FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš, Ph.D.
Student:	Bc. Tomáš Arazim
Název práce:	Nástroj pro realizaci phishingové kampaně
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	11. května 2024

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání bylo splněno. Zpočátku jsem měl pochyby o vhodnosti tohoto zadání vzhledem k obsahu a jeho potenciální zneužitelnosti, ale provedení práce tyto obavy vyloučilo. Zároveň rozsah analyzovaných aplikací do značné míry (ale ne zcela) vyvrátil moji nejistotu o tom, jestli by nemělo jít spíše o téma bakalářské.

2. Písemná část práce

80 /100 (B)

Velice kladně hodnotím druhou, nejrozsáhlejší kapitolu, ve které student pojednává o metodice hodnocení nástrojů pro vedení phishingové kampaně a o hodnocení jím zkoumaných aplikací. Tato část je velmi informačně bohatá a myslím si, že vysoce přínosná tím, že zahrnuje i skutečné experimenty autora a jeho poznatky o tom, jak je možné nástroj zprovoznit a nakonfigurovat. Také větší část třetí kapitoly o samotné pokusné realizaci kampaně je dobrá. Kapitola o vylepšení nástroje mi připadá spíš do počtu, než že by byla pro práci nezbytná. Nejméně spokojen jsem s úvodní kapitolou, která je podle mě dosti stručná a nepostihuje ideálně ani problematiku ochrany proti phishingu obecně, ani praktických aspektů samotného vedení takové kampaně (např. to, jak negativní zkušenost s podobnými kampaněmi vede někdy uživatele k tomu, že automaticky zahazují všechny maily z neznámých zdrojů a naopak je upevňuje v nezdravé důvěře k těm známým). Smysl sekce 1.5 nevidím.

Po jazykové stránce vykazuje práce značné množství chyb v gramatice, včetně čárek ve větách, shodě podmětu s přísudkem, měkkými a tvrdými i, apod. Srozumitelnost obsahu není ovlivněna, ale nepůsobí to dobře. Text by ještě potřeboval korekturu.

3. Nepísemná část, přílohy 50 /100 (E)

Nepísemná část práce je poměrně chudá, což je ale s ohledem na charakter práce pochopitelné. Tvoří ji zejména obsah jednotlivých e-mailů pokusné phishingové kampaně a následné vysvětlení pro postiženého uživatele, čeho si měl všimnout. Tato část je v pořádku, i když bych uvítal vzorové vygenerované maily např. ve formátu .eml. Druhou částí přílohy je jednoduchý addon pro nástroj Gophish, který zaregistruje podvedeného uživatele do výukového kurzu na Moodle. Soudě dle kódu funguje v pořádku, jedinou zjevnou chybou je použití case-sensitive porovnání při hledání HTTP hlaviček (specifikace říká, že case-sensitive nejsou).

Chybí mi zde zdrojový kód diplomové práce.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Hodnocení vlastních zkušeností s instalací a konfigurací jednotlivých nástrojů a jejich možnostmi vnímám jako velmi přínosnou, umožňuje to případnému realizátorovi soustředit se na 2-3 nástroje s nejlepšími charakteristikami v těch oblastech, které pro své aktuální použití považuje za nejdůležitější. Tomu pomáhá i dobře vytvořená metodika hodnocení. Chybí konkrétní detailní údaje o tom, jak nástroj prakticky použít, to si bude muset uživatel dohledat v dokumentaci (existuje-li), ale nevidím to jako problém - zmenšuje to riziko, že někdo diplomovou práci použije jako jednoduchý návod na provedení útoku.

Celkové hodnocení 80 /100 (B)

Student vytvořil vhodnou metodiku pro porovnání nástrojů pro vedení phishingové kampaně a následně podle této metodiky porovnal téměř 20 free aplikací. Pro každou popsal své zkušenosti s nimi a vysvětlil, kde jsou jejich kritické body. Připravil také dvě pokusné phishingové kampaně i včetně výukového materiálu, který vysvětluje postiženým, čeho si měli všímat. Tyto části hodnotím velmi pozitivně. Nepříliš dobře na mě působí slabý úvodní popis východisek, zejména obran proti phishingu, a množství jazykových chyb v textu práce. Nezbavil jsem se také zcela pochyb o tom, zda jde o téma vhodné pro magisterský stupeň. Přesto však považuji práci za zajímavou a jsem rád, že ji student napsal. Hodnotím B - velmi dobře.

Otázky k obhajobě

1) Máte nějakou zpětnou vazbu od cílů vašich pokusných kampaní nad rámec konkrétních statistických ukazatelů úspěšnosti?
2) Doporučil byste některou z analyzovaných aplikací pro použití na ČVUT FIT?

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.