



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



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

Monika Dandotiya¹, Abhinandan Singh Dandotiya², Nidhi Dandotiya³, Ankit Sahu⁴ ^{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.



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

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 webbased 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].



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VII July 2022- Available at www.ijraset.com

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.



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. 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.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VII July 2022- Available at www.ijraset.com

Interface: 102.100.50.1	C:\Users\ankit>arp -a				
Thermat Address Physical Address Type 1231.40.0775. 231.40.072130 01.00.50.077 114111 231.40.072130 01.00.50.00 01.00.111111 231.40.0721 01.00.100.00.076 114111 231.40.0721 01.00.100.00.076 114111 101.100.1120 01.00.00.076 114111 101.100.100.1120 01.00.076 114111 101.100.100.1120 01.00.076 114111 101.100.100.1120 01.00.076 114111 101.100.100.1120 01.00.076 114111 101.100.100.100.000 00 00 00 00 114111 101.100.100.100.000 00 00 00 00 00 00 00 00 00 00 00	Interface: 192.168.56	1 Ove			
102:100150:225:- 0:177:177:177:177:177 101111 231:00150:225:- 0:100:100:000 100:1111 10111 231:00150:225:- 0:100:100:000 100:1111 10111 231:00150:225:- 00:100:100:000 100:100:000 100:100:000 100:100:225:- 00:100:100:000 100:100:000 100:100:000 100:100:230:000 00:000:100:000 100:100:000 100:100:000 100:100:230:000 00:000:100:000 100:100:000 100:100:000 223:00:00:230:000 0:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000:000 100:100:000 100:100:000 230:00:00:200:000 0:000:000:000 100:100:000 100:100:000 230:00:00:000:000:000:000:000 100:100:0000	Internet Address	Physical Address	Type		
221 0.1 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0	192.168.56.255	FF-FF-FF-FF-FF-FF	static		
2224.04.09.251. 01.000.54.000.000-fb. static 2302.255.250.230 01.000.54.000.000-fb. static Datarrace: 129.255.250.230 01.000.54.000.000-fb. static Datarrace: 129.255.250.230 01.000.54.000.000-fb. static Datarrace: 129.255.250.230 01.000.54.000.000-fb. tatic Datarrace: 129.255.250.230 01.000.54.070.000-fb. tatic Datarrace: 129.255.250.250 01.000.54.070.000-fb. tatic Datarrace: 129.255.250.250 01.000.54.070.000-fb. tatic Datarrace: 01.000.54.070.000-fb. tatic tatic Datarrace: 01.000.54.070.000-fb. tatic tatic Datarrace: 01.000.54.070.000-fb. tatic tatic Datarrace: 01.000.54.070.000-fb. tatic tatic Datarrace: 01.000.54.071.071.071.071.071.071.071.071.071.071	224.0.0.22	01-00-50-00-00-16	static		
2234.0.0.2352	224.0.0.251	01-00-5e-00-00-fb	static		
250:255:255.200 00:100-55.27.77.76 100:rfac: 102:100:105.970813 100:rfac: 102:105:105.970813 100:rfac:102:105:105.97.114.57.67 100:rfac:102:105:200 201:00:105:220 201:00:105:220 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:221 201:00:	224 0 0 252	01 - 00 - 50 - 00 - 00 - fc	static		
Interface: 102.100.105.07 0x13 Interface: 102.100.105.07 0x13 Interface: 0x130 0x130 Interface: 0x130 0x130 Interface: 0x130 0x130 Interface: 0x130 0x130 Interface: 0x130 0x140 Interface: 0x140 0x141 Interface: 0x140 0x140 Interface: 0x140 0x140 Interface: 0x140 0x140 Interface: 0x140 0x140	239.255.255.250				
Internet Address Physical Address Physical Address 100:100:100:200 00:000:000 00:000:000 00:000 100:100:200 00:000:000 00:000 00:000 100:100:200 00:000:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:000 100:100:200 00:000 00:000 00:0000 100:100:100:200 00:0000 00:0000 <t< td=""><td>Interface: 192.168.16</td><td>5.97 0x13</td><td></td><td></td><td></td></t<>	Interface: 192.168.16	5.97 0x13			
132.100.105.25 0.0012000.001400000000000000000000000000	Internet Address	Physical Address	Type		
100:100:100:200 07:00:27:10:07:7 07 100:100:100:200 07:00:27:10:07:7 07 201:00:27:10:100:200 07:10:00:00:00:00:00:00:00:00:00:00:00:00:	192.168.165.153	9a-b2-6a-cf-a7-59	dynamic		
132,100,195,255 117,17,17,17,17,17,17,17,17,17,17,17,17,	192.168.165.236	08-00-27-14-5d-4c	dynamic		
2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 2231.0.0.221 Discretion of the second secon	192.168.165.255	FF-FF-FF-FF-FF-FF	static		
224.40.0 251. 01.000.50.000.000.000 51.0116 230.555.55.250.000 01.000.50.777.777.76 51.0116 230.555.255.250.000 100.577.7777.76 51.0116 230.555.255.250.000 100.577.7777.76 51.0116 230.555.255.250.000 50.1 100.577.7777 51.0116 107.100.557.255.777 100.557.7777777 51.0116 51.0116 230.555.255.000 77.777.777 51.0116 51.0116 230.555.555.250 01.000.5777.777.76 51.0116 51.0116 230.555.555.250 01.000.5777.777.76 51.0116 51.0116 230.555.555.250 01.000.5777.777.76 51.0116 51.0116 107.100.555.255 01.000.5777.777.76 51.0116 51.0116 107.100.5155.250 01.000.577.777.76 51.0116 51.0116 107.100.5155.250 01.000.577.077.76 51.0116 51.0116 107.100.5155 01.000.577.077.77 51.0116 51.0116 107.100.105.07.77.777.777.777 01.0116 51.0116 107.100.105.07.77.777.777 01.000.576 00.000.576 51.0116 107.100.105.07.77.7777.7777 01.000.576 00.000.576 51.0116 107.100.105.07.77 01.000.576 00.000.576 51.0116	224.0.0.22	01-00-5e-00-00-16	static		
224.6.0.252	224.0.0.251	01-00-5e-00-00-Fb	static		
J30:J30:J30:J30:J30:J30 01-00-30-27-77-77-77 Number Schemer J30:J30:J30:J30:J30:J30:J30:J30:J30:J30:	224.0.0.252	01-00-5e-00-00-fc	static		
