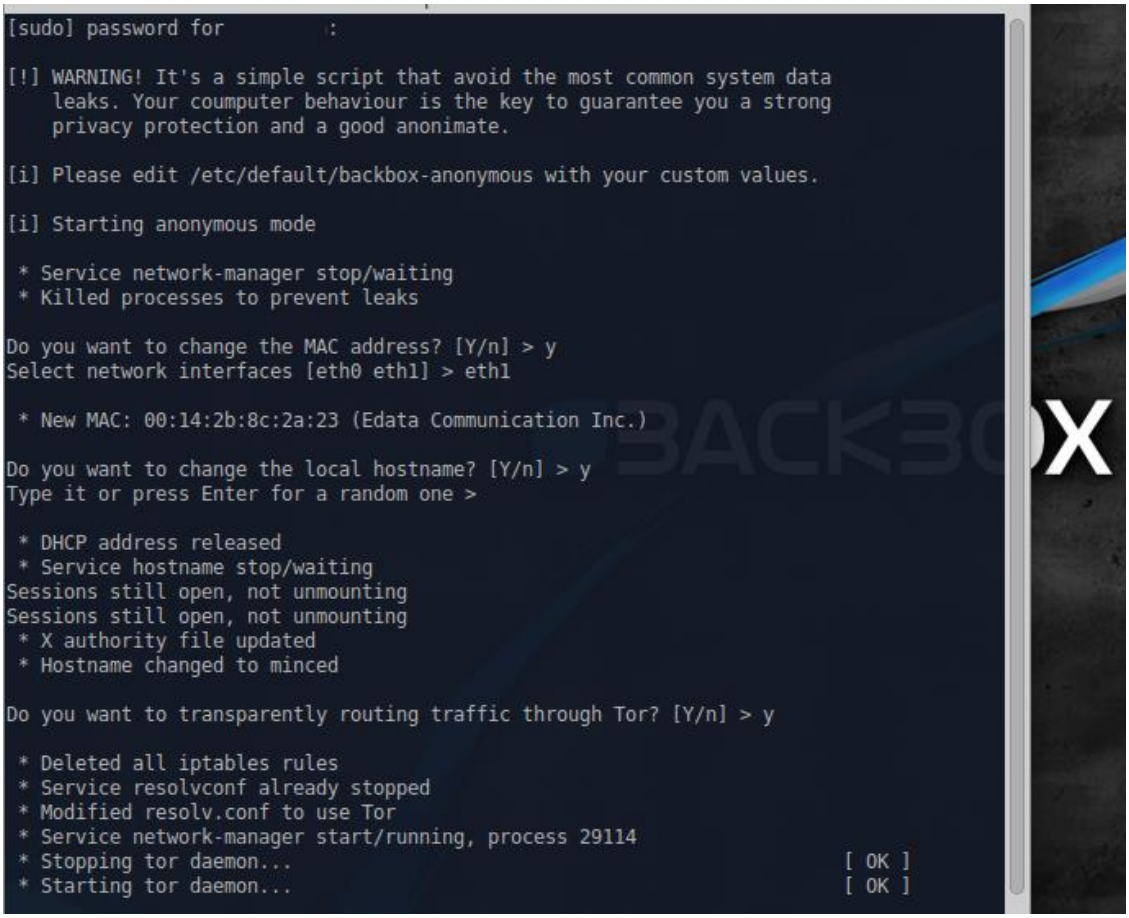
System for secure communication via USB

The project of secure communication via USB is the result of a long-term research on the protection of personal privacy and communication over the Internet. The goal of the project is to completely protect user communications, change its identity, hide (encrypt) all of its activities on the Internet, and prevent anybody from gaining insight into the content of the Internet. In other words, the user on USB has everything it needs for secure communication, and if this device falls into the wrong hands, there is no possibility of unauthorized access.

Namely, this is the complete installation of Backbox Linux distribution on USB memory inside the LUKS encrypted container. The operating system that is on USB can be picked up from almost any desktop or laptop. Although any Linux distribution can be used for this purpose, Backbox has proved to be the best choice since it already has almost all the necessary security scripts and programs.

Backbox is a specialized distribution for penetration testing, or simply to check the security of computer systems, i.e. hacking (Figure 6.1). It contains the necessary tools for all possible types of hacking and it has built-in Anonymous mode, as well as the RAM wiping memory option when shutting down the system. More precisely, by typing Anonymous mode, the user has the ability to change the MAC address (physical address of the network card), public IP addresses and hostname, so that every new start of this mode enters a complete change of user identity. Anonymous script completes the complete Internet traffic of the operating system to the popular Tor network and thus changes the IP address of the user and encapsulates all of its activities on the Internet. By turning off Anonymous mode, in addition to restoring data to the previous state, the complete deletion of all data from the system will occur, which could compromise users with later analysis.

Picture 1. Backbox



Picture 2. RAM wiping script

The RAM wiping script (Figure 6.2) completely cleans the RAM memory so that there is no possibility for digital forensics to access any data. Backbox (like most Linux distributions) offers the ability to fully encrypt an operating system when it is installed, which is very useful because it prevents unauthorized access and insight into what is on the hard disk or partition on which the system is installed. In our case, it's about USB memory. Encryption is strong enough that it's almost impossible to unlock the partition and lift the operating system without a code.

In case of danger, it is enough for a few seconds for the USB to be pulled out of the computer, hide it somewhere or throw it out of the window. Installing on USB allows the user to change the physical location and lift its operating system from any computer available to it.