Oponentský posudek diplomové práce Tomáše Kouby

Virtual honeynet with simulated user activity

Diplomová práce si klade za cíl navržení a implementaci „honeynetu", (virtuální) sítě simulující dostatečně přesvědčivým způsobem uživatelskou i systémovou aktivitu a tvářící se tak jako produkční virtuální síť. V případě napadení této sítě útočníkem by mělo být možné sledovat jeho chování, a to pokud možno takovým způsobem, aby toto sledování nebylo odhaleno.

Práce je členěna do několika logických celků. V první části (kapitoly 1 a 2) autor nastiňuje cíle práce a zabývá se rozborem přístupů k tvorbě honeynetů, současnými řešeními a jejich problémy. Kapitola 3 pojednává o možnostech skrývání rootkitů na straně jedné a nástrojů pro monitoring útočníka na straně druhé. Kapitola 4 rozebírá možnosti virtualizace. V 5. kapitole je pak popsána instalace virtuální sítě, popsán způsob simulace uživatelské a systémové aktivity a rozebrána knihovna pro monitoring útočníka.

Hlavním přínosem práce je rozšíření knihovny VAcesss Bryana D. Payna o možnost monitoringu uživatelské oblasti paměti, rozšíření monitoringu paměti jádra a odchytávání systémových volání read() a write(), které případný útočník zavolá. Tento monitoring je řešen tak, aby byl z pohledu útočníka nepozorovatelný. Ke knihovně je naprogramováno uživatelské rozhraní, které však nepodporuje veškerou funkcionalitu knihovny. Knihovna je psána pouze pro linux, nicméně jsou podporovány (po rekompilaci) různé verze jádra.

Simulace uživatelské aktivity se ukázala jako poměrně složitý úkol, který by pravděpodobně vydal na vlastní diplomovou práci, nicméně pro dosažení ilustrace problému je dostačující.

Práce je napsána v anglickém jazyce. Jazyková úroveň práce je nadprůměrná.

Mé otázky a připomínky pro Tomáše Koubu:

- Proč bylo použito zrovna virtualizační prostředí Xen a ne jiná paravirtualizační (viz sekce 4.1.3) prostředí
- Je možné zautomatizovat některé úlohy typu: „Porovnej seznam běžících procesu (získaný např. příkazem „top"), seznam procesů, které mají stopu v adresáři „/proc" a seznam procesů, které jsou fyzicky v paměti jádra, ve spojovém seznamu procesů a vypiš mi zákeřné procesy (rootkity), které jsou ve spojovém seznamu procesů, ale už se například nevypíšou příkazem „top"? Případně, co by bylo potřeba udělat, aby to bylo možné?
- Byla daná virtuální síť nasazena v praxi a podařilo se chytit nějakého útočníka/robota?

Práce se ukázala býti velmi náročnou, některé části a myšlenky bohužel nebyly plně doimplementovány. Přesto však práce Tomáše Kouby splňuje zadání, vede k zajímavým zjištěním a k praktickému rozšíření knihovny VAccess, proto ji **doporučuji uznat** jako práci diplomovou.

V Praze, 21. 1. 2009

Mgr. Tomáš Knap
Oponent diplomové práce