FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Gabriel Hévr
Název práce:	Analýza a demonstrace zranitelnosti ProxyLogon
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	17. 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 bylo splněno ve větším než očekávaném rozsahu, student provedl velmi detailní analýzu i řady spojených útoků a také technikami reverzního inženýrství zjistil přesná místa v kódu, na která bylo útočeno.

2. Písemná část práce 95 /100 (A)

Písemná část práce je velmi detailní, principy útoku, jeho provedení i následky jsou systematicky, pečlivě a srozumitelně popsány. Je trochu otázka, jestli do technického textu patří poněkud spekulativní části podsekcí sekce 2.3, ale pravda je, že dobře uvádějí čtenáře do celkového kontextu útoku.

Narazil jsem na několik chyb, které ovlivňují faktickou správnost, ale jsou spíše charakteru překlepu (např. na straně 11 je psáno OT__2, myšleno je však OT__x) a čtenář je snadno odhalí. V příkladu vytvořeného programu na str. 37 je použit parametr -s, který však není v textu zdokumentován. V práci se také stále vyskytují menší jazykové chyby, je jich však jen málo. Matoucí jsou sekce 3.4, 3.5 a 3.6, které by zřejmě měly být spíš v samostatné kapitole nebo jako podsekce nějaké sekce.

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

Nepísemnou část práce tvoří za prvé samotné virtuální prostředí pro demonstraci zranitelnosti. Z licenčních důvodů nemůže být publikováno, postup jeho vytvoření je však uveden.

Druhou nepísemnou částí je pak sada demonstračních skriptů, které automatizují celý útok a přesvědčivě tak demonstrují jeho nebezpečnost. Ta je ještě viditelnější, jakmile si všimneme, jak jsou tyto skripty krátké a poměrně jednoduché - provedení útoku je evidentně velmi jednoduché i pro začátečníka.

Pozn.: Tyto skripty by šlo snadno použít i proti reálným serverům. Nepovažujeme to však za velkou hrozbu, protože zranitelnost byla v uplynulém roce masivně zneužívána a zranitelné servery, které ještě na internetu jsou, už skoro jistě napadeny byly.

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

Praktickým přínosem práce je zejména detailní popis vysoce kritické zranitelnosti, která minulý rok proběhla světem, spolu s detailními ukázkami, jak snadno ji lze zneužít. Těžko si představit, jak ještě lépe správce MS Exchange přesvědčit, aby své servery aktualizovali. Práce by tak měla přispět k tomu, aby zranitelné servery zmizely co nejdříve ze světa.

Za neméně důležitý přínos považuji i analýzu příčin, které vedly ke vzniku zranitelnosti. Vývojáři by si měli všimnout, jak se relativně drobné odchylky od principů bezpečného programování zkombinovaly v katastrofální celek. Mělo by jít o názorný důkaz, proč tyto principy chceme dodržovat a proč není dobré v nich hledat zkratky.

5. Aktivita studenta

- [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

6. Samostatnost studenta

- [1] **výborná samostatnost**
- [2] velmi dobrá samostatnost
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Celkové hodnocení 95 /100 (A)

V rámci své bakalářské práce student provedl velmi detailní a pečlivou analýzu poměrně čerstvé kritické zranitelnosti. Podrobně popsal způsob, jakým mohla být zneužita, a nad rámec očekávání provedl i reverzní analýzu postižené části kódu za účelem zjištění konkrétních příčin zranitelnosti. Připravil také demonstrační prostředí a skripty, které by měly každého váhajícího administrátora přesvědčit o nutnosti okamžité aktualizace. V řadě ohledů jde o práci nad rámec toho, co očekáváme od práce bakalářské, snadno by se mohla uplatnit i jako diplomová. Doporučuji k obhajobě, hodnotím známkou A=výborně a doporučuji ke zvážení na udělení ceny děkana.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.