235.255.255.255 (*)WarrStankitSarp = 0 Interface: 192.168.56.1 0xe Interface: 192.168.56.1 0xe Interface: 192.168.56.1 0xe 192.108.525 224.0.0.221 102.108.162.55 224.0.0.222 102.108.162.52 103.108.162.52 104.00.522 104.00.522 104.00.522 104.00.522 105.008.163.57 105.008.163.57 105.008.163.57 105.008.163.57 105.008.163.57 105.008.165.57 105.008.165.57 105.008.165.57 105.008.165.57 105.008.165.57 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155 105.008.155	239.255.255.250	01-00-5e-7f-ff-fa	static		
C: Wiserstumkitzerp					
Interface: 102.108.50.1 0xe Type: 103.708.2005 FTP162740747777 Type: Type: 103.708.2005 FTP16274077777777777777777 Type: Type: 224.0.0.0221 61.000.500000000 Type: Type: 224.0.0.0222 61.000.500000000 Type: Type: 224.0.0.0222 61.000.5000000000 Type: Type: 224.0.0.0222 61.000.50000000000 Type: Type: 224.0.0.0222 61.000.500000000000000000000000000000000					
Internet Address Physical Address Type 104 cross 01 cos s-00 cos 17 Title 2241 cos (22) 01 cos s-00 cos 17 Title 2241 cos (22) 01 cos s-00 cos 17 Title 2241 cos (22) 01 cos s-00 cos 17 Title 2241 cos (22) 01 cos s-00 cos 17 Title 230 cos (25) 01 cos s-00 cos 17 Title 104 cos (20) 01 cos s-00 cos 17 Title 105 cos (160: 155) 00 cos (27) co	Interface: 192.168.56	.1 0xe			
132 160 35 235 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177 177	Internet Address	Physical Address	Type		
221.0.0.027 01.00.00.00.00.00 10.00.00.00.00 221.0.0.027 01.00.00.00.00 10.00.00.00 221.0.0.027 01.00.00.00 00.00 Thernet Address Physical Address Type 100.000 Physical Address Physical Address 100.000 <t< td=""><td>192.168.56.255</td><td>ff-ff-ff-ff-ff-ff-ff</td><td>static</td><td></td><td></td></t<>	192.168.56.255	ff-ff-ff-ff-ff-ff-ff	static		
224.0-0.0-251 01.000-30-000-00-0 static 230.255.250.250 01.000-30-000-0 static Thereface: 102.100.105.07 static 103.255.250.250 01.000-30-07.0 static 104.255.256.250 01.000-30-07.0 static 105.105.105.107 01.000-30-07.0 static 102.106.105.107 01.000-30-07.0 dynamic 102.106.105.107 01.000-30-07.0 dynamic 102.106.105.107 01.000-30-00.0 dynamic 102.106.105.107 01.000-30-00.0 static 102.106.105.107 01.000-30-00.0 static 102.106.105.107 01.000-30-00.0 static 102.106.105.20 01.000-30-00.0 static 201.007.200 01.000-30-00.000-05 static 201.005.203.203 01.000-30-00.000-05 static 201.005.203.203 01.000-30-00.000-05 static 201.005.203.203 01.000-30-00.000-05 static 201.203.203.203 01.000-30-00.000-05 static CiWasersumkit> 01.000-000-05	224.0.0.22	01 - 00 - 5e - 00 - 00 - 16	static		
2234.0.0.322	224.0.0.251	01-00-5e-00-00-fb	static		
240.255.255.256 00.1-00-50-7777-70 static Therefore 100-100-105.07	224.0.0.252	01-00-5e-00-00-fc	static		
Interface: 102.108.103.07 0x13 Interface: 102.108.103.07 0x13 ID2.108.108.103.07. 01.002.27.14.534 0ynamic ID2.108.106.103.07 01.002.27.14.534 0ynamic ID2.108.106.103.07 01.002.27.14.534 0ynamic ID2.108.106.103.07 01.002.57.00.00 01.012.10 ID2.108.106.27 01.002.57.00.00 01.012.10 ID2.108.106.27 01.002.57.00 01.012.10 ID2.108.106.27 01.002.57.00 00.116.116 ID2.108.07 01.002.57.00 00.116.116 ID2.109.07	239.255.255.250	01-00-5e-7f-ff-fa	static		
Internet Address Physical Address 102:106:106:130 00:000 102:106:106:130 00:000 102:106:106:130 00:000 102:106:106:130 00:000 102:106:106:130 00:000 103:106:106:130 01:000 104:106:106:130 01:000 104:106:106:130 01:000 104:106:106:130 01:000 104:106:106:100 01:000 104:106:106 01:000 104:106:106 01:000 104:106:106 01:000 105:106:106 01:000 105:106:106 01:000 105:106:106 01:000 105:106:106 01:000 106:106:106 01:000 106:106:106 01:000 106:106:106 01:000 106:106:106 01:000 106:106:106 01:000 106:106:106 01:000 106:106:106 01:000 106:106:106 01:000	Interface: 192.168.10				
102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:103 102:108:105:105 102:108:105:105 102:108:105:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:108:105 102:105	Internet Address	Physical Address	Туре		
103:108:105:205 103:108:105:205 104:00:271 104:00:271 104:00:271 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:270 104:00:2	192.168.165.153	08-00-27-14-5d-4c	dynamic		
1392,1468,1456,255 ff+ff+ff+ff+ff+ff+ff static 1392,1468,1456,251 01.005.80-00.00 static 2241.616,2521 01.005.80-00.00 static 2241.616,2522 01.005.80-00.00 static 2241.616,2523 01.005.80-00.00 static 2251.255,2551,255 ff+ff+ff+ff+ff+ff static c:\Users\unklt> 01.005.80-00.00 static	192.168.165.236	08-00-27-14-5d-4c	dynamic		
224.0.0.0.22 01.000-50-00-00-10 static 224.0.0.0221 01.000-50-00-00-10 static 224.0.0.0222 01.000-50-00-00-10 static 224.0.0.0223 01.000-50-00-00-10 static 235.255.255.250 01.000-50-76-ff-fg static 235.255.255.255 01.000-50-76-ff-fg static CiVusersvanktz Static static	192.168.165.255	FF-FF-FF-FF-FF-FF	static		
251.0.0.251 01.00.30.000 00.100.100 201.00.250.000 01.00.100 00.000 201.000.000.000 01.000.000 01.000 201.000.000.000 01.000.000 01.000 201.000.000.000 01.000 01.000 201.000.000 00.000 01.000 201.000.000 00.000 01.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000 201.000 00.000 00.000	224.0.0.22	01-00-50-00-00-16	static		
234.6.06.252 01.00:37:00.60.45 stattc 235.255.255 55.755.755 rf-rf-rf-rf-rf stattc c::VLorestunktt>	224.0.0.251	01-00-5e-00-00-fb	static		
230.255.255.256 01-00-5e-7f-ff-fa static 255.255.255.255 eff-ff-ff-ff-ff static EI(Users\ankit>	224.0.0.252	01-00-5e-00-00-fc	static		
255,255,255,255 ff-ff-ff-ff static C:\Users\ankit>	239.255.255.250	01-00-5e-7f-ff-fa	static		
C:\Users\ankit>	255.255.255.255		static		
- Q Type here to search	C:\Users\ankit>				
		to search		H+	-

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.

S 💷 🧰 🍃 🖗 I		- Basen		0 6 (#110 B B D HARD
				0 6 1 0
Hortst #				
7 Address 92 (68, 965, 97 688 (6 89) 554 (1466) 5736	NACADINA Description OCFSIDECH496 OCFSIDECH496			
12/16/30/2014	94326439259			
				l I
				Aprilo Tanget 2
IN 192 108 105 153 acces	10 140 2012			
				Í.
KON DO ERIOS O DEFINI NON DO ERIOS O DEFINI	184.02/64/CF-07 59 [1608.657 112.108/105.17			

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.

Time	Source	Destination	Protocol	length Info	-
1 0.00000000	192.168.165.97	239.255.255.250	SSOP	215 N-SEARCH * HTTP/1.1	
2 0.278004494	9a:b2:6a:cf:a7:59	Broadcast	ARP	60 Who has 192.168.165.97? Tell 192.168.165.153	
3 1.001405813	192.168.165.97	239.255.255.250	SSDP	215 H-SEARCH * HTTP/1.1	
4 2.002336282	192.168.165.97	239.255.255.250	SSOP	215 M-SEARCH * HTTP/1.1	
5 2.815724655	13.224.21.5	192.168.165.236	TCP	66 443 + 45268 [ACK] Seg=1 Ack+1 Win+175 Len+0 TSval+2405447877 TSecr+3075988989	
6 2.815724909	13.224.21.5	192.168.165.236	TCP	66 443 + 45276 [ACK] Seg=1 Ack=1 Win=195 Len=0 TSval=1219799778 TSecr=3075989072	
7 2.815724934	13.224.21.5	192.168.165.236	TCP	66 443 + 45288 [ACK] Seg=1 Ack=1 Win=168 Len=0 TSval=2288843613 TSecr=3075989831	
8 2.815724959	13.224.21.5	192.168.165.236	TCP	66 443 + 45274 [ACK] Seg=1 Ack=1 Win=178 Len=0 TSval=4868583652 TSecr=3875989195	
9 2.815724983	13.224.21.5	192.168.165.236	TCP	66 443 + 45278 [ACK] Seg=1 Ack=1 Win=168 Len=0 TSval=1575262021 TSecr=3075989245	
10 2.815725008	13.224.21.5	192.168.165.236	TCP	66 443 + 45272 [ACK] Seq=1 Ack=1 Win=170 Len=0 T5val=2512805011 TSecr=3075988990	
11 3.003215743	192.168.165.97	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1	
12 6.880924527	192.168.165.236	18.66.63.108	TCP	66 46992 + 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 T5val=3812525062 TSecr=2370712127	
13 6.880947883	192.168.165.236	18.66.63.108	TCP	66 46986 + 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3812525062 TSecr=2370712126	
14 6.880951989	192.168.165.236	18.66.63.108	TCP	66 46988 + 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3812525062 TSecr=2690817214	
15 6.880956377	192.168.165.236	18.66.63.108	TCP	66 46990 + 443 [ACK] Seg=1 Ack=1 Win=501 Len=0 TSval=3812525062 TSecr=4091253839	

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.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VII July 2022- Available at www.ijraset.com

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	val 000000000000000000000000000000000000
Tor (m) <	D 2 wainin Goston end m 10 10 10 10 10 10 10 10 10 10
Image: Second	B B Known de daaken wet K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K
Benerit 9 Purt 1 Purt 2 Purt	xmax biotete ent xmax biotete ent xmax biotete ent xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax xmax
Bandi B, McJ McJ Total Total Total Total CD240000 B TO D Min Non	s 100 304 305 305 305 305 305 305 305 305 305 305
Attra Totade Byen Byen Totade Byen Totade Byen Byen Totade Byen Byen Totade Byen By	a 100 20 20 20 20 20 20 20 20 20 20 20 20 2
CDD/sECOND II UCL 0 0 II CDD/sECOND II UCL 0 0 II CDD/sECOND II III 0 0 0 III CDD/sECOND III IIII 0 0 0 III CDD/sECOND IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	121 121 121 121 121 121 121 121 121 121
	181 200 200
Name resolution Limit to skiplay filter	ExtentType: Cap + May Care Heb
· Option: (255) End	
110 53 45 54 28 35 2e 39 37 0e 61 63 95 94 11 21 25 SFT 5.67	
DHCP/SODTP optien type (dhcp.optien.type), 16 bytes	Paders W01-Displayet: 28 (2.0%) Profile: Default
KP: gooding: https://doi.org/10.1016/j.com/sof.2016.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.00176.0017 Augusta and analysis analysis Analysis analysis anal Analysis analysis anal	

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).

