Oponentský posudek diplomové práce

Jméno studenta: Bc. Pavel Rypien

Název práce: Zabezpečení a analýza útoků na firemní síť.

Autor se ve své práci zaměřuje na zabezpečení firemní sítě zejména proti útoku z vnější či vnitřní zóny. Pro účely analýzy a testování navržených řešení autor navrhl počítačovou firemní síť, pro kterou následně představil potenciální způsoby zabezpečení. V první části práce student analyzoval možnosti útoků, jednotný vnější přístup a omezení dostupných služeb v různých bezpečnostních úrovních sítě. V úvodu práce se autor také stručně věnuje problematice základních principů TCP/IP sítí, ale bez zřejmých souvislostí s navrhovaným způsobem zabezpečení. I v dalších částech práce je patrná snaha autora představit velké množství běžně používaných síťových diagnostických nástrojů, či bezpečnostních rizik. Pro tuto část je bohužel charakteristická přílišná stručnost. Každá z vyjmenovaných hrozeb by si jistě zasloužila mnohem větší prostor, případně více odkazů na vhodnou literaturu. V této části se také objevuje velké množství deklarativních tvrzení bez doložení (např.: na Internetu lze najít spoustu stránek…, Spousta síťových zařízení má nastaveno…).

Pátá kapitola se věnuje vlastnímu návrhu lokální sítě. Jsou zde uvedeny základní vlastnosti sítě. Z popisu však není zřejmé, zda se jedná o dokumentaci stavu již existující sítě, či požadavky na síť nově navrhovanou. Případné požadavky také nejsou dostatečně analyzovány (počty uživatelů, typy služeb, datové toky, personální politika zabezpečení, agregace diagnostických informací, atd.).

Popis zabezpečení jednotlivých služeb je nedostatečný. Nejsou diskutovány způsoby zabezpečení použitých OS, globální konfigurace jednotlivých síťových služeb (démonů) jsou uvedeny pouze formou konfigurací v příloze bez bližšího zdůvodnění jednotlivých záznamů. LDAP se omezuje pouze na hrubý popis bez politiky uživatelských účtů. Další služby nejsou diskutovány vůbec, ačkoli v návrhu sítě na str. 4. jsou například tři blíže nespecifikované VLAN sítě, VoIP prvky, bezdrátové prvky a mnohé další. DHCP, IPv6 a další služby chybějí.

Stylistická úroveň práce je na dobré úrovni. Zadaný cíl práce – návrh vnitropodnikové sítě byl splněn, ale zasloužil by si v popisu mnohem detailnější prostor.

Otázky:

1. Na straně 12 klasifikujete potenciální útočníky sítě. Jak byste ve své navržené síti řešil problematiku RAP umístěné zaměstnanci.
2. Specifikujte blíže topologii VLAN a příslušnost jednotlivých služeb do VLAN, včetně VPN přístupu.

Vzhledem k výše uvedeným připomínkám **doporučuji práci k obhajobě** a navrhuji klasifikační stupeň: **velmi dobře mínus**.

Pardubice, 6.9.2012 Ing. Martin Dobrovolný, Ph.D.