Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Martin Šeminský** **Oponent:** **Ing. Josef Kaderka, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2009/2010**

Téma diplomové práce: **Počítačová síť malé a střední organizace**

Hodnocení práce:
Na základě podrobného prostudování diplomové práce Bc. Martina Šeminského (dále diplomanta) konstatuji: Předloženou diplomovou považuji za úplnou. Její téma hodnotím jako velmi aktuální, zabývá se konkrétními problémy jak do šířky, méně už do hloubky. Vlastní řešené úkoly pokládám za středně obtížné, neboť diplomant musel zvládnout širokou škálu odborných témat jak po stránce teoretické, tak především po stránce praktické. Domnívám se, že všechny dílčí požadavky dané „Zásadami pro vypracování“ byly splněny. Diplomovou práci považuji za přínosnou. Je z ní zřejmé, že diplomant je schopen kvalitní a samostatné práce v oblasti počítačových sítí, bezpečnosti a správy operačních systémů Windows. Po stránce formální považuji práci za plně vyhovující. Za velmi pozitivní rys považuji její vypracování v jazyce anglickém a to v dobré kvalitě.
Některé dílčí připomínky:

15	Bezpečnostní politika není jen seznam bodů.
22	Cabling jako „nejdelší trasa“? Co bezdrátové sítě a speciálně satelitní spoje?
22	Switchboard – tento pojem odpovídá spíše telefonnímu prostředí
27	Switch nepracuje s ARP tabulkou, ale s tabulkou MAC adres
28	Není jasné, co je myšleno „traffic between root input/output …“, ledaže by se jednalo o útok vůči protokolu Spanning Tree; to ovšem v textu není uvedeno.
28, 29	Úvaha o „privilegované síti“ a jejím nastavení je poněkud zcestná. Předmětem nastavení budou vždy konkrétní zařízení, nikoliv abstraktní síť. Zastávám názor, že by směrovače při volbě zabezpečení neměly být děleny na méně a více důležité. Snadno pak dojde k chybě.
29	Obecně neplatí, že lze rozbít každé heslo
29	Úvahy o šifrování heslech neplatí obecně a pro každý směrovač. V praxi směrovač nikdy nemá vlastní hešovací algoritmus, nýbrž používá některý standardní (např. relativně překonaný MD5). Nepoužívá se náhodné číslo, ale např. údaj odvozený od aktuálního času, který poslouží společně s heslem jako vstup pro hešovací algoritmus („solení“ hesel).

V rámci obhajoby by měl diplomant objasnit:

- Jaký podmínky je třeba dodržet, aby bylo heslo (resp. šifra) zaručeně nerozluštitelné?

- Jak vidí perspektivu nasazení protokolu IPv6 a jaké bezpečnostní implikace toto bude mít v přechodovém období?

Celkové hodnocení práce:
Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 22. 6. 2010 Podpis oponenta diplomové práce