Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **Krenželák Nikola** **Oponent:** **Ing. Petr Žáček**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie v administrativě**
Akademický rok: **2017/2018**

Téma bakalářské práce: **Kybernetická bezpečnost malých firem**

Hodnocení práce:

		A	B	C	D	E	F
	Hodnocení: A – nejlepší; F - nevyhovující						
1.	Obtížnost zadaného úkolu	☐	☒	☐	☐	☐	☐
2.	Splnění všech bodů zadání	☐	☐	☐	☐	☒	☐
3.	Práce s literaturou a její citace	☐	☐	☐	☐	☐	☒
4.	Úroveň jazykového zpracování	☐	☐	☐	☐	☒	☐
5.	Formální zpracování – celkový dojem	☐	☐	☐	☐	☒	☐
6.	Logické členění práce	☐	☐	☐	☒	☐	☐
7.	Vhodnost zvolené metody řešení	☐	☐	☐	☐	☒	☐
8.	Kvalita zpracování praktické části	☐	☐	☐	☐	☒	☐
9.	Výsledky a jejich prezentace	☐	☐	☐	☐	☒	☐
10.	Závěry práce a jejich formulace	☐	☐	☐	☐	☐	☒
11.	Přínos práce a její využití	☐	☐	☐	☒	☐	☐

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení

E - dostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
1. Jste si naprosto jistý, že si nežádoucí osoba nepřečte obsah vámi zašifrované správy bez šifrovacího klíče ? Z jakého důvodu se symetrické šifrování může jevit jako "riskantní", když mají obě strany klíč ?
2. Jste si jistý, že se asymetrická kryptografie používá k zašifrování zpráv ? Pokud ano, nemá například šifrování pomocí RSA svá omezení ve velikosti šifrované zprávy ?
3. Je jediný důvod pro nepoužívání MD5 jeho zastaralost ?
4. Co je to Malware ?
5. Jaký je rozdíl mezi hrozbou a rizikem ?
6. Jak se dá z odkazu webové stránky poznat, jestli se jedná o zavirovanou stránku ? viz vaše tvrzení strana 19, kapitola 1.4.1

7. Můžete uvést příklad, kdy reálně počítačový virus způsobil vyhoření HW ? viz kapitola 1 + 1.4.2.1.
8. Jaký je rozdíl mezi zákonem 101/2000 Sb. Zákon o ochraně osobních údajů a GDPR ?
9. Vysvětlete prosím pojem "hacker", jeho význam. Jaký je rozdíl mezi white, grey a black hat hackerem ?
10. Které z našich bank využívá pro přihlášení biometrii ?
11. Z jakého zdroje jste vycházel, pro výběr hrozeb v kapitole 5 ?
12. Objasněte prosím důvod, proč bylo v tabulkách 9 a 10 zvoleno jako kritérium hodnocení šifrovacích nástrojů pomocí počtu podporovaných šifrovacích/hashovacích algoritmů ? Jak souvisí počet šifrovacích/hashovacích algoritmů s bezpečností ? Z čeho jste odvodil jako nejlepší ten, který obsahuje 5 a více ? Je tedy pravda, že pokud budu mít nástroj, který mi umožní svá data zašifrovat pomocí ROT10, ROT13, ROT15, ROT20 a ještě caesarovou šifrou, tak je skvělý a dostane 5 bodů ?
13. Jakým způsobem Firewall restartuje síť ? Co to znamená restartování sítě ?

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
Práce a způsob vyjadřování studenta jsou často nesrozumitelné. Student v některých částech píše "páté přes deváté". Celkově práce vypadá "neučesaným" dojmem poskládaných a poslepovaných informací v jeden celek, kdy dochází místy k absenci smyslu a logiky. Práce svým způsobem více či méně, obvykle méně, naplňuje body zadání práce. Hlavně níže uvedený bod práce 4... následně i bod 7. Dále práce velice zajimavě, dalo by se říci kuriózně, pracuje se zdroji a dochází ke špatnému uvedení či jinému upravení informací, které se v uvedených zdrojích dle citací nevyskytují nebo vyskytují, ale v jiné podobě či mají jiný smysl... Tabulky v kapitole 6 jsou vybrány bez podpory zdrojů, bez důvodu a často není zde uvedené co znamenají a co reprezentují. Práce je napsána sice ve stanoveném rozsahu, ale předaná informace bakalářskou prací je slabá. Jsou zde problémy s překlepy, chybami či špatnou formulací vět. Jsou zde i problémy s formální stránkou práce .. Nicméně, kladně alespoň hodnotím, že student oproti poslednímu pokusu zapracoval většinu podnětů oponenta a komise SZZ.

Nicméně i přes to se zde nachází spousta dalších chyb, nejasností a problémů. Zde je jejich výpis ...

1. Práce obsahuje překlepy, spoustu -> i v nadpisech. Např. kapitola 1.3 nebo věta "Před adwarem se dá bránit tak, že aktualizovaný veškerý software"..
2. Věty jsou často nejasné a styl vyjadřování nesrozumitelný. "ukládat uložená hesla", "podvody, jako například ... Malware, Počítačové virusy... "
3. Určitě je dobrý nápad instalovat na počítač více jak jeden antivirový program ? Viz tvrzení kapitola 1.4.2.1 -> "Každý počítač by měl být vybaven minimálně jedním antivirem." Prosím o uvedení zdroje tohoto doporučení ...
4. Někdy by bylo lepší části z použité literatury raději opsat a patřičně ocitovat namísto přepisu vlastními slovy a tedy ztrátě, modifikaci nebo vytvoření nového obsahu nezávisle na zdroji.
5. Bod zadání číslo 4 je pouze dalším výčtem vlastností GDPR, nikoliv popisem mezi GDPR a kybernetickou bezpečností malých firem. Tento bod je splněn maximálně ze 2 procent.
6. Hlasová detekce není biometrickou metodou ...
7. Ať hledám ve zdroji číslo [45], jak hledám, některá uvedená procenta v textu práce neodpovídají použitému zdroji..
8. Student opravil většinu problémů uvedených v předchozím posudku, ale bylo by velice vhodné, aby student po prvním neúspěšném pokusu o obhajobu zapracoval všechny připomínky oponenta ... Například připomínka číslo 14. o WPA3 a napsání v kapitole 5.4 je zde stále neopravená .. zdroj [48] ani při přepisu práce stále neobsahuje informaci o zavedení WPA3 v roce 2018 ... Ani to nenaznačuje ..

