Posudek oponenta závěrečné práce

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

Student: Bc. Martin Volek
Oponent práce: Ing. Tomáš Zahradnický, Ph.D.
Název práce: Automatické testování bezpečného nastavení služeb se šifrovanými protokoly
Obor: Počítačová bezpečnost

Datum vytvoření: 12. 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 práce hodnotím jako středně 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:
Cílem práce bylo navrhnout metodologii testování nastavení serverů a klientů zabezpečení spojení pomocí rodin protokolů SSL/TLS, a dále návrh a implementace testovacího nástroje. Problematice metodologie se student v práci samostatně nevěnuje. Očekával bych, po popsání základů protokolů bude následovat návrh metodiky, a teprve pak návrh a implementace nástroje implementujícího navrženou metodiku. Student měl rovněž jako součást zadání prostudovat vhodnost začlenění navrhovaného nástroje do standardního softwaru pro skenování nmap - kapitola 2. na str. 27 tuto část zcela postrádá. I přes tyto výhrady považuji zadání za splněné.

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 splňuje požadavky na diplomovou práci.

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

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 vykazuje významné množství kritických chyb. Jako příklad uvádím:
- v práci se zaměňují synchronní šifry se šiframi symetrickými (sekce 1.1.2 na str. 4);
- cituji: „Obvykle je seznam certifikátů důvěryhodných certifikačních autorit přímo v operačním systému“ (sekce 1.1.4 str. 5). V počítači jsou přímo instalovány kořenové certifikáty, nikoliv jen jejich seznam;
- jsou zaměňovány šifrovací algoritmy s algoritmy po digitální podpis a zřízení klíče DSA a Diffie-Hellmannův algoritmus jsou uváděny jako asymetrické šifry (str. 7);
- cituji: „Jeho bezpečnost [Diffie-Hellmannův alg.] je tedy určena obtížností vyřešit (diskrétní) odmocninu v této multiplikativní grupě.“ K prolomení Diffie-Hellmannova algoritmu je nutné vyřešit problém diskrétního logaritmu (str. 9 odst. 2).
- práce uvádí, že Zákon o kybernetické bezpečnosti č. 181/2014 Sb. (ZkKB) se povinný pouze pro orgány veřejné moci, přitom § 3 ZkKB uvádí osoby povinné k zákonu a odvětvová kritéra určuje vyhláška č. 315/2014 Sb (str. 9 sekce 1.1.8).

Logická úroveň práce by měla od sebe odlišit návrh metodiky od návrhu nástroje. S vynaložením značného úsilí lze metodiku vidět v návrhu testovacího nástroje.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*50 (E)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

Komentář:
Po formální stránce je práce podprůměrná. Na jedné straně student píše o tom, jak se seznámil s protokoly důkladně, avšak jejich popis je velmi povrchní a nepříliš korektní. Na straně 9 začíná kopie vyhlášky NBÚ č. 316/2014 Sb. přílohy č. 3 a končí na straně 11. Z tohoto dokumentu kopíruje část (cituje jej), ale doporučuje vyhlášky NIST a FIPS (str. 9). Úroveň detailů je nekonzistentní - např. u Diffie-Hellmannova algoritmu student zabíhá až do matematické úrovně (str. 8), avšak dále píše, že sdílené tajemství spočítané algoritmem cituji: „nelze zpětně rekonstruovat, ani v případě, že by útočník odchytil veškerou komunikaci“. Takovouto formulaci považuji přinejmenším za nešťastnou.

Po jazykové stránce obsahuje práce neskutečné množství anglicismů (handskaku, poisoningu, parsováním, , nacházím i hrubé chyby (např. str. 4 sekce 1.1.3 řádek 2 - strany ... ověřily).

Po typografické stránce nacházím jen drobné nedostatky (např. jednoznaková předložka k na konci řádku na téže straně, apod.), parchant-sirotek na straně 54.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*60 (D)*

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 velké množství zdrojů, avšak některé z nich jsou pochybné kvality. Nacházím 5 odkazů na Wikipedii. Většinou jde o webové stránky. Jen málo z odkazů směřuje do knih a vědeckých publikací, které by v oboru kryptografie měly být základem. Odkazy do kryptografických knih např. B. Schneiera anebo byť jen odkaz na přednáškové materiály předmětu Bezpečnost, naprosto chybí, což se také odráží na terminologické insuficienci. Řazení literatury není podle jmén autorů, ale podle výskytu v práci, což ztěžuje orientaci v seznamu literatury.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*75 (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 v práci navrhl a implementoval nástroj pro hodnocení konfigurace SSL/TLS spojení. Nástroj řádně otestoval, bohužel i na cizích serverech - seznam.cz, cvut.cz a google.com. Spouštění nástrojů pro testování na serverech třetích osob je bez souhlasu vlastníka serveru zakázáno, proto nepovažuji za vhodné takové výstupy v práci ukazovat.

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:
Použitelnost výsledků práce vidím, bohužel, jako značně omezenou, a to z několika důvodů:

1. Volba implementační platformy TypeScript/NodeJS je __naprosto__ nestandardní a zcela mimo oblast penetračního testování. V prostředí penetračního testování je standardem jazyk Python, případně Ruby pro moduly frameworku Metasploit. Pro jednodušší projekty se běžně používá Shell, nejčastěji Bash. Student měl analyzovat možnost zapojení nástroje do skeneru nmap. U tohoto nástroje bych očekával, že bude součástí nástroje nmap anebo jiného analyzátoru, např. sslyze anebo jako modul pro Metasploit. Tím se ale bohužel práce nezabývá.
2. Licence v práci uvádí, že výsledky práce smí být použity pouze se souhlasem autora. U obdobné práce bych očekával GPL, LGPL, anebo CC BY SA licenci.

Volba implementační platformy a licence de-facto diskvalifikují využití práce i její další rozvoj.

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. Vysvětlete rozdíl mezi synchronní a symetrickou šifrou?
2. Vysvětlete, proč jste se rozhodl pro Vaši implementační platformu?
3. Jaké osoby jsou osoby povinné podle Zákona o kybernetické bezpečnosti č. 181/2014 Sb. v platném znění a které z nich jsou orgány veřejné moci?

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

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:
Práce mohla poskytnout metodiku a nástroj pro hodnocení konfigurace serverů používajících SSL/TLS spojení. Výstupem práce sice nástroj je, avšak je vyvinut na zcela nestandardní bázi, navíc s licencí vyžadující souhlas autora s použitím. Tato nešťastně zvolená kombinace de-facto znemožňuje využití nástroje a zvolená implementační báze jeho rozvoj. Toto však není důvodem níže uvedeného rozhodnutí.

Primárním důvodem je, že práce obsahuje extrémní množství faktických chyb a terminologických faux-pas, které jsou podle mého názoru neslučitelné s obhajitelností práce v oboru Počítačová bezpečnost. Je naprosto nezbytné ji přepracovat a dát do pořádku.

Pro výše uvedené nedostatky NEDOPORUČUJI práci k obhajobě a hodnotím ji stupněm F (nedostatečně).

Podpis oponenta práce: