

Posudek oponenta bakalářské práce

Student: Krůl Michal
Téma: Analýza provozu protokolů Kerberos, NTLM, SAML 2.0 (id 22531)
Oponent: Orsák Michal, Ing., UPSY FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**
Popsané útoky a protokoly jsou poměrně známé. Výsledný plugin do Flowmon sondy se ukázal být poměrně jednoduchá záležitost. Získávání potřebných dat, vytváření testovacího prostředí a práce s uzavřeným software však zvyšuje obtížnost.
- 2. Splnění požadavků zadání** **student se odůvodněně odchýlil od zadání**
Detekce útoků a monitorování protokolů Kerberos, NTLM a SAML 2.0 již byla zdokumentována, což limituje možnosti návrhu.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
Rozsah technické zprávy odpovídá požadavkům kladeným na bakalářskou práci. Větší část práce je věnována popisu protokolů, útoků a detekcí.
- 4. Prezentační úroveň předložené práce** **75 b. (C)**
Technická zpráva je napsána přehledně a kapitoly jsou uspořádány v logickém sledu. Některé myšlenky jsou formulovány neodborně. Řada kapitol působí dojmem, že jsou uměle natahovány.
- 5. Formální úprava technické zprávy** **75 b. (C)**
Vytvořený text má charakter odborného textu práce obsahuje určité množství překlepů. Na řadě míst jsou však špatně použity pojmy.
- 6. Práce s literaturou** **90 b. (A)**
Studijní prameny jsou voleny vhodným způsobem a jsou v textu správným způsobem citovány.
- 7. Realizační výstup** **75 b. (C)**
Realizačním výstupem je především rešerše útoků na zmiňované protokoly, samotný plugin do Flowmon sondy je poměrně přímočará věc.
- 8. Využitelnost výsledků**
Práce může sloužit jako dobrý úvod do problematiky útoků na zmiňované protokoly. Plugin do Flowmon sondy může být použit pro analýzu daných protokolů.
- 9. Otázky k obhajobě**
 - Jakou informaci musí sonda extrahovat pro detekci útoků na Kerberos, NTLM a SAML 2.0?
 - Byla provedena alespoň orientační měření výkonnosti Flowmon s daným pluginem?
- 10. Souhrnné hodnocení** **79 b. dobře (C)**
Práci hodnotím jako průměrně až středně obtížnou s tím, že jádrem práce byla rešerše. Práce nepřináší nové návrhy monitorování ani útoků na dané protokoly.
Proto navrhuji hodnocení stupněm 'dobře' (C).

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

V Brně dne: 25. června 2020

Orsák Michal, Ing.
oponent