S 💷 🖿 🎍 🕅 🖿	* <u>s</u>	e Ettercap	Frefax	🗞 çtermiral	4 Wreshark		0457PH C 40 8 8 6 6 0
6							0.0 0
File Edit View Go Ca	plane Analyze Statistics	Telephony Wireless Tools H	Ka .				
4-40.1		0					
		···· ··· ··· 🖬 🔳 🖬					
bootp option thep							00.
No. Time	Source	Destination	totacci Length Info				
1421 2321 741633.	192.168.165.236	192.158.165.256	HCP 582 CHCP	ACK - Transaction 1	D 2xc44511c		
5426 2321.735478.	192.158.145.236	192.168.185.153	324 OKCP 324 OKCP	Request - Transaction II	0 Oct44d11c		
1406 2201.412936.	132-108-295-298	102.108.100.220	HUP 002 URUP	ALK - IFINSACCION II	D UKDUBSAD43		
1407 2201.410214.	192.100.205.200	192.100.100.103	HUP 324 URUP	weglest - Irmisaccion II	D UXPUESAD43		
1305 2206 35/610.	132.100.000.200	192,100,100,200 0	1417 UD2 UD2 UD2	Semiest - Transcript II	D OXTRESTIC		
1302 21/2 /01051	102 168 185 218	102 158 165 216 5	1870 663 5810	NY . Transaction 1	h dygaata9f5		
1391 2148 484661	192.158.145.234	192, 168, 165, 153	SHCP 324 DHCP	Benjest - Transaction II	D Ochestal S		
1383 2388 .393327.	192.168.165.236	292.158.165.236	HCP 582 DRCP	ACK . Transaction II	D Bx807cd9c4		
1352 2958 .392699.	192.168.165.236	192.150.165.153	HCP 324 DHCP	Request - Transaction II	0 0x617cd9c4		
1357 2919.585190.	192.168.145.236	192.168.165.226	CHCP 582 DHCP	ACK - Transaction II	0 0x8c93794a		
1356 2919.584336.	192.168.165.236	192.168.165.153	HCP 324 DHCP	Request - Transaction II	D 0x8c93794a		
1302 1959.528992.	192.168.165.236	192.158.165.236	CHCP S82 DHCP	ACK - Transaction II	D 0xc405265a		
1301 1959.522938.	192.158.165.236	192.158.165.153	CHCP 324 DHDP	Request - Transaction II	D 0xc485285a		
1204 1808.781624.	192.168.165.236	192.158.165.236	CHCP 582 CHCP	ACK - Transaction II	D 0xc2db0f3		
1293 1698.695372.	192.168.165.236	192.150.165.153	CHCP 324 DHCP	Request - Transaction I	D Dec2d5813		
1287 1838.257615.	192.158.145.236	192.108.105.226	HCP 582 DKDP	ACK · Transaction II	D 0xacebea1f		
1286 1838.251443.	192.168.265.236	192.168.165.153	HCP 324 DHCP	Request - Transaction 1	D Oxaceleait		
1278 1777.757178.	192.158.365.236	192.168.185.228	DRCP 552 ORCP	ACK - Transaction II	D Deelloczad		
12/8 1777.755236.	192.158.165.236	192.108.165.153	HCP 324 DRCP	Request . Transaction II	D Oxellcc220		
12/2 1/1/ (00)042.	192.100.205.200	192.100.100.200 0	MLP 002 URUP	ALK - IFINSACCION II	D 0072314009		
1271 1111 (000642.	NO. 100, PDJ. 200	107.100.007.103	ALC: 024 USUP	Megresi - Transaction 2	n destantine		
1254 1657 646511	192.100.299.200	102.100.100.200 0	1870 104 DEC	Semiest - Transaction 1	D 0x855+8+14		
1249 1598 498190	192.158.165.216	192, 168, 165, 153	UKP 324 DHDP	Request - Transaction 1	D 0x2431dc18		
1134 1535 .5981 58.	192.158.165.236	192, 168, 185, 193	HCP 324 DHCP	Benuest - Transaction II	0.0x948173+3		
919 1475 .987223.	192.168.165.236	192.150.165.153	HCP 324 DHCP	Request - Transaction II	0 0x7d8067c6		
913 1415.672114.	192.168.165.236	192.168.185.153	CHCP 324 DHCP	Request - Transaction II	0.0x862f21ce		
803 1355.481774.	192.168.165.236	192.158.165.153 B	CHCP 324 DHCP	Request . Transaction II	D 0x6594349c		
877 1295.168499.	192.168.165.236	192.158.165.153	CHCP 324 DHCP	Request - Transaction II	D 0x3fa5a183		
1889 1532 .453968.	3.8.8.0	255.255.255.255	CHCP 370 DHCP	Request - Transaction II	D 0xh1f87#82		
1888 1532.435332.	3.8.6.6	255.215.255.215	CHCP 344 DHCP	Discover - Transaction 1	D 0xa1f87e82		
Boot file more m	ot piven						
CRDC 80 90 90 00 08	CO 10 10 CR CO 10 R	1 30 30 08 08 09 ······					1
Boot file name (dhe	p.file), 128 bytes					Packets 1421 · Displayed: 32 (2.3%)	Profile: Default
DHCP specifing: Take ACK [CB) DHCP: [192.168.165.235] ACK	CD 27 10:5D:00 assigned to 1 192 168 165 295 255 255 25	92.768.165.236 5.0 Gov 192.768.765.236 DNS 4.4					
SHOP (CREDITY MEDICIN	0051192168,765236						
procession of the ACC (CB)	A DE DATE ANTE ANTE ANTE ANTE ANTE ANTE ANTE A	12-15-10-22-00 C A CHANGE WE WE WE WE HAVE A					
umon (102-108-105-236) ACC							

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.

😫 💷 🚍 🌛 🕪 💷 × 🔤 🖉	Ettercap	Firefox	🖬 🛃 🖬
e 🔲 a 🛢			
Utening on: eth) -> 08:00:27:14:50:4C 192.168.165.236(255.255.255.0 fc80::a00.27/ffc14:5d4c/64 2405:204:a70c:139c:a00:27/ffc14:5d4c/64 2405:204:a70c:139c:a08:a1e0c=ax69:8495/64			
SSL dissection needs a valid 'redir_command_on' script in the et			
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0 Privileges dropped to EUID 65534 EGID 65534	0/use_tempaddr is not set to 0.		
34 plugins 42 protocol dissectors 57 ports monitored 8230 max evendor fingerprint 8230 max evendor fingerprint 2182 known services 1282 known services 1283 known services			
Starting Unified sniffing DHCP-spoofing: using specified ip_pool, netmask 255.255.255.0 pulsep.opa.opa.txt.pd.ed.pc.ou/perstan.tr///www.sca.opa.txt.			
DHCP spoofing: fake ACK (08:00:27:14:5D:4C] assigned to 192.1 DHCP: [192.168.165.236] ACK : 192.168.165.236 255.255.255.0 DHCP: [08:00:27:14:5D:4C] REGUEST 192.168.165.236 DHCP ispoofing: fake ACK (08:00:27:14:5D:4C] assigned to 192.1 DHCP: 103:168.165.236] ArK : 102.168.165.236 255.555 555.0	168.165.236 GW 192.168.165.236 DNS 4.4.4.4 168.165.236 GW 192.168.165.236 DNS 4.4.4.4		
DHCP: [08:00:27:14:5D:4C] REGUEST 192:168.165.236 DHCP spoofing: Take ACK [08:00:27:14:5D:4C] assigned to 192.1 DHCP: [192:168.165.236] ACK: 192.168.165.236 255.255.255.255 DHCP: [08:00:27:14:5D:4C] REGUEST 192.168.165.236	168.165.236 GW 192.168.165.236 DNS 4.4.4.4		
DHCP: 192.168.165.236) ACK 192.168.165.236 255.255.0 DHCP: 192.168.165.236 ACK 192.168.165.236 255.255.0 DHCP: [08:00:27:14:5D:4C] REQUEST 192.168.165.236 DHCP spoofing: fake ACK [08:00:27:14:5D:4C] assigned to 192.1	GW 192.168.165.236 DNS 4.4.4.4 168.165.236 DNS 4.4.4.4		
LINCF: [192.108.105.230] ACK : 192.108.105.230 253.232.232.232.0 DHCP: [08:00:27:14:50:4C] REQUEST 192.108.105.236 DHCP spoofing: fake ACK [08:00:27:14:50:4C] assigned to 192.1 DHCP: [192.168.165.236] ACK : 192.108.105.236 255.255.255.0 DHCP: [192.168.105.236] ACK : 192.108.105.236 255.255.255.0	GW 192.165.155.236 DNS 4.4.4.4 GW 192.168.165.236 DNS 4.4.4.4		
DHCP : [08:00:27:14:30:46] REAUEST 192:108.105:230 DHCP : [09:168.165:236] ACK [08:00:27:14:5D:4C] assigned to 192:1 DHCP: [08:00:27:14:5D:4C] REQUEST 192:168.165:236	168.165.236 GW 192.168.165.236 DNS 4.4.4.4		
DHCP spoofing: Take ACK [08:00:27:14:5D:4C] assigned to 192.1 DHCP: [192.168.165.236] ACK : 192.168.165.236 255.255.255.0 DHCP: [08:00:27:14:5D:4C] REQUEST 192.168.165.236	168.165.236 GW 192.168.165.236 DNS 4.4.4.4		
Figure. 10) DHCP Etterca	р	

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.

S 💷 🗂 🎍 🤅			ap 🔥 Fre	fax 🛛	oterminal 🧧	0 Wresherk	C4.56PH 🖸 🚯 🛔 🙆 🏔 O
8							000
file fall yew Ge	Sectore Analyze State	itics Telephony Windess	tels Help				
₫ ∎ ₫ ⊚.	1 🖬 🖾 🖻 🔍 +	+ n + + 🖪 📕					
4				when	tark Crajokys end		0.00
Dhemet-10 Pv	1-19 Ph6-21 TCP-30	UDP-70					
Address - Pac	Ants Byles TePacke				AS Organization		
0.0.0.0							
13.224.21.5	132 8,856	66 4,355	66 4,500 -				
35,81,85,200	30 2780	18 1.505	14 1230 -				
35,244,381,201							
52.40.15.48		30 11k	39 3,138				
5286.6.42 17238.23239	50 13k 20 8.001	24 R.211 37 4.863	22 3,888				
108,254,18,58	52 11k	52 TK	0 0-				
109.254.255.255			12 1,320				
192,168,165,97	242 73k	242 738	0 0-				
102 108 105 236	548 78.8	216 35k	252 (1) -				
192.168.105.255							
224.0.0.22			18 1,102				
224.0.0.251	32 3,084		1 225-				
239.255 255 250			211 76k-				
255,235,255,255							
and the second second							for the form
Name resolution	Limit to clipity filb	*					Endpoint Types *
							Copy Map Ellose Help
+ 0x11001 (255	Cond	a					
A144 63 45 54 5							
0 10 0HCP/S001	e as ze as ar de di Poption type (dhcp.option.ty	es as ar in zi in sh gej, 16 bytes				Packets: 1402 - Displayed: 28 (2.0%)	Profile: Default
DECP spooling take AD							
DECP 108 00 17 M 4D	ACTIVICAL EST (93) 168, 765, 1	15.1.2.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1					
CHCP spooling take AD							
DHCP: [102.168.165.230							

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.

📉 💷 🖿 💊 🧿 🎟 🗉 🔟	Ettercap	Rector	a dermital	4 Wresherk		04:57 PH C 40 A 🛔 🛔 G
4						
Fie Edit Vew Go Capture Analyze Statistics	Telephony Wireless Tools Help					
₫ ∎₫◎±∎⊠₫ ٩+→	·· + → 📑 🖬 🖬 🖬	1 🔛				
1 dag						00
No. Time Source	Destination Protoco	l Lensth Info				
877 1295.165491. 192.158.365.236	192.158.165.153 EHCP	324 DHDP Reque	st - Transaction	10 0x3fa5a183		
803 1355 .481774. 192 168 165 236	192.168.165.153 EHCP	324 DHCP Reque	st - Transaction	ID 0x6594348c		
913 1415.672114, 192.168.165.236	192.150.165.153 EHCP	324 DECP Reque	st - Transaction	ID 0xbd2f21ce		
919 1475.587221. 192.188.345.236	192.108.165.153 EMCP	324 DKDF Reque	ist - Transaction	1D 0x 46836406		
2000 1532 433382 9.0.0.0	205.210.250.215 UM.P	344 0802 91500	WER - TRANSACCION	10 0X8175/002		
1009 1532 453900. 0.0.0.0 1174 1535 400110 102 100 100 545 254	100.200.200.200 ERLP	210 DELP REQUE	st - Transaction	10 0X8110/802		
1214 1000-100101 102 100 000 200	102 100 165 152 5970	224 0800 06010	at Transcript	TD DePartdena		
1254 1657 646511, 192 168 165 216	192 158 165 153 EMP	324 DECP Repue	st - Transaction	TD GuidtStaffie		
1255 1857 - 645615, 192, 188, 145, 236	192, 188, 185, 226 EHCP	582 DROP ACK	- Transaction	ID OchiSchile		
1271 1717.400642. 192.108.165.236	192.108.165.113 EMCP	324 DRCP Reque	st - Transaction	1D 0x*1314c09		
1272 1717.001042. 192.160.105.230	192.108.165.206 CHCP	582 DECP ACK	- Transaction	2D 0xf5314c09		
1278 1777.755230. 182.188.165.236	192.168.165.153 DHCP	324 DECP Regue	nt - Transaction	ID Ocelloc22d		
1279 1777.757178. 192.168.145.236	192.168.165.226 EHCP	552 DECP ACK	 Transaction 	ID Oxelice226		
1286 1838 251443 192 168 265 236	192.158.165.153 EHCP	324 DHOP Reque	st - Transaction	1D OxaceBeaif		
1217 1838.257811. 182.158.165.236	192.150.165.226 CHCP	562 DECP ACK	 Transaction 	ID OcaceBealf		
1293 1898 491372. 192.168.145.236	192.168.165.153 EHCP	324 DHCP Reque	ist - Transaction	10 0xr2db913		
1214 1898.789824. 192.108.295.299	292.108.260.200 DW.P	182 DROP 74.4	- 1F8854CC100	10 0xc2009*3		
1305 1909-122980. 192-100-205-220 1305 1958 530851 107 108 545 314	192.100.100.103 ER.P	524 DECH KROLE	St - Iransaction	10 0x14052558		
3302 1909.52(922. 152.100.955.200	102 108 165 102 FMTB	232 URLP ALL 234 (902) Junio	 Transcipt 	10 0404852858 10 0486827845		
1357 3918 505181 102 168 145 334	102 100 165 216 5400	COLONIC NY	- Transaction	TD DeBr@1794a		
1307 2002 100450 107 168 545 214	192 140 145 152 2470	324 PBPD Denie	at . Transaction	10. 0x612rdle4		
1383 2866 393327. 112.158.145.236	192, 168, 165, 276 EHCP	SIK2 OKCP ACK	- Transaction	ID 0x607cd9c4		
1391 2146 (94663, 192 168, 165 236	192,108,165,153 EMCP	324 DECP Reque	st - Transaction	1D OchalaH5		
1392 2146 691996. 192.158.165.236	192.168.185.226 EHCP	582 DECP ACK	- Transaction	10 Ochestahf5		
1308 2206.194866. 132.158.145.236	192.168.165.113 EMCP	324 DRCP Reque	st · Transaction	10 0x PCc85 Fbe		
1309 2208.997678. 192.168.165.236	192.168.165.236 EHCP	582 DHOP ACK	- Transaction	ID 0x76c85Toe		
1407 2281.410274. 182.158.165.236	192.158.165.153 EHCP	324 DRDP Reque	st - Transaction	ID 0xe085ab43		
L 1408 2201.412990. 192.158.105.230	192.158.565.226 DHCP	582 DECP ACK	 Transaction 	10 0xe485ab43		
Next server IP address: 112.158.165.23						
CITCE BD 30 30 00 08 08 63 63 50 68 63 63 8						
A Boot file name idean Biel, 178 hater	and the second se				Reviews 1028 - Displayed: 30(2) 594	Profile: Defect
a contrast in the bardward marsher					Contraction of the state of the state	Contraction of the second s
CPCP second contract of CO 27 14-50:40 ensigned to 3	57.45.85.739					
414 F [117 Bill 103 F 10 [12 Bill 105 215 255 255 25	ALLOW DOLLAR AND ADDED S ALLE					
and persons manufacture 20151 92.068 85.236						
and the second s	CARDINAL SCIENCE AND AND A					
ALAL TOT REPORT AND AND TO						

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.

		E HERLED	Hartor		0 🏦 #28 🖬 🔹 🕁 KA 12:50
				Ettercap 1.6.3.3 EE	89100
Hattist ×					
IP Address	MACAddress Description	in .			
192 168 155 97	DC/5/05/ED/F/SF				
1080124013331463110	Sa DCHSISSEDHISH				
192.108.305.753	SAED:MCK4759				
Fort 192 158 165 158 act	Stel to TARGET2				
GRP poisoning sictimes					
GROUP 1: 192 168 165 9					
GROUP 2: 192 168 165 1 DHCP (DCH5/0XE01H1	53 94 82 64 67 47 59 94 (NECUES) 192 168 365 97				

Figure. 13 Ettercap

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VII July 2022- Available at www.ijraset.com

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.

1	lo. Tine	Source	Destination	Protocol	Length Info						
	1 0.00000000	9a:b2:6a:cf:a7:59	Broadcast	ARP	60 Who has 192.168.165.97? Tell 192.168.165.153						
	2 3.558404519	192.168.165.97	239.255.255.250	SSOP	216 N-SEARCH * HTTP/1.1						
	3 4,559189174	192.168.165.97	239.255.255.250	SSOP	216 N-SEARCH * HTTP/1.1						
	4 5.559523777	192.168.165.97	239.255.255.250	SSOP	216 N-SEARCH * HTTP/1.1						
	5 6.296101841	192.168.165.39	49.50.66.193	TCP	74 51288 + 88 [SYN] Seq=0 Nin=64240 Len=0 NS5=1468 SACK_PEXM=1 T5val=1533057865 TSecr=0 NS=128						
	6 6.296136519	192.168.165.39	49.50.66.193	TCP	74 51210 + 80 [SYN] Seq=0 Nin=64240 Len=0 NS5=1460 SACK_PEXM=1 TSval=1533057865 TSecr=0 NS=128						
	7 6.296172371	192.168.165.39	49.50.66.193	TCP	74 51214 + 80 [SYN] Seq=0 Nin=64240 Len=0 NS5=1460 SACK_PEM=1 TSval=1533057865 TSecr=0 NS=128						
	8 6.296253252	192.168.165.39	49.50.66.193	TCP	74 51216 + 80 [SYN] Seq=0 Nin=64240 Len=0 NS5=1460 SACK_PEM=1 TSval=1533057865 TSecr=0 NS=128						
	9 6.378639483	49.58.66.193	192.168.165.39	TCP	74 80 + 51216 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1318 SACK_PERM=1 TSval=2487423601 TSecr=1533857865 WS.						
	10 6.370687709	192.168.165.39	49.50.66.193	TCP	66 51216 + 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T5val=1533857940 TSecr=2487423601						
	11 6.370639474	49.58.66.193	192.168.165.39	TCP	74 00 + 51214 [SYN, ACK] Seq=0 Ack=1 Win=20960 Len=0 MSS=1310 SACK_PERV=1 TSval=2407423603 TSecr=1533857865 WS.						
	12 6.370712305	192.168.165.39	49.50.66.193	TCP	66 51214 + 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T5val=1533857940 T5ecn=2487423683						
	13 6.370639534	49.58.66.193	192.168.165.39	TCP	74 80 + 51200 [SYN, ACK] Seq=0 Ack=1 Win=20960 Len=0 MSS=1310 SACK_PERM=1 TSval=2407423602 TSecr=1533857065 WS.						
	14 6.370725662	192.168.165.39	49.50.66.193	TCP	66 51288 + 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1533857940 TSecr=2487423682						
	15 6.370686626	192.168.165.39	49.50.66.193	TCP	78 51208 + 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=12 TSval=1533057940 TSecr=2407423002 [TCP segment of a reas						
	(1) A start of the second o										
) Etharnat II Serve	02+h7+K2+cf+27+50 (02	*h7*fa*cf*a7*50) Det*	Rmadra	24 (#14-44-44-44-44)						
	r santas agus valennennen (valennennen) (valennennen) valennennen (ministrististist)) blenne Banlista Bastani (valennet)										
	Hadress Nesotacton	Lincores (ichaese)									

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).

