spoofing cyberattacks, [14] provides a new and robust security protocol. Using the SimEvents toolkit, the first step was to create a networked control system for an airplane. Another way to detect and remove suspect communication packets in airplane network traffic was based on. Last but not least, a real-world cyber-security assault scenario was used to combine the NCS and the detection system. Based on the True Positive and True Negative algorithm detection rates, the algorithm's accuracy was 0.96.

The defenders' perspective on ICPS security risk is taken into account in this strategy. There are mathematical replicas of the physical plant and feedback controller recognized for ICPS under assault as a dynamic closed-loop fusion model. Disruption resources are mathematically characterized using the fusion model [15]. The residual value of the system is used to assess effectiveness of the Kalman filter in perceiving assaults. Further, a broad security risk level model is built based on the system's disruption resources and detection capabilities. According to the findings of MATLAB simulations, a qualitative analysis approach provided by the authors is capable of accurately describing the security risk caused by cyberattacks [16-18]. It is created for CPSs subjected to fake data injection attacks Nonlinear systems are used to simulate the physical system of CPSs.

FDIA [19][20] is injected by an attacker into the control channel through a wireless network. The abnormal dynamics created by FDIA are simulated using a time-derivative constrained abnormal effect to get quicker to the actual cyber-attack consequence. Attack effect spectators are tasked with gauging the impact of unusual attacks. An attack effect observer-based security control architecture is built on the estimation signal and rejects unusual assaults to guarantee consistently limited performance. Finally, the A-4D aircraft simulation experiment is created to verify efficacy of suggested security control manner.

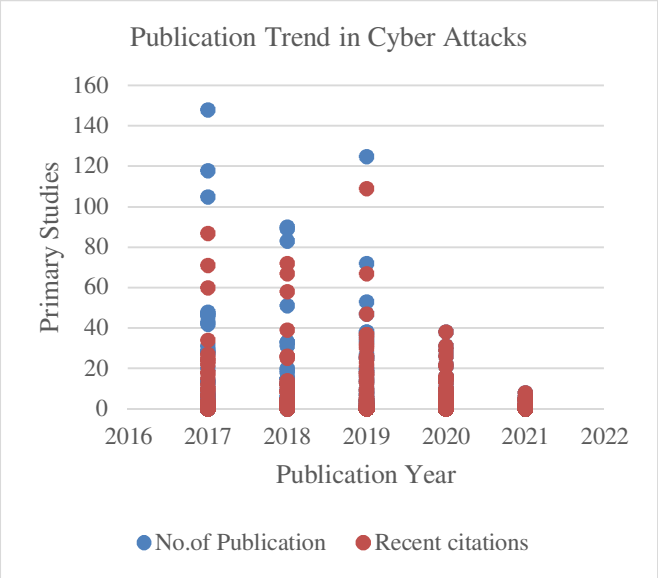


Figure. 2 The publication trend in the area of cyber attack

Publication-related cyber-attack statistics are depicted in the graph above. The rise in the number of articles published demonstrates the scientific community's interest in this topic. We utilize a low-interaction honeypot dataset to showcase the framework's application, but we note that the system may also be used to analyses high-interaction honeypot data, which provides more information about the assaults. Honeypot-captured cyber assaults display long-range dependency (LRD) for the first time, according to a case study. According to the results of this case study, it is possible to accurately anticipate cyber assaults by using statistical features (LRD in this example). Defendants would have enough time to change their defenses or resources if they had this type of early warning capacity.

