Bulletin of Electrical Engineering and Informatics
Vol. 11, No. 4, August 2022, pp. 2280~2291
ISSN: 2302-9285, DOI: 10.11591/eei.v11i4.3810

Provably curb man-in-the-middle attack-based ARP spoofing in a local network

Hiba Imad Nasser, Mohammed Abdulridha Hussain
Department of Computer Science, College of Education for Pure Science, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Mar 14, 2022
Revised May 9, 2022
Accepted Jun 20, 2022

Keywords:

ARP poisoning
ARP spoofing
MITM
MITM sniffing
Network security

ABSTRACT

Even today, internet users" data security remains a significant concern. One problem is ARP poisoning, otherwise referred to as ARP spoofing. Such attacks are intended to exploit the identified ARP protocol vulnerability. Despite no straightforward remedy for ARP spoofing being apparent, certain actions may be taken to maintain one"s safety. The most basic and common defence against a poisoning attack is manually adding MAC and IP addresses to the static ARP cache table. However, this solution is ineffective for large networks where static entries require considerable time and effort to maintain, whether by human input or via special tools and settings for the static entries of network devices. Accordingly, this paper aimed to monitor network packet information and detect the behaviour of ARP poison attacks on operating systems, for instance Windows and Linux. The discovery and defence policy systematically and periodically check the MAC addresses in the ARP table, enabling alerts to be issued if a duplicate entry is detected. This enables the poison-IP address to be blocked before a reply is sent. Finally, the results showed that the superiority was successfully achieved in the detection, prevention and reporting mechanisms in the real-world environment.

Corresponding Author:

Hiba Imad Nasser
Department of Computer Science, College of Education for Pure Science, University of Basrah
Basrah, Iraq
E-mail: eduppg.hiba.amad@uobasrah.edu.iq

1. INTRODUCTION

The Internet has emerged as a fundamental aspect of daily life. By January 2022, the numbed of Internet users amounted to 4.88 billion internationally, equating to almost 62% of the global population. This number continues to grow, with almost 257 million new Internet users being added last year; over 700,000 unique users are added daily [1]. The majority of people use it for communication and information exchange. Therefore, security is deemed a foremost threat to computer networks and their applications, requiring action to be initiated in order to safeguard networks and services against illegal activity [2]. Through such malicious attacks, computer systems and technology-dependent businesses are targeted. These assaults primarily involve the computer code twitch, the modification or deletion of data on computer systems, as well as other forms of illegal access. The most prevalent of these types of attacks are cyber-attacks, Man-in-the-middle (MITM), social engineering, replay, as well as denial of service (DoS) attacks. An MITM attack is a cyber-attack through which the attacker intercepts a two-party conversation, mirrors both parties and has access to information provided by both parties [3]. Whenever an MITM attack occurs, a malicious client places his computer in the path of two communicators" transmissions. The use of a packet sniffer afterwards enforces sniffing. To ensure that the communication appears unbroken, the unethical client"s computer passes traffic between the unsuspecting clients, as presented in Figure 1.