Cílem práce je navrhnout a implementovat “honeypot” (past na útočníky), který bude umět simulovat uživatelskou a jinou obvyklou systémovou aktivitu dostatečně přesvedčivým způsobem tak, aby ztížil rozpoznání honeypotu od obyčejného systému. Bude také vést skryté záznamy o akcích útočníků, kteří honeypot napadnou. Bude umožňovat sestavit celou virtuální sít těchto honeypotů (tzv. honeynet) na jednom fyzickém stroji. Implementace by měla být odolná vůči známým technikám používaným k detekci modifikovaného operačního systému nebo jeho jádra jako to delá např. utilita kstat.