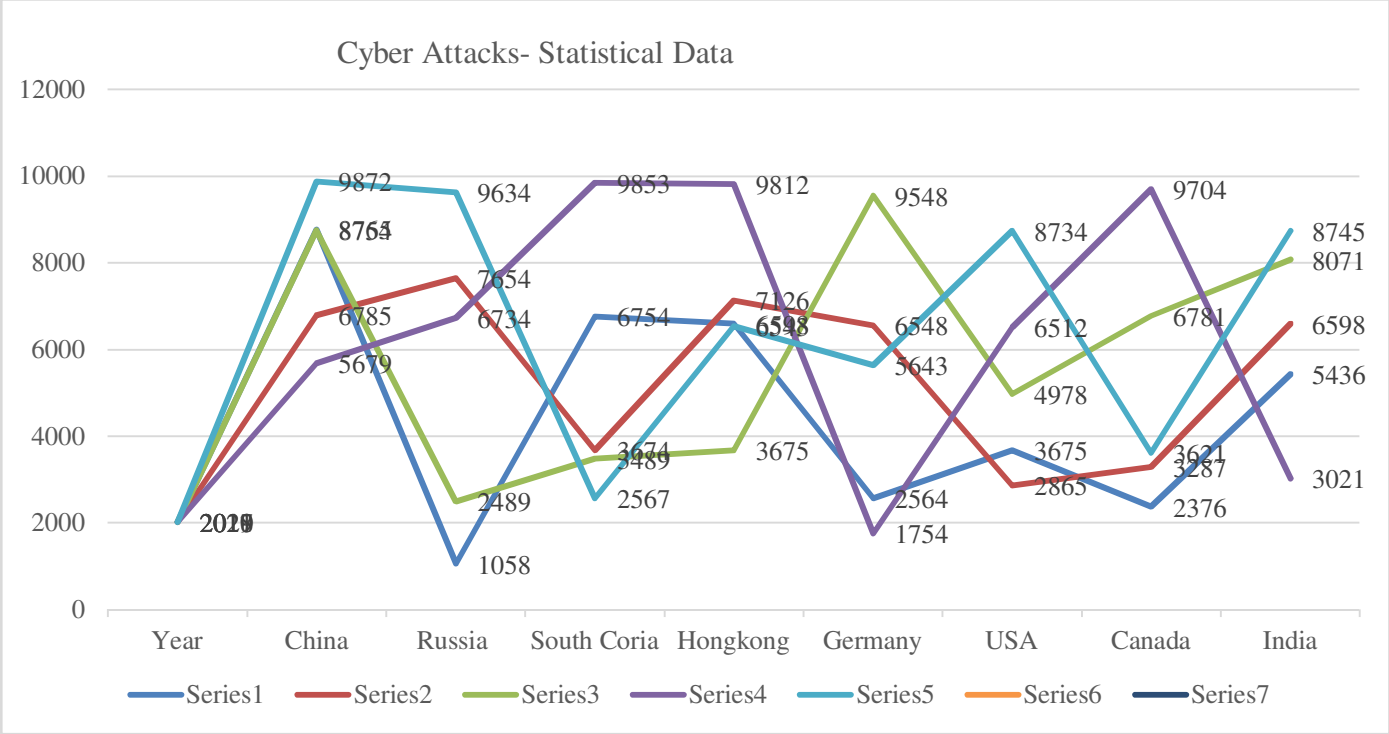


Figure. 3 The cyber-attacks attempted in different countries

A. Experiment & Implementation

ARP spoofing, DHCP poisoning, and DOS attacks are all examined in this study. System availability is reduced in DoS attacks to prevent genuine users from accessing systems. They impose computationally intensive tasks on the target by exploiting the system's flaws or just flooding it with an enormous number of pointless requests. The system services are severely harmed when the targeted server is taken offline for minutes or days at a time. As a result, effective detection of DoS assaults is critical to the safety of online services. When it comes to DoS flooding assaults, even while software patching helps fight against some of the most common attacks, it falls short in other ways. Network administrators are not in charge of the server that is known as the "rogue DHCP server." We utilized KALI Linux 2021.4, Hydra v9.2,10.3-10704 for BRUTEFORCE ATTACK, DHCP SPOOFING, and ARP POISONING. Wireshark 3.6.0 and Burp Suite Community Edition. ettercap 0.8.3.1. has been utilized. We utilized KALI Linux 2021.4 with ION CANNON | v.2.9.9.99 for a DOS attack.

B. ARP Implementations

ARP Poisoning refreshes its target computer's ARP cache using bogus ARP request and reply packets. As a result, the target computer is being deceived into thinking that the attacker machine (which has a completely different MAC and IP address) is the one that has the desired IP and MAC address. When an attacker intercepts packets transmitted from a target computer to its original destination, he or she can monitor them before they reach their final destination, which is the original target.

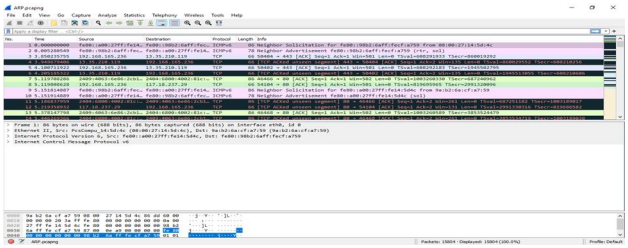


Figure. 4 ARP P-cap analyses

ARP is used to dynamically generate and maintain a mapping database between link local layer 2 addresses and layer 3 addresses in above Fig. 4.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

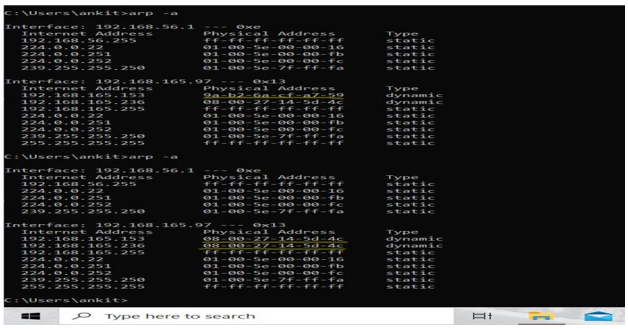


Figure. 5 Windows command prompts for ARP analysis

An IP addresses ARP table may be examined by using this command. In addition, it displays all entries in the ARP cache or table, as well. It is possible to utilize AR with the -g option. Using this command is similar to using ARP -a. the command arp -d: Remove an entry from the ARP table for a specified interface with this command.

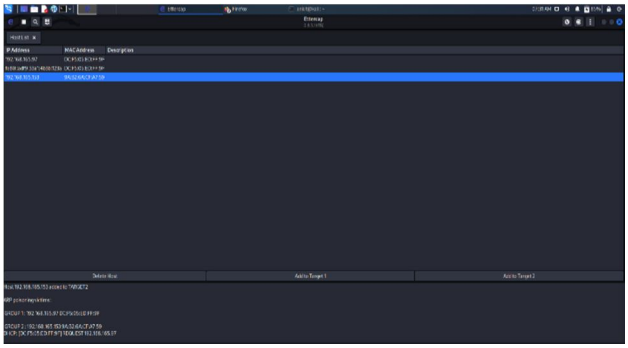


Figure. 6 Ettercap analysis

Like Dsniff, Ettercap may sniff communications and look for specified kinds of credentials for specific kinds of protocol types as a sniffing instrument (e.g., email passwords). Filtering (dropping packets based on specified filter criteria) and modifying traffic are other features. To put it another way, an ARP poisoning attack is one in which an attacker poisons the target computer's ARP cache by flooding it with fraudulent ARP request and response packets. Because the ARP answers have been falsified, frames sent from the victim's computer to the attacker's machine can be read. In the event of a successful ARP attempt, it is completely undetectable to the user.

C. Dynamic Host Configuration Protocol (Dhcp) Implemenations

It is possible to reserve an IP address for a specific device on your network, essentially preventing other devices from receiving the IP address from the router. This capability is called DHCP Reservation.

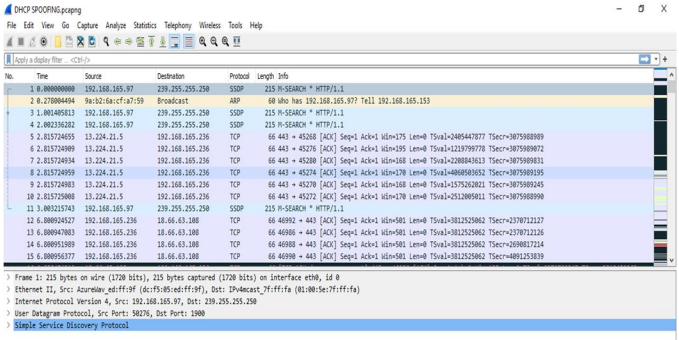


Figure. 7 DHCP spoofing

As seen in the Fig. 7 above, DHCP spoofing happens when an attacker attempts to reply to DHCP queries and lists itself (spoofs) as the default gateway or DNS server.

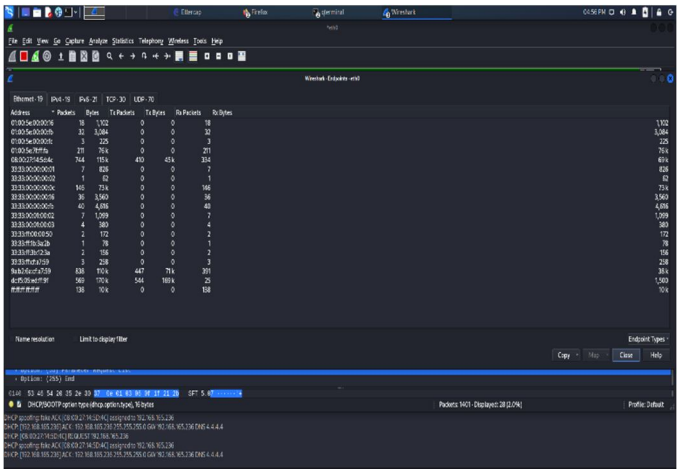


Figure. 8 The number of the DHCP packets

Using UDP services, it is a client-server protocol. There is a pool of IP addresses from which an IP address is drawn. There are 8 DHCP messages involved in DHCP, however the client and the server exchange mainly four messages in order to establish a connection (also known as the DORA process).

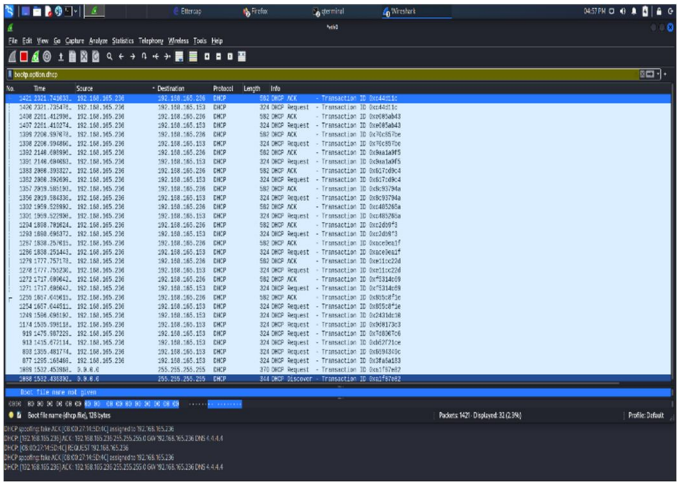


Figure. 9 DHCP command

The ifconfig command allows us to: Initiate the DHCP client – The command ifconfig interface DHCP start commences interaction between the DHCP client with DHCP server to receive an IP address with a fresh set of configuration settings.

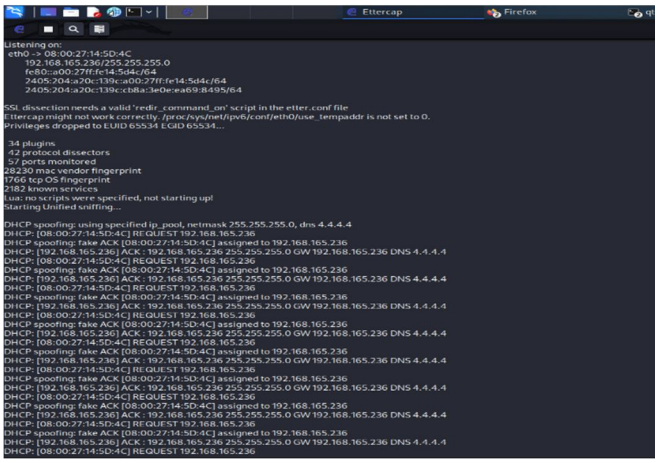


Figure. 10 DHCP Ettercap

We can defend your network from untrusted hosts by monitoring the traffic between your network's trusted DHCP servers. The following is possible because of this feature: monitoring the activity of the DHCP server. Filters off communications from untrusted DHCP servers.

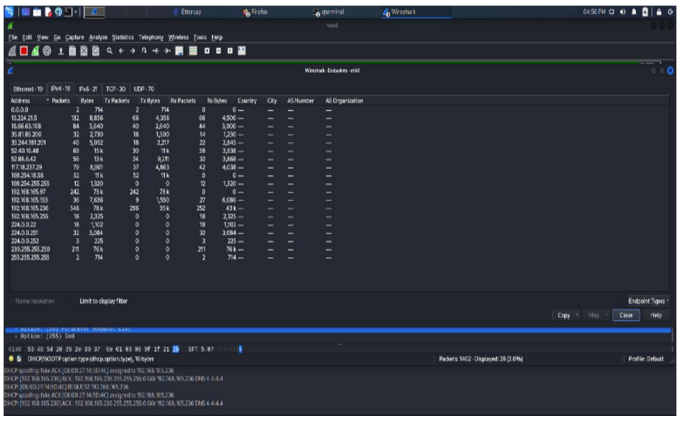


Figure. 11 DHCP IP address

Dynamic Host Configuration Protocol (DHCP), a client/server protocol, delivers IP addresses and other configuration data, such as subnet masks and default gateways, to an IP host.

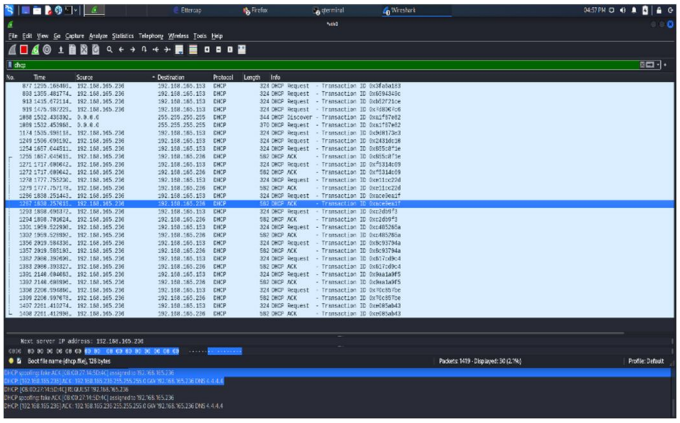


Figure. 12 DHCP protocol

It is possible to dynamically allocate an IP address to any device or node on a network using DHCP, a network management protocol (IP) (Internet Protocol). DHCP is responsible for automating and centrally managing these setups.

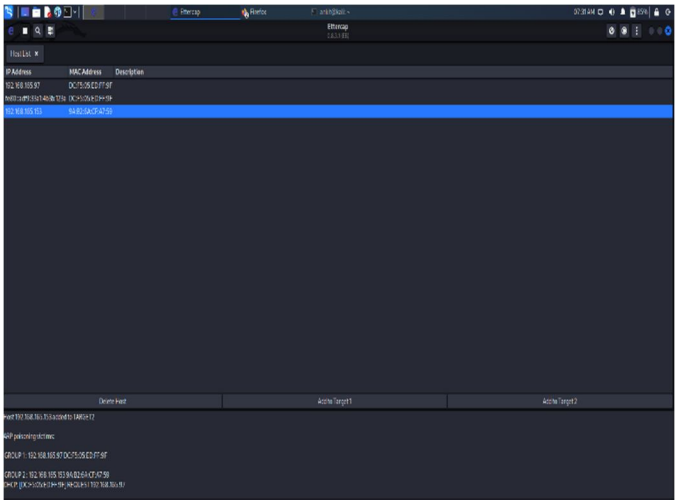


Figure. 13 Ettercap

Unix-based systems can benefit greatly from Ettercap, a packet sniffer, and ARP cache poisoning utility. It can sniff MAC and IP traffic, intercept and modify packets, decode passwords, and launch a denial-of-service attack on other Ethernet hosts. All of these capabilities are built into the malware.

D. TCP DoS Implemenations

Three-way handshake for establishing connections in TCP. State allocation on the server-side upon receipt of SYN to keep information about the unfinished connection. An SYN flood's objective is to clog up the server's resources, preventing it from responding to valid connections. This is done by having the client disregard the server's SYN, ACK, and not transmit the final ACK back to the server. As a result, the server keeps the partially allocated state from the original SYN request.

