Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Jméno studenta: Miroslav Bartoš

Název práce: Analýza a optimalizace softwarových firewall na operačních systémech Linux

Autor posudku: Ing. Jan Štěpán

Cíl práce: Popsat tvorbu firewallu na operačním systému Linux a optimalizovat stávající řešení.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	A	**C**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☒	☐	☐
Zpracování teoretických aspektů tématu	☒	☒	☐	☐
Zpracování praktických aspektů tématu	☐	☒	☒	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☒	☐	☐
Hloubka a správnost provedené analýzy	☒	☒	☐	☐
Práce s literaturou	☐	☒	☐	☐
Logická stavba a členění práce	☒	☒	☐	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐
Formální úprava a náležitosti práce	☐	☒	☒	☐
Vlastní přínos studenta	☐	☒	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☒	☒	☐	☐

Dílčí připomínky a náměty:

Autor v práci pojednává o problematice tvorby firewallu na počítači s operačním systémem Linux a jeho praktickém nasazení. V úvodní kapitole vysvětluje, jaký je účel firewallu a je popsána historie vzniku této technologie. Jsou popsány všechny možné variace softwarových i hardwarových firewallů. Možná by bylo lepší popis konkrétního řešení v systému Linux poprvé zmínit až v dalších kapitolách, včetně detailů jako historie implementace firewall daemona netfiler.

Druhá kapitola pak analyzuje jak je firewall implementován v operačním systému Linux. Bylo by vhodné doplnit text uvádějící kapitolu pod hlavní nadpis. Nejprve se autor věnuje popisu pravidel pro přístup neboli ACL. Ty jsou součástí nejpoužívanějšího nástroje na tvorbu firewallu v os Linux, iptables. Další část kapitoly je věnována rozdílům mezi paketovými, aplikačními a stavovými filtry. Jsou shrnuty jejich výhody a jejich nevýhody.

Třetí kapitola popisuje běžné základní konfigurace firewall a to paranoidní nebo benevolentní. Také velmi detailně popisuje proces filtrování paketů a vysvětluje různé politiky při vyhodnocování ACL.

Velká část kapitoly popisuje různé síťové architektury lokálních sítí od těch nejjednodušších s jedním routerem až po velmi komplexní s demilitarizovanou zónou. Další část kapitoly ukazuje na útoky, kterým firewall díky svému principu zabránit nemůže. Poslední část naopak popisuje možné útoky, které je možné na firewall provést.

Na začátku čtvrté kapitoly je celkem zbytečně znovu zmíněna historie vývoje firewall v jádře systému Linux. Dále je ukázáno jak pracovat s iptables. I tato část je již jednou zmíněna, a to v druhé kapitole. Podkapitoly se věnují rozdílům implementace mezi nejrozšířenějšími distribucemi systému Linux, a to Ubuntu a Fedora. V textu jsou ukázky konfigurace jak tradičně přes konzoli i přes výchozí GUI aplikace jednotlivých distribucí.

Pátá kapitola se zaměřuje na problematiku nasazení firewall v malých společnostech. Autor dobře popisuje výhody a nevýhody použití levného routeru místo dedikovaného počítače. Zmiňuje i náklady na provoz u obou řešení. Také ukazuje, že i při použití staršího PC nejsou znatelné propady v propustnosti sítě. Další část kapitoly ukazuje aktuální stav v nejmenované firmě, kde autor nasazuje nový firewall na systému Linux. Zmiňuje, že současný stav ve firmě není zdaleka ideální a jejich architektura obsahuje několik zranitelných míst.

Kapitola šestá pak pojednává o implementaci nového firewallu na distribuci Ubuntu, který nahrazuje původní router. Nová síťová architektura s demilitarizovanou zónou značně optimalizuje předchozí stav. Kroky popsané v této kapitole mohou být využity jako ukázka pokročilého zabezpečení pro malé až střední firmy. Poslední část této kapitoly testuje původní i nové řešení a ukazuje velké zvýšení bezpečnosti. Závěr práce pak vše sumarizuje a navrhuje i alternativní možnosti konfigurace brány firewall na systému Linux.

Práce obsahuje stylistické chyby, jako například obrázek vložený uprostřed věty a chybějící prázdné řádky za obrázky. Na velké množství obrázků není vůbec odkazováno v textu a tabulky mají podivné formátování. Popisky tabulek by měli být nad tabulkou a ne pod tabulkou. Autor cituje svědomitě a celkový počet zdrojů vzhledem k tématu lze hodnotit jako dostatečný. Nevyhnul se citování z Wikipedie, ale tyto citace jsou podloženy i dalšími zdroji.

Celkové posouzení práce a zdůvodnění výsledné známky:

Práce obsahuje chyby spojené nejvíce s formální stránkou a stylistikou. Obsahově je práce dobrá, podrobně vysvětluje teorii a vše doplňuje praktickými ukázkami. Některé části textu se ale bohužel zbytečně opakují. Výsledky práce je možné využít při implementaci zabezpečení v malých až středních firmách.

Otázky k obhajobě:

Lze stejnou architekturu firewallu implementovat i na Windows?

Práci doporučuji k obhajobě.

Navržená výsledná známka: C - velmi dobře

V Hradci Králové**, dne 29. srpna 2016**

podpis