Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Jan Rydlo

Název práce: Využití penetračního testování v bezdrátových sítích

Autor posudku: Ing. Jan Štěpán

Cíl práce: Představit možnosti využití principů a postupů penetračního testování pro ověření a zajištění bezpečnosti bezdrátových sítí.

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:

Práce obsahuje stylistické chyby hlavně v podobě střídání 1. osoby jednotného číslo, 1. osoby množného čísla a neutrálního stylu. Dále autor zbytečně několikrát po sobě zmiňuje název citované knihy, i když ji předtím představil v literární rešerši. K samotnému obsahu práce již nemám žádné dílčí připomínky. Bylo by také vhodné řadit zdroje podle pořadí výskytu v textu.

Celkové posouzení práce a zdůvodnění výsledné známky:

Práce se zabývá problematikou penetračního testování a jeho využití při zjišťování zranitelností bezdrátových sítí. V úvodu autor definuje cíle práce, tedy v teoretické části představit principy penetračního testování, definování pojmů a výběr vhodných nástrojů. V praktické části pak bude využívat Linuxovou distribuci Kali Linux pro testování bezpečností domácích i firemních sítí.
V druhá kapitola obsahuje literární rešerši. Autor zdůvodňuje, které knihy si vybral pro zkoumanou problematiku. Knihy jsou velmi dobře zvoleny a jsou napsány odborníky v oboru testování a bezpečnosti. Třetí kapitola pak ukazuje teoretické principy penetračního testování. Nejdříve autor definuje pojmy etický hacking, etický hacker a penetrační testování. Dále popisuje druhy

penetračního testování. Poslední část kapitoly velmi detailně popisuje všechny rozšíření standardy pro rámce penetračního testování. Čtvrtá kapitola představuje populární softwary pro penetrační testování bezdrátových sítí. Jedná se jak o nástroje pro monitoring, tak i pro exploitaci, kompletní penetrační testy a také populární Linuxové distribuce zaměřené na síťovou bezpečnost. V páté kapitole pak autor ukazuje technologii WiFi (standard 802.11), strukturu jeho rámců, možnosti zabezpečení a ověřování. Součásti kapitoly je i podrobný návrh postupu penetračního testování se všemi jeho fázemi. Kapitolu zakončuje seznam několika útoků, které je možné v bezdrátových sítích provést, včetně jejich dopadů. Předposlední kapitola je pak již ryze praktická a autor ukazuje na routeru TL-WR811N (populární router, který instalují i poskytovatelé internetového připojení ke klientům) potencionální bezpečnostní rizika. Ukazuje, že WEP zabezpečení, skryté SSID i filtrování MAC adres jsou už zastaralé techniky, které je možné jednoduše prolomit. Další část kapitoly pak ukazuje útoky proti přístupovým bodům a věnuje se i zabezpečení WPA/WPA2. Bohužel autor neměl k dispozici síť s enterprise ověřováním RADIUS a nemohl otestovat její zranitelnosti. V závěru pak sumarizuje zjištěné poznatky a opakuje, že WEP zabezpečení je nedostatečné, stejně jako slabý PSK klíč.
Práce je tedy po obsahové stránce velmi kvalitní, autor projevil velkou znalost dané problematiky a práci tak pouze mírně sráží stylistické a gramatické chyby.

Otázky k obhajobě:

Jaké informace je možné získat ze sítí s RADIUS ověřováním?

Práci doporučuji k obhajobě.

Navržená výsledná známka: B - výborně-velmi dobře

V Hradci Králové**, dne 5. září 2016**

podpis