Detecting ARP Spoofing on Wireless Networks Using the StringMatching Method with the Boyer Moore Algorithm and Brute Force

Syafrullah Anwar[1], Siti Amatullah Karimah[2], Erwid Musthofa Jadied[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]syafrullah@students.telkomuniversity.ac.id, [2]pembimbing1@telkomuniversity.ac.id,
[3]pembimbing2@telkomuniversity.ac.id

Abstract

Address Resolution Protocol (ARP) is a protocol used to translate Internet Protocol (IP) addresses into Media Access addresses Protocol (MAC) on a network. An ARP request broadcast for get the MAC address of the destination device which is useful for communication between devices. When the host receives the address of the ARP request that addressed to it, the receiving device will send an ARP reply packet to the sending device. The ARP protocol has a significant security vulnerability make these security holes can be attacked by spoofing. ARP spoofing is an attack that sends a fake ARP that has been modified to poison the victim's ARP cache table, this attack supports the occurrence of attacks other computer networks such as denial of service (DoS) attacks, Man in the Middle Attack, and others. In this study, detection of ARP spoofing was carried out by looking for a MAC Address that has been changed by the Attacker using string matching with Boyer Moore algorithm and brute force.

Keywords: ARP, ARP Spoofing, String Matching, Boyer Moore, Brute Force