FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Michal Franc
Oponent práce: Ing. Josef Kokeš
Název práce: Analýza bezpečnosti počítačové sítě
Obor: Bezpečnost a informační technologie

Datum vytvoření: 8. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. 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 dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Problém se splněním zadání této práce je, že není jasné, co byl vlastně výchozí stav, co byl cíl a co se mělo v rámci práce udělat. Kapitola o definici cílů sice v práci je, ale je tak obecná, že si ji každý může vyložit jinak. Z mého pohledu zadání spíše splněno nebylo, hovoříme-li o provedení bezpečnostní analýzy, očekával bych podstatně větší spektrum provedených testů a také jejich podstatně větší hloubku. V práci se například vyskytuje slovo "heslo" čtyřikrát, ale ani jednou v souvislosti s nějakými testy.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*20 (F)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Dodaný text mi připadá spíše jako svodka pro CEO o tom, co IT oddělení udělalo v uplynulém roce se síťovou infrastrukturou, než jako bakalářská práce. Téměř úplně chybí teoretická rešerše (jaké jsou aktuální best-practices v přístupu k řešenému problému), což je vidět i na seznamu literatury čítajícímu 4 položky, z nichž jen [3] je v textu skutečně využita, ostatní jsou pouze odkazovány. Přístup k analýze podle textu využívá standard PTES, který ve mě nebudí důvěru (léta neaktualizovaný, jeho webová stránka nemá HTTPS), ale prakticky to v práci není vidět. Je využita metodika STRIDE pro modelování hrozeb, ale tak stručně, že působí spíš jako slovníkové heslo než jako skutečné modelování. Každopádně velké množství hrozeb úplně chybí, asi - bohužel nejsou stanoveny bezpečnostní cíle, takže nedokážu určit, co vlastně měla analýza řešit. Zcela chybí vyhodnocení jednotlivých nalezených hrozeb. U navrhovaných řešení chybí jakákoliv diskuse o tom, jaké varianty byly zvažovány a proč student vybral ty, které vybral. Práce je také velice krátká, drtivou část tvoří výstupy pentestovacích nástrojů (ovšem nijak nevysvětlené, co z nich pro bezpečnost plyne) nebo výpisy konfigurace. Nemohu vyloučit, že pro deklarovaný účel (odstranění bezpečnostních slabin počítačové sítě dané společnosti) to stačí, ale nejde o dostatečnou bakalářskou práci.

Naproti tomu technická stránka dokumentu se mi velice líbí, určitě prosím zachovat!

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*10 (F)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:

Nepísemnou část práce tvoří konfigurační soubory pro LDAP, ShoreWall, Suricatu a Zabbix, bez jakékoliv dokumentace a bez jakékoliv informace, co je vlastní dílo studenta a co jsou převzaté vzorové soubory. Z pohledu praktického uplatnění bych tu očekával aspoň vytvořené a nakonfigurované virtuální stroje, které mají být v síti později nasazeny, včetně detailního popisu, jak je vytvořit od nuly. V současném stavu nevidím v této části práce žádný přínos.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*50 (E)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Navzdory kritice výše nemohu vyloučit, že práce je pro společnost, pro kterou byla vytvořena, využitelná. Moje výhrady se týkají primárně využití práce jako práce bakalářské, pro praktické využití u konkrétního uživatele skutečně práce může mít význam. Zejména pokud jde o uživatele, který o problematice nic neví a vědět nechce a celou práci chápal od začátku v duchu "máme nějakou počítačovou síť, nic o ní nevíme, podívejte se nám na to a udělejte něco, aby to fungovalo nějak bezpečně; ale hlavně po nás nic nechtějte a už vůbec to nechtějte po našich uživatelích". Toto mimochodem mělo být vysvětleno v textové části.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

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

Otázky:

1) Co všechno z vašich úprav bylo skutečně uživatelem realizováno?
2) Nasadil jste IDS/IPS systém. Kdo a jak bude sledovat jeho výstupy?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*20 (F)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Ve své současné podobě je podle mě bakalářská práce neobhajitelná. Může být užitečná pro svého uživatele, ale nelze ji uplatnit jako bakalářskou práci. Chybí rešerše dostupného teoretického aparátu, chybí popis metodiky, kterou student použil, chybí diskuse a výběr alternativ řešení, chybí přehledné vyhodnocení výsledků, chybí uplatnitelný výstup pro kohokoliv, kdo chce vědět i "proč" a ne jen "jak". Za daného stavu věci bohužel práci nemohu doporučit k obhajobě a hodnotím známkou F.

Podpis oponenta práce: