Hodnocení vedoucího závěrečné práce

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

Student: Bc. Martin Volek
Vedoucí práce: Mgr. Rudolf Bohumil Blažek, Ph.D.
Název práce: Automatické testování bezpečného nastavení služeb se šifrovanými protokoly
Obor: Počítačová bezpečnost

Datum vytvoření: 31. 1. 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 hodnotím jako průměrně obtížné.

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:
Práce splňuje všechny body zadání, mám ale výhrady k rozsahu prostudování možnosti implementovat vyvinutý nástroj jako zásuvný modul pro penetrační testovací software nmap. Rozhodnutí tento modul neimplementovat je zdůvoděno jedinou větou v prvním odstavci kapitoly 2 na str. 27. Nad rámec zadání student vytvořil nástroj na konverzi značení šifrovacích sad mezi formátem "TLS Cipher Suite Registry" používaným v RFC 5246 (TLS 1.2) a souvisejících RFC na jedné straně a formátem knihovny OpenSSL na straně druhé.

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 rozsahem a podrobností zpracování splňuje požadavky na diplomovou práci. Pouze diskuse jednodlivých fází komunikace pomocí šifrovaných algoritmů by měla být v některých částech podrobnější a ucelenější.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*59 (E)*

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:
Práce má dobrou logickou strukturu, avšak po věcné stránce má nedostatky, obsahuje některé věcné chyby a nepřesnosti a místy by si zasloužila preciznější formulace. Především v kapitole 1 v popisu technologií a postupů používaných pro komunikaci pomocí šifrovaných protokolů. Příkladem nedostatků je zaměňování termínů "symetrické" a "asymetrické" šifry s termíny "asynchronní" a "synchronní" šifry, na které byl student upozorněn vedoucím práce. Dalším příkladem je záměna pojmů asymetrický šifrovací algoritmus a algoritmus pro výměnu šifrovacího klíče. Je však nutné zmínit, že tyto nedostatky se v práci vyskytují ojediněle (každý cca 2x) a jinde je terminologie až na drobnosti správná.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*90 (A)*

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:
Z formálního hlediska je práce napsána odpovídajícím způsobem, bez závažných typografických prohřešků. Z jazykového hlediska by bylo vhodnější používat méně anglických termínů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*70 (C)*

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 se zdroji je na akceptovatelné úrovni. Mnoho zdrojů student získal na základě vlastní aktivity. Odkazy na wikipedii slouží často jako počáteční bod pro vyhledání odbornějších publikací, což je v pořádku.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*70 (C)*

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:
Student vytvořil nástroj, který analyzuje výstup programu nmap a jeho skriptů pro vyhodnocení bezpečnosti povolených verzí testovaného SSL/TLS protokolu a jeho povolených šifrovacích sad. Ověřuje časovou platnost certifikátů identity serveru a detekuje změny certifikátu od dřívější konfigurace. Podobný nástroj vytvořil též pro protokol SSH, který vyhodocuje bezpečnost povolených verzí protokolu a detekuje změny veřejného klíče serveru od dřívější konfigurace.

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:
Student implementoval nástroje, které vyhodnocují výstup programu nmap a jeho vybraných skriptů tak, aby ohodnotil úroveň zabezpečení testovaných šifrovacích protokolů. Hlavním přínosem je možnost ohodnocení bezpečnosti konfigurace testovaných protokolů na základě kritérií určených uživatelem, což umožní kontrolu, zda konfigurace odpovídá zákonným požadavkům či interním normám. Praktické využití nástrojů v bezpečnostní komunitě IT může být bohužel omezeno volbou vytvořit je jako nadstavbu a nikoliv zásuvný modul programu nmap. Nadstavba existujících nástrojů obvykle sjednocuje více technologií v komplexní bezpečnostní systém se širokým pokrytím různých aspektů síťové a počítačové bezpečnosti. Nástroj s úzkým záběrem, který využívá převážně výstupů programu nmap, by měl jako zásuvný modul nmapu lepší šanci být akceptován komunitou odborníků v IT bezpečnsosti.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* ***2=velmi dobrá aktivita,*** *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student byl dostatečně aktivní a samostatný, v poslední fázi práce na schůzky chodil pravidelně a připraven. Bohužel však někdy byl příliš samostatný, když se bez vzevrubné analýzy a konzultace rozhodl implementovat vyvinuté nástroje v rozporu se zadáním práce jako nadstavbu nmapu, nikoliv jako jeho zásuvný modul.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*69 (D)*

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:
Hlavní slabinou práce je fakt, že vyvinuté nástroje byly implenetovány v rozporu se zadáním práce bez potřebné analýzy. Zadáno bylo ověřit vhodnost vytvořit nástroje jako zásuvné moduly programu nmap. Bez řádného zdůvodnění ale byly vytvořeny jako jeho nadstavba. Dalším negativním aspektem jsou věcné chyby a nevyváženost jednotlivých částí v kapitole analýza. Na druhou stranu výsledky práce jsou potenciálně užitečné, především možnost ohodnocení bezpečnosti konfigurace testovaných protokolů na základě kritérií určených uživatelem, s cílem umožnit kontrolu, zda konfigurace odpovídá zákonným požadavkům či interním normám. Užitečnou se jeví i automatická konverze značení šifrovacích sad mezi formátem "TLS Cipher Suite Registry" a knihovny OpenSSL na straně druhé.

Podpis vedoucího práce: