Posudek diplomové práce

Tomáš Kouba

Virtual honeynet with simulated user activity

Posuzovaná práce má za cíl navrhnout a vytvořit tzv. honeynet, tj. síť počítačů tzv. honeypotů, které budou sloužit jako pasti zachycující útoky zvenčí zejména pro účely jejich výzkumu. Tento honeynet by měl být tvořen virtuálními počítači, což dovolí simulovat celou síť na jediném fyzickém počítači, měl by být schopen skrytě a bezpečně sledovat a zaznamenávat aktivity útočníků a měl by obsahovat mechanismy pro simulaci aktivity reálných uživatelů.

Práci je možno rozdělit do tří hlavních bloků:

První blok zahrnuje první až třetí kapitolu a obsahuje úvod do problematiky honeypotů a honeynetů, stručný popis existujícího systému Sebek a diskusi jeho slabých míst a v třetí kapitole poměrně obšírný a ilustrativní popis metod používaných útočníky pro ukrytí jejich přítomnosti a aktivit v napadeném systému a pro ochranu jejich know-how proti případné forenzní analýze a také způsobů, jak tyto metody překonat. Uvedeny a diskutovány jsou i konkrétní existující nástroje na straně útočníků i obránců. Výsledkem, byť možná nepříliš explicitně artikulovaným, této části jsou požadavky na základní funkce, které by měl honeynet implementovat.

Druhý blok zahrnující čtvrtou kapitolu se velmi detailně věnuje problematice virtualizace. Popsány jsou různé přístupy k virtualizaci, technické obtíže vznikající na architektuře x86 (možná až příliš detailně) a reprezentativní vzorek existujících řešení včetně diskuse jejich výhod a nevýhod (byť aktuálnost některých informací poněkud utrpěla dlouhou dobou, po kterou byla práce vytvářena). Připojeno je porovnání výkonnosti jednotlivých řešení, které má však v kontextu práce význam spíše jen orientační. Výsledkem této části je rozhodnutí použít virtualizační systém Xen a poznatek, že jeho snadná detekovatelnost nemusí být na závadu pro zamýšlené použití.

Třetí blok zahrnující pátou kapitolu tvoří vlastní těžiště práce, neboť se zabývá konstrukcí vlastního honeynetu. Nejprve je uvedena zamýšlená topologie virtuální sítě a stručně popsána instalace a konfigurace jednotlivých uzlů, dále je opět jen krátce vysvětlen mechanismus simulace uživatelské aktivity a konečně detailněji mechanismus monitorování virtuálních počítačů, který dovoluje mj. zjišťovat seznam jaderných modulů a běžících procesů (a to i v případě, že byly využity metody pro jejich ukrytí popsané ve třetí kapitole) a také sledovat komunikaci mezi procesy uvnitř virtuálního stroje, což je funkce poměrně neobvyklá, ale pro zamýšlený účel velmi užitečná. Slabým místem této části je až přílišná stručnost zejména v porovnání s předchozím textem (konkrétně chybí detailnější popis toho, jakým způsobem honeypot zprovoznit a používat) a také absence propojení vytvořených komponent s nějakým sofistikovanějším systémem pro sběr dat a jejich analýzu.

Vlastní softwarové dílo (nebo spíš díla) na přiloženém CD působí poněkud neuspořádaným dojmem a sestavení jednotlivých komponent do funkčního celku je sice proveditelný ale poměrně náročný úkol a to zejména (jak již bylo

výše naznačeno) kvůli tomu, že v práci není dostatečně úplně a detailně uveden správný postup a požadované prostředí (Xen, knihovny, vývojové nástroje apod.). Část vytvořeného kódu (knihovna VAccess) je založena na již existujícím díle, nicméně podíl diplomantova příspěvku lze považovat za dostatečně významný.

K práci je připojeno několik příloh zabývajících se tématy, která vybočují ze základní linie práce.

Práce je napsána v anglickém jazyce. Jazyková stránka není zcela dokonalá, ale text je celkově dostatečně srozumitelný. Estetickou úroveň práce lze hodnotit jako dobrou.

Domnívám se, že práce i navzdory všem uvedeným výhradám v zásadě splnila cíle stanovené v zadání, a doporučuji, aby byla uznána jako práce diplomová.

V Praze, 27. 1. 2009