No. Ime Source Destruction Protocol Length Imp 1 0.000000000 192.168.155.39 49.50.65.133 UDP 54.58624 + 80 Len=12 2 0.000005559 192.168.155.39 49.50.65.133 UDP 54.48879 + 80 Len=12 3 0.000064121 192.168.155.39 49.50.65.133 UDP 54.5458 + 80 Len=12 4 0.000004023 192.168.155.39 49.50.65.133 UDP 54.5458 + 80 Len=12 5 0.000004023 192.168.155.39 49.50.65.133 UDP 54.5438 + 80 Len=12 6 0.000024083 192.168.155.39 49.50.65.133 UDP 54.5438 + 80 Len=12 7 0.00006007 192.168.155.39 49.50.65.133 UDP 54.5453 + 80 Len=12 9 0.00105514 192.168.155.39 49.50.65.133 UDP 54.6524 + 80 Len=12 10 0.00105514 192.168.155.39 49.50.66.133 UDP 54.6624 + 80 Len=12 12 <td< th=""><th></th><th>Terr</th><th>C</th><th>Destination</th><th>Destand</th><th>Lough tof</th><th></th></td<>		Terr	C	Destination	Destand	Lough tof	
1 0.000000000 192.168.165.39 49.50.66.193 UDP 54.58684 + 80 Lem=12 2 0.000015559 192.168.155.39 49.50.66.193 UDP 54.48879 + 80 Lem=12 3 0.000064121 192.168.155.39 49.50.66.193 UDP 54.5458 + 80 Lem=12 4 0.00006479 192.168.155.39 49.50.66.193 UDP 54.5458 + 80 Lem=12 5 0.000064023 192.168.155.39 49.50.66.193 UDP 54.54684 + 80 Lem=12 6 0.000064023 192.168.155.39 49.50.66.193 UDP 54.54584 + 80 Lem=12 7 0.00005007 192.168.155.39 49.50.66.193 UDP 54.54583 + 80 Lem=12 9 0.001805475 192.168.155.39 49.50.66.193 UDP 54.45524 + 80 Lem=12 10 0.001805474 192.168.15.39 49.50.66.193 UDP 54.46524 + 80 Lem=12 10 0.001125232 192.168.15.39 49.50.66.193 UDP 54.56884 + 80 Lem=12 12 0.001140637 192.168.15.39 49.50.66.193 UDP <th>N0,</th> <td>Ime</td> <td>Source</td> <td>Destnation</td> <td>Protocol</td> <td>Length Into</td> <td></td>	N0,	Ime	Source	Destnation	Protocol	Length Into	
2 0.000015559 192.168.155.39 49.50.66.193 UDP 54 48679 + 80 Lem-12 3 0.000064121 192.168.155.39 49.50.66.193 UDP 54 54586 + 80 Lem-12 4 0.000064023 192.168.155.39 49.50.66.193 UDP 54 51038 + 80 Lem-12 5 0.000964083 192.168.155.39 49.50.66.193 UDP 54 54638 + 80 Lem-12 7 0.000954087 192.168.155.39 49.50.66.193 UDP 54 55226 + 80 Lem-12 8 0.001095475 192.168.155.39 49.50.66.193 UDP 54 45483 + 80 Lem-12 9 0.00185464 192.168.155.39 49.50.66.193 UDP 54 45524 + 80 Lem-12 10 0.00125221 192.168.155.39 49.50.66.193 UDP 54 45524 + 80 Lem-12 11 0.00125222 192.168.155.39 49.50.66.193 UDP 54 45624 + 80 Lem-12 12 0.001486464 192.168.155.39 49.50.66.193 UDP 54 46524 + 80 Lem-12 13 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46828 + 80 Lem-12 13 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46828 + 80 Lem-12 14 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.00126561 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.00125261 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.00125269 192.168.155.39 49.50.66.193 UDP 54 54684 + 80 Lem-12 15 0.00125269 192.168.155.39 49.50.66.193 UDP 54 54684 + 80 Lem-12 15 0.00125269 192.168.155.39 49.50.66.193 UDP 54 54684 + 80 Lem-12 15 0.00125269 192.168.155.39 49.50.66.193 UDP 54 54688 + 80 Lem-12 15 0.00125269 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12	Г	1 0.000000000	192.168.165.39	49.50.66.193	UDP	54 58684 → 80 Len=12	
3 0.000064121 192.168.155.39 49.50.66.193 UDP 54 54558 + 80 Lem-12 4 0.000080479 192.168.155.39 49.50.66.193 UDP 54 51038 + 80 Lem-12 5 0.000964023 192.168.155.39 49.50.66.193 UDP 54 54638 + 80 Lem-12 7 0.000963007 192.168.155.39 49.50.66.193 UDP 54 55226 + 80 Lem-12 8 0.001095475 192.168.155.39 49.50.66.193 UDP 54 45483 + 80 Lem-12 9 0.00185464 192.168.155.39 49.50.66.193 UDP 54 45524 + 80 Lem-12 10 0.00105514 192.168.155.39 49.50.66.193 UDP 54 45524 + 80 Lem-12 11 0.001125222 192.168.155.39 49.50.66.193 UDP 54 45624 + 80 Lem-12 12 0.00114037 192.168.155.39 49.50.66.193 UDP 54 46524 + 80 Lem-12 13 0.00125214 192.168.155.39 49.50.66.193 UDP 54 46824 + 80 Lem-12 14 0.001125221 192.168.155.39 49.50.66.193 UDP 54 46824 + 80 Lem-12 15 0.001261561 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 46879 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56684 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56684 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56684 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56684 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.001261591 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884 + 80 Lem-12 15 0.002615910 192.168.155.39 49.50.66.193 UDP 54 56884		2 0.000015659	192.168.165.39	49.50.66.193	UDP	54 48879 → 80 Len=12	
4 0.000080479 192.168.155.39 49.50.66.193 UDP 54.5787 + 80 Lem-12 5 0.000904023 192.168.155.39 49.50.66.193 UDP 54.51083 + 80 Lem-12 6 0.000904023 192.168.155.39 49.50.66.193 UDP 54.36438 + 80 Lem-12 7 0.000905007 192.168.155.39 49.50.66.193 UDP 54.45433 + 80 Lem-12 8 0.001095475 192.168.155.39 49.50.66.193 UDP 54.45433 + 80 Lem-12 9 0.001095475 192.168.155.39 49.50.66.193 UDP 54.45634 + 80 Lem-12 10 0.00103514 192.168.155.39 49.50.66.193 UDP 54.46524 + 80 Lem-12 11 0.00112322 192.168.15.39 49.50.66.193 UDP 54.46504 + 80 Lem-12 12 0.001140937 192.168.15.39 49.50.66.193 UDP 54.46808 + 80 Lem-12 12 0.001140937 192.168.15.39 49.50.66.193 UDP 54.46807 + 80 Lem-12 13 0.001203216 192.168.15.39 49.50.66.193 UDP 54.46808 + 80 Lem-12 14 0.002051319 192.168.15.39 49.50.6	1	3 0.000064121	192.168.165.39	49.50.66.193	UDP	54 54458 → 80 Len=12	
5 0.000094023 192.168.155.39 49.50.66.193 UDP 54.51038 + 80 Lem-12 6 0.000024983 192.168.155.39 49.50.66.193 UDP 54.36438 + 80 Lem-12 7 0.000054983 192.168.155.39 49.50.66.193 UDP 54.55226 + 80 Lem-12 8 0.001065475 192.168.155.39 49.50.66.193 UDP 54.45634 + 60 Lem-12 9 0.00134464 192.168.155.39 49.50.66.193 UDP 54.46524 + 60 Lem-12 10 0.001053614 192.168.155.39 49.50.66.193 UDP 54.46808 + 60 Lem-12 11 0.001123232 192.168.155.39 49.50.66.193 UDP 54.46808 + 60 Lem-12 12 0.001140037 192.168.15.39 49.50.66.193 UDP 54.46808 + 60 Lem-12 12 0.001140037 192.168.15.39 49.50.66.193 UDP 54.46808 + 60 Lem-12 13 0.001203219 192.168.15.39 49.50.66.193 UDP 54.46808 + 60 Lem-12 14 0.002051919 192.168.15.39 49.50.66.193 UDP 54.56804 + 60 Lem-12 15 0.0020519219 192.168.15.39 49.		4 0.000880479	192.168.165.39	49.50.66.193	UDP	54 55787 → 80 Len=12	
6 0.000924983 192.168.155.39 49.50.66.193 UDP 54 36438 + 80 Lem-12 7 0.000963007 192.168.155.39 49.50.66.193 UDP 54 55226 + 80 Lem-12 8 0.00105475 192.168.155.39 49.50.66.193 UDP 54 45634 + 80 Lem-12 10 0.001053614 192.168.155.39 49.50.66.193 UDP 54 66808 + 80 Lem-12 11 0.00112322 192.168.155.39 49.50.66.193 UDP 54 56864 + 80 Lem-12 12 0.00114037 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 13 0.00125326 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 13 0.001263614 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 13 0.001263619 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 13 0.00126195 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 13 0.001261951 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615911 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002615912 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 586		5 0.000904023	192.168.165.39	49.50.66.193	UDP	54 51038 → 80 Len=12	
7 0.000063007 192.168.155.39 49.50.66.193 UDP 54.55226 + 80 Lem-12 8 0.00105475 192.168.155.39 49.50.66.193 UDP 54.45433 + 80 Lem-12 9 0.001053614 192.168.165.39 49.50.66.193 UDP 54.46524 + 80 Lem-12 10 0.001053614 192.168.165.39 49.50.66.193 UDP 54.66080 + 80 Lem-12 11 0.001123222 192.168.165.39 49.50.66.193 UDP 54.46824 + 80 Lem-12 12 0.001140377 192.168.165.39 49.50.66.193 UDP 54.48879 + 80 Lem-12 13 0.001261696 192.168.165.39 49.50.66.193 UDP 54.48879 + 80 Lem-12 14 0.002615911 192.168.165.39 49.50.66.193 UDP 54.5888 + 80 Lem-12 15 0.0022615911 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.0022615912 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.0022615912 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.0022615912 192.168.165.39	-	6 0.000924983	192.168.165.39	49.50.66.193	UDP	54 36438 → 80 Len=12	
8 0.001065475 192.168.155.39 49.50.66.193 UDP 54.45483 + 80 Lem-12 9 0.00105464 192.168.165.39 49.50.66.193 UDP 54.4524 + 80 Lem-12 10 0.001053614 192.168.165.39 49.50.66.193 UDP 54.68080 + 80 Lem-12 11 0.00112322 192.168.165.39 49.50.66.193 UDP 54.8864 + 80 Lem-12 12 0.00114037 192.168.165.39 49.50.66.193 UDP 54.48879 + 80 Lem-12 13 0.001261696 192.168.165.39 49.50.66.193 UDP 54.58684 + 80 Lem-12 13 0.001261696 192.168.165.39 49.50.66.193 UDP 54.58884 + 80 Lem-12 14 0.002619319 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.002655082 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.002655082 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12		7 0.000963007	192.168.165.39	49.50.66.193	UDP	54 55226 → 80 Len=12	
9 0.001834464 192.168.165.39 49.50.66.193 UDP 54 46524 + 80 Lem-12 10 0.001053614 192.168.165.39 49.50.66.193 UDP 54 60808 + 80 Lem-12 11 0.001123232 192.168.165.39 49.50.66.193 UDP 54 48679 + 80 Lem-12 12 0.001140837 192.168.165.39 49.50.66.193 UDP 54 48679 + 80 Lem-12 13 0.001201696 192.168.165.39 49.50.66.193 UDP 54 5458 + 80 Lem-12 14 0.002129319 192.168.155.39 49.50.66.193 UDP 54 68088 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 68088 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 68088 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 68088 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.65.193 UDP 54 58684 + 80 Lem-12 15 0.002655802 192.168.155.39 49.50.500 49.500 49.500 49.500 49.500 49.500 49.500 49.500 49.500 49.500 49.500 49.500		8 0.001005475	192.168.165.39	49.50.66.193	UDP	54 45483 → 80 Len=12	
10 0.001053614 192.168.165.39 49.50.66.193 UDP 54 60008 + 80 Lem-12 11 0.001123232 192.168.165.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 12 0.001140037 192.168.165.39 49.50.66.193 UDP 54 48879 + 80 Lem-12 13 0.001201696 192.168.165.39 49.50.66.193 UDP 54 5458 + 80 Lem-12 14 0.002619319 192.168.165.39 49.50.66.193 UDP 54 68088 + 80 Lem-12 15 0.002653802 192.168.165.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12 15 0.002653802 192.168.155.39 49.50.66.193 UDP 54 58684 + 80 Lem-12		9 0.001034464	192.168.165.39	49.50.66.193	UDP	54 46524 → 80 Len=12	
11 0.001123232 192.168.165.39 49.50.66.193 UDP 54.58684 + 80 Lem-12 12 0.001140037 192.168.165.39 49.50.66.193 UDP 54.48879 + 80 Lem-12 13 0.001201696 192.168.165.39 49.50.66.193 UDP 54.54458 + 80 Lem-12 14 0.002619319 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.002653802 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem-12 15 0.002653802 192.168.165.39 49.50.66.193 UDP 54.86884 + 80 Lem-12		10 0.001053614	192.168.165.39	49.50.66.193	UDP	54 60808 → 80 Len=12	
12 0.001140037 192.160.165.39 49.50.66.193 UDP 54.48879 + 80 Lem=12 13 0.001201696 192.168.165.39 49.50.66.193 UDP 54.54458 + 80 Lem=12 14 0.002619319 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem=12 15 0.002653082 192.168.165.39 49.50.66.193 UDP 54.68088 + 80 Lem=12 15 0.002653082 192.168.165.39 49.50.66.193 UDP 54.86884 + 80 Lem=12		11 0.001123232	192.168.165.39	49.50.66.193	UDP	54 58684 → 80 Len=12	
13 0.001201696 192.160.165.39 49.50.66.193 UDP 54 54458 + 80 Len=12 14 0.002619319 192.168.165.39 49.50.66.193 UDP 54 60008 + 80 Len=12 15 0.002653002 192.168.165.39 49.50.66.193 UDP 54 50684 + 80 Len=12		12 0.001140037	192.168.165.39	49.50.66.193	UDP	54 48879 → 80 Len=12	
14 0.002619319 192.160.165.39 49.50.66.193 UDP 54 60000 + 00 Len=12 15 0.0026553002 192.160.165.39 49.50.66.193 UDP 54 58684 + 00 Len=12		13 0.001201696	192.168.165.39	49.50.66.193	UDP	54 54458 + 80 Len=12	
15 0.002635002 192.168.165.39 49.50.66.193 UDP 54 58684 + 80 Len=12		14 0.002619319	192.168.165.39	49.50.66.193	UDP	54 60808 → 80 Len=12	
A constance of the second s		15 0.002635802	192.168.165.39	49.50.66.193	UDP	54 58684 → 80 Len=12	
7 rrame 1: 54 bytes on wire (452 bits), 54 bytes captured (452 bits) on interface etn0, 10 0	>	Frame 1: 54 bytes o	n wire (432 bits),	54 bytes captured (4	32 bits) on	n interface eth0, id 0	

> Ethernet II, Src: PcsCompu_04:6b:89 (08:00:27:04:6b:89), Dst: 9a:b2:6a:cf:a7:59 (9a:b2:6a:cf:a7:59)

> Internet Protocol Version 4, Src: 192.168.165.39, Dst: 49.50.66.193

> User Datagram Protocol, Src Port: 58684, Dst Port: 80

> Data (12 bytes)

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.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VII July 2022- Available at www.ijraset.com

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).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538

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

- [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.

45.98

IMPACT FACTOR: 7.129

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 🕓 (24*7 Support on Whatsapp)