FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Miroslav Prágl, MBA
Student:	Gabriel Hévr
Název práce:	Analýza a demonstrace zranitelnosti ProxyLogon
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	30. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Zadání práce je objektivně náročné, přesto je splněno resp. překročeno ve všech bodech. První dojem je skvělý, písemná část je přehledná, jednotlivé body jsou rozpracovány velmi pečlivě a hlavně srozumitelně. Práce tak potenciálně zaujme jak bezpečnostního specialistu, tak i rutinního správce informačních technologií.

2. Písemná část práce 95 /100 (A)

Rozsah je nadstandardní, práce je vyvážená, přes bohatost informací dobře a lehce čtivá. Logická struktura a návaznosti jsou plynulé a přirozené. Členění a typografie jsou harmonizující, použití obrázků přiměřené a doplňující. Gramatických chyb je minimum a díky dobré stylistice si jich čtenář pravděpodobně ani nevšimne. Seznam zdrojů je obsáhlý, jsou korektně citované / odkazované. Pro demonstraci byly korektně použity zkušební verze komerčního SW (Windows Server, Exchange) a skriptovací jazyk Python s BSD kompatibilní licencí.

3. Nepísemná část, přílohy 95 /100 (A)

Použité technologie jsou standardní a vhodné. Praktická část, tedy prostředí pro demonstraci zranitelnosti, využívá virtualizaci Exchange a Windows serveru pomocí VirtualBoxu (z kapacitních důvodů v prostředí Cloud FIT), vlastní útok je realizován sadou skriptů v jazyce Python. Potenciální nebezpečnost skriptů byla potvrzena na mém počítači hned při stahování antimalwarem (Windows Defender), který za blokoval soubor proxylogon.py. Student po dohodě úspěšně demonstroval výsledek útoku až po RCE - vzdálený shell.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Práce kvalitně syntetizuje poměrně čerstvě zveřejněné informace o zranitelnostech do uceleného díla a současně provádí analýzu příčin i (potenciálních) následků těchto zranitelností vč. konkrétních i obecných bezpečnostních doporučení. Obzvlášť hodnotím práci na skriptech v multiplatformním Pythonu - ty musel autor objektivně napsat sám jen na základě popisů konceptu zranitelnosti a střípků v diskusích; případné kompletní funkční skripty jsou z pochopitelných důvodů z Internetu okamžitě odstraňovány.

Celkové hodnocení 99 /100 (A)

Přiznám se, že jsem se k této oponentuře přihlásil kvůli příležitosti přečíst si něco o konkrétní závažné zranitelnosti a zvědavosti, jak se student tématu zhostil. Výsledek mne příjemně překvapil a nemám k němu v podstatě co dodat - tato bakalářská práce je na úrovni výborné diplomové práce či edukativní odborné publikace.

Otázky k obhajobě

Jak zmiňuji výše, práce je natolik rozsáhlá a obsáhlá, že na tomto místě namísto otázek autorovi děkuji za mimořádný výsledek.

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.