CLAIMS

1.- A method (100) for detecting unauthorized port scanning in a computer network (10) in particular to avoid a computer attack, the computer network (10) being made up of a plurality of communication terminals (11, 12A,..,12E) each defining a plurality of communication ports (P_1,..,P_3) and able to communicate with one another via these communication ports (P_1,..,P_3), each terminal (11, 12A,..,12E) being associated with a unique terminal identifier (ID_1) in the network (10), each port (P_1,..,P_3) being associated with a unique port identifier (ID_2) within the corresponding terminal (11, 12A,..,12E),

at least some of the terminals (11, 12A,..,12E), called initiating terminals, being able to initiate a computer connection with at least one other terminal (11, 12A,..,12E), called receiving terminal, via at least one port (P_1,..,P_3) of the receiving terminal (11, 12A,..,12E), each receiving terminal (11, 12A,..,12E) being able to reject a connection initiated by an initiating terminal (11, 12A,..,12E),

the method (100) being implemented by terminals (12B,..,12E) forming an identified group of terminals and including the following steps:

- detection (110), by each receiving terminal (12B,..,12E) in the group, of each connection initiated by an initiating terminal (11, 12A,..,12E) via at least one port (P_1,..,P_3) of that receiving terminal (12B,..,12E);

- identification (120), by each receiving terminal (12B,..,12E) of the group, of rejected connections among all of the initiated connections;

- for each rejected connection, generating (130) security information (I) comprising a first datum (D_1) and a second datum (D_2) respectively corresponding to the identifiers (ID_1, ID_2) of the receiving terminal (12B,..,12E) and one of its ports (P_1,..,P_3) corresponding to this rejected connection, and adding (140) the generated security information (I) in a security database (BI) shared between the terminals (12B,..,12E) in the group; and

- analyzing (150) the shared security information database (BI) to determine unauthorized port scans,

wherein each terminal (12A,…,12E) of the group further includes a storage unit (24) able to store at least part of the security information database (BI).

2.- The method (100) according to claim 1, wherein each rejected connection corresponds to an initiated connection toward a closed port (P_1,..,P_3) or toward a port (P_1,..,P_3) comprising a filter refusing the connection with the corresponding initiating terminal (11, 12A,..,12E).

3.- The method (100) according to claim 1 or 2, wherein the security information database (BI) is shared in the group using so-called "peer-to-peer" (P2P) type technology.

4.- The method (100) according to any one of the preceding claims, wherein the security information database (BI) comprises a correspondence graph (G) whose nodes are provided by the first data (D_1) and the second data (D_2) from each added item of security information (I).

5.- The method (100) according to claim 4, wherein each added item of security information (I) corresponds to an edge (51,..,54) between two nodes formed by the first datum (D_1) and the second datum (D_2) coming from the security information (I), a set of nodes connected via one or more edges (C_1, C_2, 61, 62) forming a connected component of the correspondence graph (G).

6.- The method (100) according to claim 5, wherein the addition of an item of security information (I) comprises the following sub-steps:

- creating (142) a new node formed by the first datum (D_1) of this security information item (I) if such a node does not exist in the correspondence graph (G);
- creating (144) a new node formed by the second datum (D_2) of this security information item (I) if such a node does not exist in the correspondence graph (G);
- identifying (145) a first connector component (C_1) of the correspondence graph (G) containing a node formed by the first datum (D_1);
- identifying (146) a second connector component (C_2) of the correspondence graph (G) containing a node formed by the second datum (D_2);
- if the first component (C_1) and the second connected component (C_2) are different, merging (148) the first connected component (C_1) with the second connected component (C_2) by creating an edge (A) between the nodes formed by the first datum (D_1) and the second datum (D_2).

7.- The method (100) according to claim 5 or 6, wherein the analysis of the security information database (BI) comprises determining the number of nodes of at least one connector component of the correspondence graph (G).

8.- The method (100) according to claim 6 and 7, wherein the at least one connector component for which the number of nodes is determined corresponds to a

component obtained after merging the first connected component (C_1) and the second connected component (C_2).

9.- The method (100) according to claim 7 or 8, wherein port scanning is determined when the number of identified nodes exceeds a predetermined threshold.

10.- The method (100) according to any one of the preceding claims, wherein each security information item (I) further comprises the identifier (ID_1) of the initiating terminal (11, 12A,..,12E) having initiated the rejected connection corresponding to the security information (I).

11.- The method (100) according to any one of the preceding claims, wherein the security information database (BI) further comprises the number of occurrences of each security information item (I) in that database (BI).

12.- The method (100) according to any one of the preceding claims, further comprising a step (160) for updating the security information database (BI) in particular making it possible to erase the oldest security information (I) contained in that database.

13.- A computer program product comprising software instructions which, when implemented by a computer, carry out the method according to any one of the preceding claims.

14.- An analysis device (40B,..,40E) for detecting unauthorized port scanning in a computer network (10) in particular to avoid a computer attack, the computer network (10) being made up of a plurality of communication terminals (11, 12A,..,12E) each defining a plurality of communication ports (P_1,..,P_3) and able to communicate with one another via these communication ports (P_1,..,P_3), each terminal (11, 12A,..,12E) being associated with a unique terminal identifier (ID_1) in the network (10), each port (P_1,..,P_3) being associated with a unique port identifier (ID_2) within the corresponding terminal (11, 12A,..,12E),

at least some of the terminals (11, 12A,..,12E), called initiating terminals, being able to initiate a computer connection with at least one other terminal (11, 12A,..,12E), called receiving terminal, via at least one port (P_1,..,P_3) of the receiving terminal (11, 12A,..,12E), each receiving terminal (11, 12A,..,12E) being able to reject a connection initiated by an initiating terminal (11, 12A,..,12E),

the analysis device (40B,..,40E) being able to:

- detect each connection initiated by an initiating terminal (11, 12A,..,12E) via at least one port (P_1,..,P_3) of that receiving terminal (12B,..,12E);

- identifying connections among all of the initiated connections;

- for each rejected connection, generating security information (I) comprising a first datum (D_1) and a second datum (D_2) respectively corresponding to the identifiers (ID_1, ID_2) of the receiving terminal (12B,..,12E) and one of its ports (P_1,..,P_3) corresponding to this rejected connection, and adding the generated security information (I) in a shared security database (BI); and

- analyzing the shared security information database (BI) to determine unauthorized port scans.