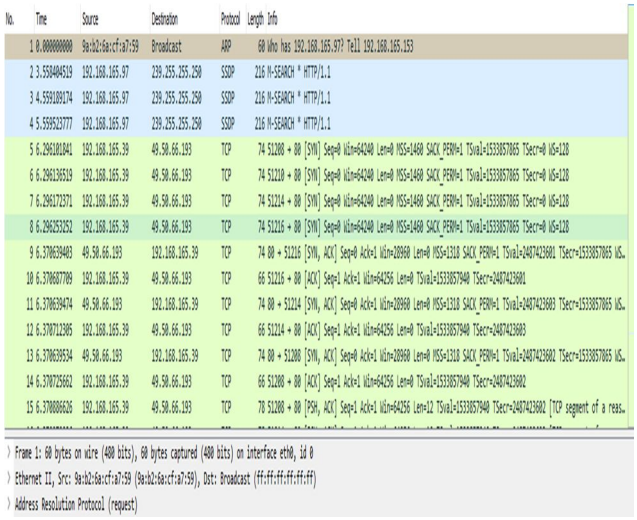


Figure. 14 TCP DoS

In a Distributed Denial of Service (DDoS) attack, the TCP SYN flood (also known as SYN flood) consumes resources on the targeted server and renders it useless (a.k.a. SYN flood) (a.k.a. SYN flood).

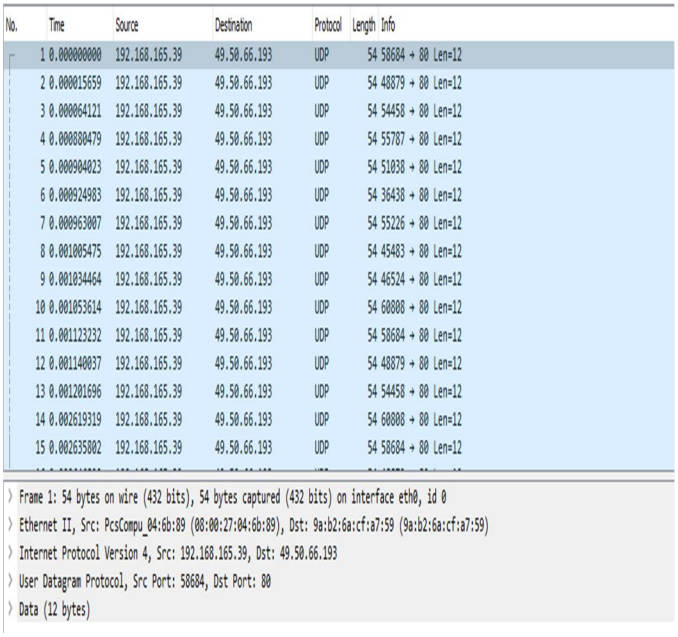


Figure. 15 UDP DoS

It's possible to perform a volumetric denial-of-service attack using UDP floods, in which the attacker uses UDP packets to flood arbitrary ports on the target host.

III. CONCLUSION

In this study, we use Kali Linux to analyze and identify DHCP, UDP Denial of Service, Transmission Control Protocol Denial of Service, and ARP Poisoning attacks. The ARP protocol (together with secure DHCP), as well as TCP DoS and UDP DoS, is more efficient in terms of both performance and security than ARP poisoning. Because the S-UARP request is unicast and routed solely to the secure DHCP server, it decreases broadcast congestion in the network. The more secure S-UARP is, the more difficult it is for an attacker to conduct an ARP poisoning assault. ARP packet content cannot be manipulated by an attacker; hence it is safe from message integrity attacks and masquerades attacks (when new ARP bogus packet injection can be done by an attacker). In addition, MAC spoofing attacks are no longer possible because of the enhanced security of the DHCP protocol. It's because these approaches didn't take into account DHCP's security concerns. The DHCP hunger attack cannot be mitigated by most of the strategies offered in the works to safeguard DHCP messages and objects. Because of the security flaws in local area networks, bandwidth on these networks is limited when there is a high volume of traffic, which has a detrimental impact on the network devices' processing performance. As a result, it has been established that the nerve lines that carry local network traffic have been cut off. DDoS attacks must be carried out by a huge number of computers to overwhelm a server's resources (DDoS Attack). Otherwise, the traffic created by a small set of machines will not accomplish the denial of service, which is what we want.

