Posudek oponenta diplomové práce

Autor/autorka práce: **Miroslav Marek**

Název práce: **Zvýšení bezpečnosti Linuxu**

Obsah práce

Cílem práce je prostudovat a porovnat existující rozšíření Linuxu, jejichž cílem je zvýšení bezpečnosti tohoto operačního systému. Na základě nastudovaných vlastností dostupných řešení má být provedena analýza dopadu na provoz počítačových systémů na ZČU a mají být vyspecifikována doporučení vedoucí k zvýšení zabezpečení počítačových systémů ZČU.

V úvodních teoretických kapitolách jsou detailně představeny jednotlivé technologie, pojmy a postupy, které jsou následně použity v praktické části. Tyto kapitoly 1 až 8 jsou velice detailně propracované a poskytují ucelený pohled na řešenou problematiku, včetně popisu existujících hrozeb a dostupných systémů, které tyto hrozby umožňují řešit. Zde bych měl jen drobnou výtku k pořadí kapitol, kde logicky by kapitola 8, která popisuje jednotlivé hrozby, měla předcházet kapitole 7, kde jsou porovnány vlastnosti dustupných řešení, neboť toto srovnání je provedeno bez zohlednění možnosti eliminovat konkrétní hrozby.

Z dostupných řešení autor vybral na základě srovnání jako nejvýhodnější systém Grsecurity, jehož vlastnosti a možnosti jsou detailně popsány v kapitole 9. Stejně jako předchozí kapitoly 1 až 8 je i tato část práce přehledná a detailně zpracovaná.

V kapitole 10 je popsáno porovnání zabezpečení systému Linux oproti zabezpečení s pomocí Grsecurity patche či dalších alternativních řešení. Tato kapitola by spíše měla být spojena s kapitolou 7, kde jsou porovnána všechna dostupná řešení zvyšující zabezpečení operačního systému Linux.

Kapitoly 11 až 14 se věnují testování dopadů rozšířeného zabezpečení na výkonnost systému, což je správně, ale prezentace výsledků není příliš vypovídající. Především kapitola 13 obsahuje velké množství tabulek a grafů, které ale často, jako například grafy na obrázcích 13.26, 13.28, 14.2, 14.13 a další, nedávají defakto žádnou informaci a bylo by postačující a přehlednější pouze okomentovat tabulku hodnot. Stejně tak úvodní text kapitoly 14.2 je velice fádní až nesprávný, neboť volně přeloženo říká: „Volby, které nemají negativní dopad na výkon zapněte, volby, které mají negativní dopad na výkon nezapínejte, ale prostudujte". Toto obecné doporučení pak autor alespoň trochu konkretizuje v tabulce 14.2, kde pro 18 vybraných nastavení uvádí doporučení pro pět možných typů nasazení operačního systému Linux, která jsou uvedena v tabulce 14.1. Bohužel není uvedeno, jak tato tabulka 14.1 vznikla a proč v ní chybějí typy serverů, jako je například Kerberos server či OpenAFS, které jsou z hlediska zabezpečení systému ZČU jistě klíčové.

V poslední kapitole – Závěr - jsou všechna zjištění shrnuta a zopakována a autor zde také uvádí skutečnost, že vybraný systém Grsecurity se v průběhu realizace stal z volně dostupného placeným řešením.

Kvalita řešení a dosažených výsledků

Celá teoretická část je velice kvalitně zpracována. V praktické části práce vidím nedostatky především v rámci třetího bodu zadání a tím je dopad navrhovaných řešení na provoz v prostředí ZČU. Toto prostředí není v práci nijak popsáno. Patrně nejblíže k tomuto popisu má tabulka 14.1, ve které jsou

popsáná možná nasazení operačního systému Linux a autorova doporučení ohledně použití jednotlivých voleb zabezpečení. Ale vazba na ZČU zde specifikována není. Očekával bych zde doporučení pro servery, na kterých mohou být provozovány systémy jako je Kerberos nebo OpenAFS či virtualizační server. Především v případě virtualizačních či virtualizovaných serverů autor v závěru zmiňuje, že s aplikací svých nastavení na tyto systémy měl problém, ale už nezmiňuje, jak u těchto systémů postupovat. Při stanovení míry vhodnosti zabezpečení je jistě vhodné změřit dopad nastavení na výkon celého systému, ale zároveň by měla být stanovena míra nebezpečí zneužití jednotlivých hrozeb a výsledná doporučení by měla být stanovena jako kombinace přínosu v zabezpečení oproti snížení výkonu. Autor se v práci bohuzel soustředil jen na zjišťování dopadu na výkon systému, což je s ohlednem na propracovanost teoretických kapitol a nadstandartní rozsah práce jistě škoda.

Formální úroveň

Rozsah práce se svými 222 stranami textu je výrazně nadstandartní. I přes tento rozsah se v textu vyskytuje jen malé množství chyb a překlepů. Záhadou pro mě však zůstává systém poznámek pod čarou a to jak z hlediska jejich číslování, neboť například na staně 105 chybí poznámky 1 a 3, tak z hlediska odkazování samotného, kde na straně 107 je odkazována poznámka 10, která na této straně není uvedena, ale zas je zde pod čarou uvedena poznámka 11, která však není odkazována. Dalším drobným nedostatkem je rozložení textu, obrázků a výpisů kódu, kde například na straně 45 jsou ukázky příkazů nesmyslně roztažené přes celou jinak prázdnou stránku. Drobnou výhradu bych měl k jazyku práce, který je často výrazně volnější než by se na technickou práci slušelo. Dále by bylo vhodné pro technickou práci volit jednotné označování, neboť někde je Grsecurity označována jako patch, jinde jako záplata.

Práce s literaturou

Práci s literaturou hodnotím kladně. V práci je použito více jak 60 odkazů na literaturu. Nemalá část těchto zdrojů jsou webové stránky, ale to je s ohledem na obsah a nutnost aktuálnosti této práce pochopitelné.

Splnění zadání

Zadání bylo splněno v plném rozsahu.

Dotazy k práci

1. V závěru práce je zmíněno, že do užšího výběru se dostaly systémy SELinux, AppArmor a Grsecurity. Z jakých všech systému tedy bylo vybíráno, neboť další už v práci zmíněny ani okrajově nejsou.

2. Proč nejsou v práci uvedeny doporučení pro systémy Kerberos, OpenAFS či virtualizační platformy jako XEN či KVM, když se z hlediska bezpečnosti zcela jistě jedná o citlivé systémy?

3. Na základě jakého ohodnocení - porovnání dopadu na bezpečnost ku dopadu na výkon byla zvolena jednotlivá doporučení?

Navrhuji hodnocení známkou **výborně** a práci doporučuji k obhajobě.

V Plzni 30.8.2017

Ing. Luboš Matějka

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky