Posudek oponenta diplomové práce

Student: Dejmal David, Bc.
Téma: Server pro správu klíčů v prostředí vSphere 7.0 (id 23750)
Oponent: Homoliak Ivan, Ing., Ph.D., UITS FIT VUT

1. **Náročnost zadání** **průměrně obtížné zadání**
   Zadanie vychádzalo z praktického problému správy kľúčov vo virtualizovanom prostredí, ku ktorému podľa študenta existujú len komerčné nástroje z proprietárnym kódom.
2. **Splnění požadavků zadání** **zadání téměř splněno s drobnými výhradami**
   Jediná vec, ktorú by som vytkol je chýbajúca kvantitatívna analýza výkonnosti riešenia.
3. **Rozsah technické zprávy** **splňuje pouze minimální požadavky**
   Práca obsahuje 58 latex-om vysádzaných strán vrátane referencií a príloh. Len po záver je to 45 latex-om vysádzaných stránok. Podotýkam tiež, že niektoré obrázky ako 2.8, 2.9 a 2.10 sú zbytočné z pohľadu práce a obsah umelo navyšujú.
4. **Prezentační úroveň předložené práce** **70 b. (C)**
   Rozsahy a prehľadnosť niektorých kapitol sú prípustné. Výnimkou je kapitola 2, ktorá je zbytočne dlhá.

   Mám niekoľko ďalších poznámok. V úvode chýba organizácia práce a odkazy na jednotlivé kapitoly. V definícii základných pojmov chýba bližšia špecifikácia typov šifrovacích kľúčov. V sekcii 2.3.2 chýbajú referencie na jednotlivé útoky, resp. na dôkazy výskytu týchto útokov. Obrázok 4.4 znázorňuje schému útoku na navrhnuté KMS a útočník u neho získa certifikáty KMS a vCenter, na základe čoho dokáže vytvárať vlastné záznamy v KMS ale nedokáže odcudziť žiadny kľúč. Je zvláštne, že v tomto type útoku je certifikát tajomstvom, ktoré umožňuje útočníkovi delegovať svoj prístup ku KMS. Vo všeobecnosti sú certifikáty zpravidla zverejniteľné bez akýchkoľvek následkov. Chcel by som tiež poukázať na to, že teoreticky dokáže takýto útočník uskutočniť DoS útok vyčerpaním výpočetných alebo priestorových zdrojov na KMS.
5. **Formální úprava technické zprávy** **70 b. (C)**
   Práca je typograficky na priemernej úrovni. Práca obsahuje malé množstvo preklepov a miestami aj gramatické chyby.

   Poznámky pod čiarou sú typograficky nesprávne. Nesprávne sú tiež použité citácie na konci vety - majú byť súčasťou vety, zatiaľčo študent ich umiestňuje za vetu. Obrázky 2.2, 2.4, 2.8, atď. plávajú v strede stránky, namiesto typograficky správnejšieho zarovnania na vrch alebo spodok stránky.

   Chýbajú bodky na konci popiskov obrázkov 2.3, 2.4, 2.6, 2.8, atď.
   Niektoré obrázky mi prídu zbytočné - obrázok 2.8 a 2.9, ktoré zobrazujú fyzické kľúče a v jednom prípade sú doplnené aj heslovitými popiskami, ktoré nenesú dôležitú informáciu.
6. **Práce s literaturou** **75 b. (C)**
   Práca s literatúrou je na vyhovujúcej úrovni. Zvolené študijné prameňe sú relevantné a sú aj odlíšené od vlastných výsledkov. Na druhej strane treba poznamenať, že väčšina referencií sú webového charakteru, aj napriek tomu, že literatúra obsahuje mnoho recenzovaných článkov súvisiacich s použitými technológiami.
7. **Realizační výstup** **70 b. (C)**
   Práca má pekný realizačný výstup. Experimenty a implementácia sú na dobrej úrovni. Študent tiež diskutuje možnosti ďalšieho rozvoja.
8. **Využitelnost výsledků**
   Výsledky sú využiteľné v praxi, keďže práca bola riešená v spolupráci s firmou, ktorá bola čiastočne zadávateľom.
9. **Otázky k obhajobě**
   Uveďte možnosti útočníka, ktorý získal certifikáty ku KMS & vSphere a tiež možné techniky obrany.
10. **Souhrnné hodnocení** **72 b. dobře (C)**
    Práca je štandardne obtiažneho zadania. Zadanie bolo splnené vo všetkých bodoch, z malými výhradami. Rozsah práce spĺňuje minimálne požiadavky. Študent volil vhodnú literatúru. Práca poskytuje realizačný výstup, ktorý je využiteľný praxi. Celkovo prácu hodnotím stupňom **C (72 bodov)**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 9. června 2021

Homoliak Ivan, Ing., Ph.D.
oponent