Hodnocení diplomové práce – oponent

Autor hodnocení:	Ing. Lukáš Kapičák
Vedoucí diplomové práce:	Ing. Pavel Nevlud
Oponenti:	Ing. Lukáš Kapičák
Téma:	Analýza síťových anomálií pomocí síťových statistik NetFlow
Verze ZP:	1
Student:	Bc. Václav Stefek

1. *Splnění požadavků zadání.*

   Náročnost řešení diplomové práce spočívala ve studiu problematiky analýzy síťového provozu. Diplomant otestoval veškeré nástroje uvedené v zadání pro analýzu síťového provozu a provedl základní konfiguraci těchto nástrojů. V diplomové práci postrádám přehledně zpracovaný šestý bod zadání, kde porovnání jednotlivých řešení nebylo dostatečně podrobné.

2. *Hodnocení formální stránky závěrečné práce.*

   Kapitoly diplomové práce na sebe logicky navazují. Rozsah diplomové práce a jednotlivých kapitol je dostačující. Jazyková stránka je na velmi špatné úrovni. V diplomové práci se vyskytují jak gramatické chyby, tak i hovorové výrazy.

3. *Hodnocení výsledků závěrečné práce.*

   Hlavním cílem diplomové práce bylo provést teoreticky popis IDS/IPS nástrojů. Tato část byla dostatečně zpracována. Diplomant také analyzoval pcap soubor a popsal NetFlow protokol. Na základě teoretických zjištění provedl diplomant instalaci, konfiguraci a otestování nástrojů Bro IDS a Suricata IDS. V diplomové práci postrádám ucelené zhodnocení výsledků testování a také podrobnější analýzu získaných dat. Nejednoznačnost výsledků umocňuje také fakt, že zde nebyly uvedeny hardwarové parametry počítačů, na kterých byly instalovány IDS/IPS systémy.

4. *Hodnocení práce z hlediska přínosu nových poznatků.*

   Diplomová práce nepřináší nové poznatky, přináší jen ucelený pohled na IDS/IPS systémy. Výsledky diplomové práce nejsou použitelné v praxi.

5. *Charakteristika výběru a využití studijních pramenů.*

   Výběr studijních pramenů je zvolen správně vzhledem k tématu diplomové práce. Převzaté prvky jsou správně odlišeny od vlastních výsledků a úvah.

6. *Otázky k obhajobě.*

   V diplomové práci uvádíte:
   "Například Bluetooth lze odchytávat pouze na systému linux." Můžete tuto skutečnost objasnit?

   V diplomové práci uvádíte:
   "Pokud toto pole zůstane prázdné a za předpokladu, že naše síťová karta je nastavena do promiscuous módu (zobrazí i data, která nejsou přímo určena nám) uvidíme všechna protékající data v dalším bloku, který se automaticky posouvá s přibývajícími daty." Jakým způsobem je možno získat data, která ,jak uvádíte, nejsou určená přímo nám?

   V kapitole zabývající se Netflow uvádíte:
   "Při 10000 aktivních tocích je využití CPU o 4% vyšší, při 65000 aktivních tocích je využití CPU vyšší dokonce o 16%." U jakého procesoru a jaké architektury tato skutečnost platí?

   V diplomové práci uvádíte:
   "Je zde zabudovaná podpora pro hardwarovou akceleraci a více vláknové zpracování, díky tomu dosahuje rychlosti zpracování dat až 10G/s v reálné síti." O jakou hodnotu se jedná?

   V diplomové práci uvádíte:
   "Stroje běží v aplikaci „VirtualBox“." Můžete tuto skutečnost blíže objasnit?

7. *Souhrnné hodnocení.*

   V případě podrobného zpracování této diplomové práce mohly výsledky sloužit jako ucelený pohled

na IDS/IPS systémy. Na základě získaných výsledků by pak bylo možno postavit základní zabezpečení počítačové sítě. Jelikož se však v diplomové práci vyskytuje velké množství nesrovnalostí a hlavně nedůsledné zpracování výsledků testování, jsou výsledky jen s obtížemi použitelné v praxi. Kvalitu diplomové práce také snižuje jazyková stránka, která je na špatné úrovni. Celkově hodnotím diplomovou práci jako dobrou.

Celkové hodnocení: dobře

Ostrava, 21.07.2016

Ing. Lukáš Kapičák