Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Petr Klejch
Oponent práce: Ing. Tomáš Zahradnický, Ph.D.
Název práce: Kryptograficky bezpečné metody port knocking a single packet authorization
Obor: Počítačové systémy a sítě

Datum vytvoření: 6. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání diplomové práce považuji za náročnější vzhledem k tomu, že zadání požaduje kryptograficky bezpečný návrh klepání na porty. Důkladný návrh je obtížný vzhledem k tomu, že vyžaduje pochopení mnoha principů a jejich následnou integraci.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Konstatuji, že zadání práce bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Práce svým rozsahem převyšuje požadavky na diplomovou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*75 (C)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Faktická úroveň práce je vpořádku. Úroveň detailů a bohatost informací je vpořádku až na výjimky dole.

Logická úroveň práce je velmi dobrá. Kapitole 1 - Analýza - chybí závěr, který je de-facto na začátku kapitoly 2 - Návrh v sekci Vyhodnocení analýzy.

Jako nedostatek vidím de-facto žádnou analýzu toho, proč dochází ke zpoždění v zápisu firewall logu na Windows. Práce jen konstatuje, že bylo zaznamenáno zpoždění, analýzu příčiny a možností jejího řešení nenacházím.

Další nedostatek spatřuji v tom, že je používána služba na OS Windows a pojmenovaná roura pro interprocesovou komunikaci. Vůbec není řešeno zabezpečení služby a roury. Práce měla pro tento účel obsahovat diskuzi o tom, s jakým uživatelským účtem bude služba běžet, jak se služba zbaví nepotřebných práv a security ID ze svého bezpečnostního tokenu, a dále jaká budou přístupová práva k pojmenované rouře.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*75 (C)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Formální úroveň práce by mohla být také lepší. Nacházím nekonzistence například v psaní názvů operačních systémů - jako příklad uvádím "Mac OS" na straně 14, zatímco strana 28 uvádí "MacOS X", přičemž správně je macOS. Strana 7 nazývá paket segmentem. Prezentační vrstvě ISO/OSI modelu se na str. 3 říká prezenční vrstva (pravděpodobně jde o překlep). Jednou se píše $HOME/.cesta, podruhé /home/<uživatel>/cesta.

Typografická úroveň práce by mohla být lepší. Nacházím občas vytékající slova ze zrcadla stránky (např. str. 17, 18, ...).

Jazyková úroveň by také mohla být lepší. Práce obsahuje mnoho anglicizmů typu "útoků typu buffer overflow".

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*95 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Práce obsahuje 63 zdrojů rozmanitého charakteru. Mohly by být řazeny podle jména autora, nikoliv podle výskytu v práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*85 (B)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Návrh schémata pro autorizační paket hodnotím jako pečlivé. Student si dal tu práci a nastudoval existující implementace i jejich kryptografickou stránku. Z nich pak zvolil implementaci Moxie Merlinspika, kterou doplnil o postrádanou vlastnost IND-CCA.

Jako problematické považuji:
a) nutnost instalace mnoho softwaru na server i klienta;
b) nedostatečný návrh zabezpečení jednotlivých komponent na Windows.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Výsledky práce považuji za použitelné pro testovací provoz. Pro provoz v produkčním prostředí bych je zatím nedoporučoval, dokud se nevyjasní zabezpečení jednotlivých komponent na Windows.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1. Podle měření na str. 41 dochází k průměrné prodlevě mezi událostí a zápisem do logu ve výši 35 sekund. Z jakého důvodu k takové prodlevě dochází? Lze ji nějakým způsobem ovlivnit např. upravením vhodného klíče v registru Windows?
2. Navržené schema vyžaduje zdrojovou IP adresu. Jakým způsobem ji student získává na LAN za NAT?
3. Proč je zvoleno tolik softwaru třetích stran pro implementaci serverové komponenty?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*80 (B)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Jde o výbornou diplomovou práci. Je škoda že díky zbytečným konzistenčním chybám, a díky opomenutí návrhu zabezpečení jednotlivých komponent na Windows ji musím hodnotit jen jako velmi dobrou. Diplomovou práci pana Bc. Petra Klejcha doporučuji k obhajobě a hodnotím ji stupněm B (velmi dobře).

Podpis oponenta práce: