MASARYKOVA UNIVERSITA
FAKULTA INFORMATIKY

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Student: Andrej Růžička

Název: MONITOROVANIE SÍŤOVEJ PREMÁVKY HONEYPOTU

Posudek:

Předkládaná práce obsahuje přehled některých open-source honeypotů a popis vybraných monitorovacích nástrojů. V praktické části je pak představen skript pro zpracování NetFlow dat o síťové komunikaci.

Práce začíná průřezem některými honeypoty, které jsou dostupné v open-source prostředí. Autor uvádí, že navazuje na předchozí bakalářské práce na podobné téma, bohužel ale tato vazba velmi nezřetelná. Místo toho autor popisuje některé oblasti znovu a zejména se nezabývá vlastnostmi důležitými pro zaměření práce, tj. monitorování síťového provozu honeypotů. Popis honeypotu Thp je nejasný. Není např. zřejmé, co znamená, že honeypot „zveřejňuje porty služeb", ani to, jak vlastně komunikuje (zda vůbec) s útočníkem.

Práce pokračuje popisem monitorovacích nástrojů, které jsou také vybrány značně nahodile (specializovaný Sebek vs. syslog). Opět není jasné, proč jim byla věnována pozornost a jakou mají roli v plánovaném výsledku. Přinejmenším sporná je poznámka o nevhodnosti databáze MySQL, zejména když odkazovaný zdroj, který ji má potvrdit sám uvádí, že MySQL je bezproblémová databáze.

V praktické části je představen skript pro zpracování NetFlow záznamů. Zcela zde chybí celkový popis prostředí, zejména k čemu se využívá skutečnosti, že sondy jsou postaveny před honeypoty a jaký je tedy přínos honeypotů. Jaký je např. rozdíl oproti situaci, kdy by byl na příslušném segmentu nebo IP adrese libovolné (adresovatelné) zařízení.

Autor uvádí, že vytvořený skript je v provozu několik měsíců. Neuvádí však téměř žádné zkušenosti s nasazením, vyjma případu detekce červa *Conficker*, k jehož detekci by ovšem zřejmě stejně posloužil pohled přímo do NetFlow, bez nutnosti použití honeypotů. V práci mi chybí popis, zda a jak jsou realizovány notifikace správců a možnost procházet historii zachycených spojení, což jsou vlastnosti požadované v zadání.

Práce není dobře strukturována. Např. kapitola o honeypotech s vysokou mírou interakce začíná popisem honeypotů s nízkou mírou interakce a jejich typickým představitelem *honeyd*. Podobně úvod kapitoly o nízkoúrovňových honeypotech uvádí další možné rozdělení honeypotů. Takové uspořádání je matoucí pro čtenáře a snižuje čitelnost celého celého textu. Celkově autor často sklouzává k popisu zbytečných podrobností, ale zanedbává popis širších souvislostí a kontextu. Ne-

dobře působí často opakované citace dvou knih. Na druhé straně se v práci objevují tvrzení, která nejsou podložená citacemi (např. použití honeypotů v komerčním prostředí). Práce zmiňuje projekt Inteligentní logovací server, ale neuvádí jeho bližší popis ani souvislost s představovanými výsledky.

Po celkovém zhodnocení předložené práce konstatuji, že práci lze uznat jako bakalářskou a navrhuji ji hodnotit známkou **D**.

V Brně, 9. června 2010 Daniel Kouřil