The goal of the work is to design and implement a honeypot (a trap for attackers) that will be able to simulate working user and other usual system activity in a convincing way so as to make it difficult to distinguish a honeypot from an ordinary system, will keep a stealth record of actions of any attackers who would attack the honeypot, and will make it possible to deploy a whole virtual network of honeypots (a honeynet) on a single host machine. The implementation should be resistant to any of the well-known techniques used to detect a modified operating system or OS kernel such as the kstat utility.