What is a backdoor?

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected, the backdoor may take the form of an installed program, or could be a modification to an existing program or hardware device. It hides in the computer, scans existing loopholes, opens corresponding ports, as well as modifies system registration files.

Backdoor will not duplicate or actively spread itself. It will only open a certain port through which a remote computer in the network can control the infected computer. Generally the backdoor will not influence normal communication of the network, so firewalls or IDS can hardly detect its existence.

Is my network infected with a backdoor?

According to statistics, most of the backdoors work under port 31337, 31335, 27444, 27665, 20034, 9704, 6063, 5999, 5910, 5432, 2049, 1433, 444, and 137-139. So whether there is communication through these ports in the network determines whether the network is infected with a backdoor.

Note: we are not able to list all the ports since the backdoor develops so fast. If you find other ports, just add them in the monitoring list.

Let's check whether there is a host infected with backdoor in the network by using Colasoft Capsa to monitor those ports.

Step 1. Open the Filter dialog box, click the Add button.
Step 2. Input the settings as the figure below and set the multiple ports value as"31337,31335, 27444,27665,20034,9704
".

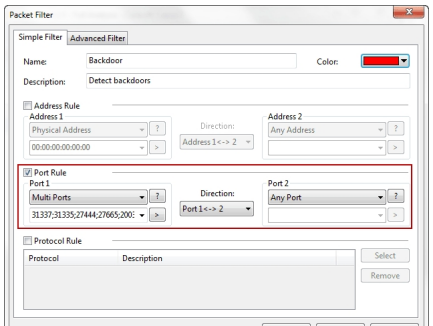

Figure 8 Backdoor Filter Condition

Click the Filter window, check Accept box to enable the filter (figure 9). Then, any packet of the backdoor Colasoft Capsa, it indicates the network

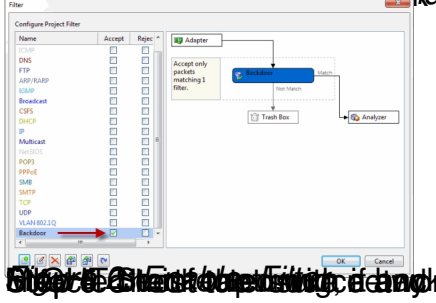

Figure 9 Backdoor Filter Accept