9. CNSA nevyužívá 192 bitových klíčů, i kdyby se jednalo o eliptické křivky, tak 192 bitů je málo ... Navíc, opět tuto informaci zdroj [48] neuvádí, zdroj [48] celkově nezmiňuje CNSA ... viz zdroj například https://tools.ietf.org/id/draft-jenkins-cnsa-cert-crl-profile-00.html. Navíc je rozdíl mezi informací, že WPA3 bude využívat klíče o délce 192-bitů a použitím klíčů se zabezpečením 192-bitů ...
10. Informace o WannaCry a opět pozoruhodné nakládání s informacemi ze zdrojů ... Viz strana 40, kapitola 5.5.2, jak jste se dostal k číslu 230000 ? Zdroj [42] toto číslo neuvádí ...
11. Kapitola 5.5.3 -> "Tento malware se začal objevovat v červnu..." - Kterého roku ? Pravděpodobně letošního, ale bylo by vhodné to uvést .. Navíc zdroj [44] informaci o červnu neuvádí .. Opět a neustále "zajimavá" reprezentace dat ze zdrojů.. Zdroj [44] neuvádí ani souvislost s Dánskem, Ruskem, atd. Je kuriózní, jak si student "vycucává" informace z prstu ... Nebo špatně cituje a uvádí zdroje ...
12. Kapitola 5.5.1, spam ještě neznamená, že se jedná o soubor...
13. Kapitola 5.5.1.1 a zdroj [40], opět se zde nikde neuvádí, že docházelo ke krádeži hesel pomocí Quant Loaderu ..
14. Jazyk dokumentace, kapitola 6.1.1, jakému jazyku odpovídá hodnota 1 ?
15. Tabulka 1. je nesmyslná a formulace v ní jsou zavádějící ... logický člen "nebo" ("OR") se používá jiným způsobem ... Neboli, pokud 4 body použijeme pro hodnocení při volbě možnosti instalace na "Windows 7, 8, 10 + OS X nebo Linux", proč i 4 body nejsou zvoleny pro možnost "OS X nebo Linux" ? Pokud systém je instalovatelný alespoň na Linux, což pokrývají obě dvě možnosti, tak by v nich teoreticky neměl být rozdíl ... A případně, jaký Linux ? OS X je také obdobně jako Linux založený na unixovém jádře ...
15. Tabulka číslo 3 podobný problém jako tabulka číslo 1 ...
16. Tabulka 11. přítomnost backdooru v šifrovací aplikaci dostává 5 bodů (je nejlepší) ... Tady se doufám student pouze upsal ... Protože VeraCrypt, snad, neobsahuje backdoor ... viz tabulka 30
17. Tabulka 12. vytrhnout z kontextu znakové sady využité ke stavbě hesla bez vztahu k délce hesla je nesmysl ... Proč jsou v prvním řádku uvedeny mezery a co znamená "vlastní řetězec" ???
18. Tabulka 13. Opravdu je stejné -> napsáno vtextu lepší, když zvolím dva z uvedených prohlížečů, třeba Edge a Operu, jako když zvolím jeden a to Chrome ??
19. Kapitola 6.1.5 "Firewall je určen pro monitorování sítě, detekování neţádoucích událostí v síti a jejich případnému řešení. Může například blokovat, restartovat síť nebo zablokovat komunikaci se serverem nacházejícím se v jiné síti." -> Zde by bylo vhodné uvést zdroj ... Tato informace není moc korektní ...
20. Tabulky 15 a 16. Firewall vyžaduje CPU a RAM o daných parametrech nebo Firewall obsahuje CPU a RAM daných parametrů ??? Opět, bylo by vhodné popsat tabulky.
21. U tabulek by jednotlivé parametry měly být odůvodněné a zvoleny na základě opory zdrojů. Například, proč u násgtrojů pro ukládání hesel není brán v potaz faktor, že byla někdy narušena jejich bezpečnost ?
22. V kapitole 6.3 dochází k "náhodnému" výběru bez uvedení důvodu výběru open source softwaru. Pro analýzu by bylo vhodné v jednotlivých kategoriích nevybírat pouze jeden, ale více nástrojů, aby došlo k vzájemnému porovnání. Například důvod, proč nebyl zvolen LastPass ale KeePass.
23. Chyby v závěru ...

Na základě výše uvedených připomínek (určitě se nejedná o kompletní výčet) a příhlednutím zapracování výtek z předchozího pokusu doporučuji práci k obhajobě, s tím, že by student u obhajoby i tak měl vysvětlit a patřičně zodpovědět všechny výše uvedené dotazy a vyjasnit všechny nejasnosti, které se v práci nacházejí. Práci doporučuji hodnotit maximálně stupněm E - dostatečně.

Datum 4.9.2018 Podpis oponenta bakalářské práce