International Review on Computers and Software, vol. 8(11), 2013, pages 2624-2627

Propose approach for UDP random and sequential scanning detection based on the connection failure messages

Abstract

Network scanning usually lunched by attackers for exploring and gathering information about the target network, this information may includes the network topology and services running on the network, based on the gathered information the attacker will put his attack plan to gain access to the target network. Attackers sometimes scan the target network with none previous knowledge concerning the active service or host in the target network which will generate a high ratio of connection failure message which come in form of ICMP type 3 code 3 packets (port unreachable) and ICMP type 3 code 1 packets (host unreachable). This paper will propose approach for random and sequential type of UDP scanning detection based on the connection failures messages.

Keywords

Connection failure; Network scanning; UDP random scanning; UDP sequential scanning