Conflicts of Interest (Mandatory)

There is no conflict of interest in this paper.

Author Contributions (Mandatory)

The study was conceptualized and designed by all of the writers. [complete name], [Ankit Sahu], and [Monika Dandotiya] do the material preparation and data analysis. It was authored by Abhinandan Dandotiya, and all of the contributors provided feedback on prior draughts. The final draft was authorized by all of the writers after it had been reviewed and revised by them all.

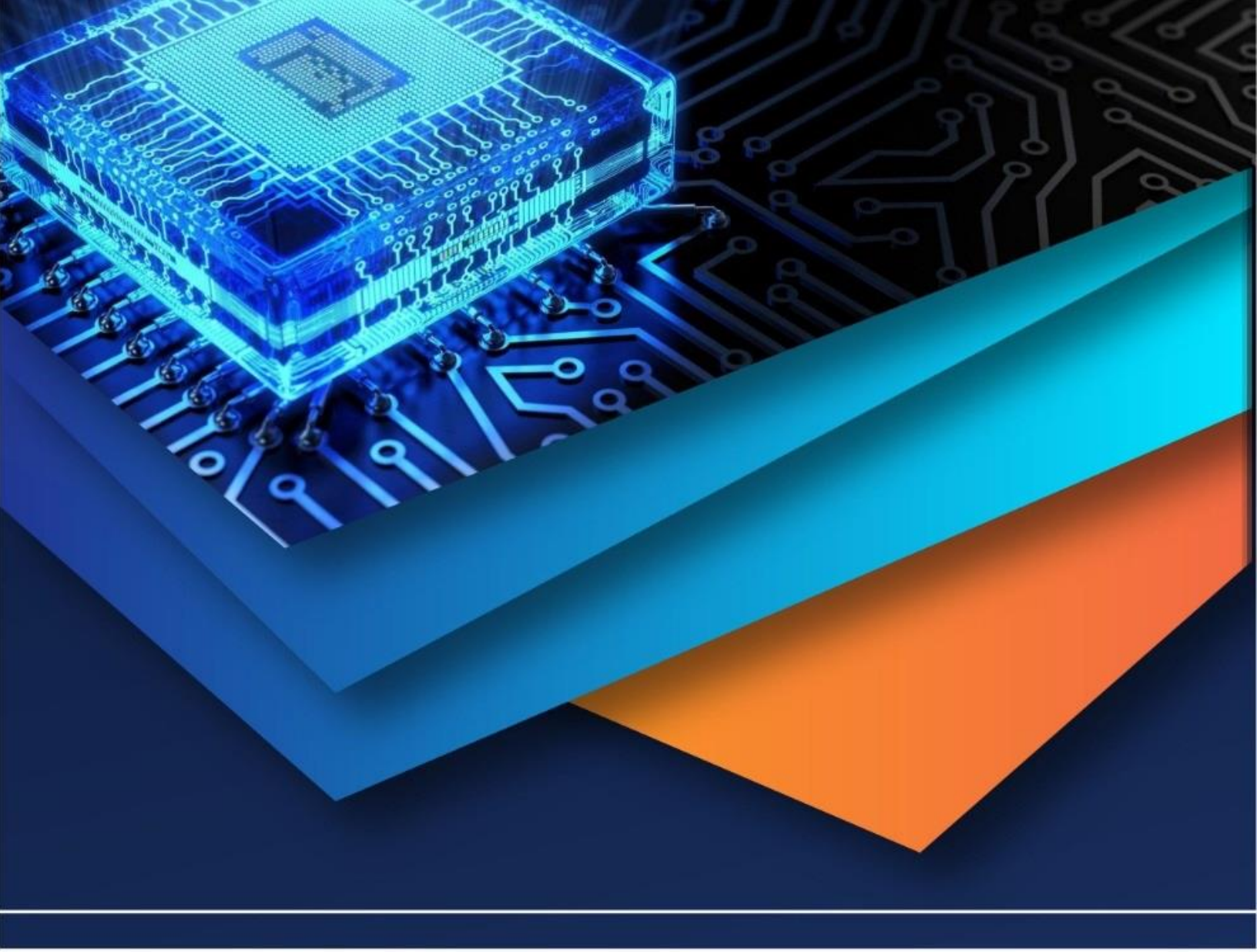
IV. ACKNOWLEDGMENTS

Acknowledgments are to show that the article is supported by what organization. For example, “This work was supported by the National Nature Science Foundation under Grant No. 405”.

