Andrey Groshenkov
A.A. Baranov, research supervisor
M.L. Isakova, language adviser
SHEI “National Mining University”, Dnipropetrovsk

The Problem of Sniffing and Ways to Fight it

Sniffing is the interception of packets, that is transmitted between two computers. Interception can take place at any point in the data path. In a LAN, the interceptor can be at any node in the network, in the Internet - provider. In networks that are based on TCP / IP, all information is transmitted in an open type (even sensitive data - passwords and user names). Therefore, it is very advantageous customize software on the same machine, which will see all the packets on the network, and check them for some passwords. This is sniffing. And such software is called a sniffer.

The biggest threat of sniffing consists in interception passwords that are often used in protocols - Telnet, FTP, POP3, HTTP, which transmit information about the password in the network openly. With sniffing any data can be intercepted, even files sent over the network attached to any letter.

The popular packet sniffer for Linux is the Ethereal. This program has a user friendly graphical interface, which allows you to browse a list of all the captured packets, and separately the contents of each package. Ethereal has a version for Windows.

The following approach will help you avoid the majority of sniffers:

- the use of switches in the network reduces the chance of successful use of sniffer. In the case of operation of a network with switches, packets are delivered directly to the addressee and unavailable to all hosts - this reduces the possibility of their capture. And network administrators to easily determine the presence of packet sniffers, consider the network segments separately;
- IPSec encryption technology can be used to defend the packets transmitted in the network infrastructure, in the case of exchange of confidential data. IPSec to encrypt the data and supported by modern routers, firewalls and other network components. Almost the all operating systems support IPSec and this technology is widely used in the important IT-infrastructure. For the protection level of sessions traffic encryption SSL and TLS can be used;
- disabling promiscous-mode on network interfaces accidentally to disconnect most sniffers. This action can be automated by creating a custom script and adding it as a task to "cron" for using every day, or controlled by creation Access Policy to the settings of network Card at the host level.

Free operating systems do not have inbuilt mechanisms of protection from sniffers, which is a serious problem in the networks.