Oponentský posudek diplomové práce

Analýza zabezpečení podnikových sítí s protokolem IEEE 802.1X

Student: Bc. Martin Bubeník, Univerzita Pardubice, Fakulta elektrotechniky a informatiky

Předložená diplomová práce má 104 stran (včetně příloh), je rozdělena na pět kapitol, závěr a tři přílohy. Úvodní kapitola je, přirozeně, popisná a shrnuje standardy IEEE 802.11 a 802.1X týkající se bezdrátových sítí. Zaměřuje se především na mechanismy zabezpečení přístupu od nejjednodušších a nejstarších (skrývání SSID, WEP) po současné standardy (WPA2) včetně popisu protokolů. V této části student již uvádí některé slabiny mechanismů. Stať je napsána přehledně, pouze některé pojmy by mohl student lépe definovat, např. v kapitole 1.3 adresu MAC: *„Skládá se z 6 dvojic kombinací čísel a písmen oddělených zpravidla dvojtečkou či pomlčkou. V rámci MAC adresy první 3 dvojice označují výrobce bezdrátového zařízení, další 3 pak jeho identifikaci.“* Na úrovni diplomové práce bych očekával definici typu „adresa MAC je 48 bitové pole“.

Druhá kapitola podrobně rozebírá bezpečnostní rizika jednotlivých mechanismů uvedených v kapitole 1, na které se odkazuje. Je diskutabilní, zda by nebylo vhodnější uvést všechna rizika souhrnně již v kapitole 1 nebo naopak uvést všechna v kapitole 2. K obsahové stránce nemám připomínky.

Další kapitola se zabývá stručně účelem a principy bezpečnostních auditů IT technologií. Student se odkazuje na obecnou metodiku OSSTMM a definuje vlastní metodiku auditu zaměřenou na bezdrátové sítě. Při tvorbě metodiky, tj. návrhu testů, vychází z požadavku pokrytí hrozeb, které analyzuje v kapitole 1 a 2. Ve čtvrté kapitole již popisuje jednotlivé testy podrobně a uvádí přehled nástrojů z distribuce Kali Linux, které budou v jednotlivých krocích testů využity. Pátá kapitola je zaměřena ryze prakticky, tj. na vybraný přístupový bod jsou aplikovány kroky testů; diplomant popisuje detailně spouštění jednotlivých nástrojů (včetně parametrizace) a uvádí výsledky testů. Na str. 83 práce v podkapitole „Konfigurace notebooku útočníka“ student uvádí: *„Notebook útočníka pro pasivní odposlech je vybaven linuxovou distribucí Kali Linux s doinstalovanými aplikacemi EAPeak a EAPscan rozšířené o vlastní implementaci generování grafických HTML reportů“*. Je velká škoda, že v práci student dále vůbec nepopisuje toto vlastní rozšíření, přitom podrobný popis tohoto rozšíření by prokázal tvůrčí schopnost studenta i v oblasti programátorské. Závěr práce obsahuje shrnutí a nechybí doporučení pro konfiguraci sítě.

Po jazykové stránce je práce na dobré úrovni, srozumitelná pro čtenáře. Může sloužit jako vhodný návod pro provedení jednoduchého bezpečnostního testu.

Zadání diplomové práce bylo splněno, práci doporučuji k obhajobě a hodnotím známkou **C (dobře), číselně 2.**

Otázky k obhajobě:

1. Popište podrobněji pojem "sdílené tajemství", které používáte na str. 82.
2. Popište Vaše rozšíření, o kterém píšete v práci na str. 83.
3. Znáte nějaké mezinárodní normy týkající se bezpečnosti informačních technologií?

V Praze dne 6. 6. 2018

doc. Ing. Vít Fábera, Ph.D.
Ústav aplikované informatiky v dopravě
Fakulta dopravní ČVUT

Fábera Vít