REFERENCES

[1] H.C. Altunbasak, Layer 2 security inter-layering in networks, Thesis dissertation, Georgia Institute of Technology, 2006.
[2] R. Droms, “Dynamic host configuration protocol”, RFC 2131, 1997.
[3] D.C. Plummer, “An Ethernet address resolution protocol or converting network protocol addresses to 48-bit Ethernet address for transmission on Ethernet hardware”, RFC 826, 1982.
[4] J. Singh, G. Kaur, and J.A. Malhotra, “Comprehensive survey of current trends and challenges to mitigate ARP attacks”, In: International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, 2015.
[5] Y. Yao, W. Yang, Y. Yao and Y. Li, “A switch-based ARP attack containment strategy”, Second International Conference on Communication Systems, Networks and Applications, 1, pp. 123-126, 2010.
[6] M. M. Dessouky, W. Elkilany and N. Alfishawy, “A hardware approach for detecting the ARP attack,” The 7th International Conference on Informatics and Systems (INFOS), pp. 1-8, 2010.
[7] L. N. R. Group, “Arpwatch, The Ethernet Monitor Program; for keeping track of ethernet/ip address pairings”, (Last accessed April 17, 2012).
[8] ARP-Guard, Available at: http://www.arp-guard.com, Accessed October 2016.
[9] S. Puangpropitag and N. Masusai, “An efficient and feasible solution to ARP Spoof problem”, In: 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Vol. 02, pp. 910–913, 2009.
[10] D.S.G. Bhirud and V. Katkar, “Light weight approach for IP-ARP spoofing”, In: The Second Asian Himalayas International Conference on Internet (AH-ICI), pp. 1–5, 2011.
[11] X. Hou, Z. Jiang, and X. Tian, “The detection and prevention for ARP spoofing based on Snort”, In: The International Conference on Computer Application and System Modeling (ICCASM), pp. 137–139, 2010.
[12] A.P. Ortega, X.E. Marcos, L.D. Chiang, and C.L. Abad, “Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt”, In: Latin American Network Operations and Management Symposium (LANOMS), pp. 1–9, 2009.
[13] A.Z. Qian, “The automatic prevention and control research of ARP deception and implementation”, In: World Congress on Computer Science and Information Engineering, pp. 555–558, 2000.
[14] A. Boughrara and S. Mammar, “Implementation of a SNORT’s Output Plug-In in reaction to ARP Spoofing’s attack”, In: 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 643–647, 2012.
[15] Md. Ataullah and N. Chauhan, “ES-ARP: an efficient and secure address resolution protocol”, In: Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, pp. 1–5, 2012.
[16] Cisco Systems, Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) EW, Available at: http://www. cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/ 25ew/configuration/guide/conf/port_sec.html. (Accessed October 2016).
[17] Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Configuring DHCP Snooping, Available at: http://www.cisco.com/ c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.pdf. (Accessed September 2016).

[18] Catalyst 6500 Release 12.2SX Software Configuration Guide, Dynamic ARP Inspection, http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/config uration/guide/book/dynarp.html. (Accessed September 2016).
[19] D. Bruschi, A. Ornaghi, and E. Rosti, "S-ARP: a secure address resolution protocol", In: Proceedings of 19th Annual Computer Security Applications Conference, pp. 66–74, 2003.
[20] Y.I. Jerschow, C. Lochert, B. Scheuermann, and M. Mauve, "CLL: a cryptographic link layer for local area networks, security and cryptography for networks", In: Lecture Notes in Computer Science, Vol. 5229, pp. 21–38, 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY