ABSTRACT

Method for detecting unauthorized port scanning in a computer network, associated computer program product and device

The network is made up of a plurality of terminals each defining a plurality of ports, each terminal being associated with a port identifier. At least some of the terminals, called initiating terminals, are able to initiate a connection with another terminal, called receiving terminal, via at least one port of this receiving terminal.

The method (100) comprises the following steps:

- detection (110) of each connection initiated by an initiating terminal;
- identifying (120) connections among all of the initiated connections;
- for each rejected connection, generating (130) security information comprising the identifiers of the receiving terminal and one of its ports, and adding (140) security information in a shared database;
- analyzing (150) the database to determine unauthorized port scans.

Figure 5