Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Jméno studenta: Bc. Aleš Lajvr

Název práce: Simulace síťových útoků za využití Kali Linux

Autor posudku: Ing. Tomáš Svoboda, Ph.D.

Cíl práce: Cílem práce bylo provést analýzu a podrobný nástrojů pro útoky na bezdrátové sítě s využitím nástrojů v distribuci Kali Linux.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**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)	☐	☒	☐	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 13%. Po ručním přezkoumání lze konstatovat, že se jedná o citace legislativy a všeobecně uznávaných norem.

Dílčí připomínky a náměty:

Oponent práce má k předložené práci jednu připomínku. Cíle práce nejsou jednoznačně formulované. Autor v rámci anotace uvádí: *„Tato práce se zabývá kybernetickou bezpečností na úrovni zabezpečení síťových prvků v drátových a bezdrátových sítích. Jejím cílem je poukázat na vybrané zranitelnosti a možnosti jejich zneužití pomocí nástrojů Kali Linux, a především informovat čtenáře, jak zneužití předejít.“* Lze se tedy pouze domnívat, že cílem práce bude představení a praktické ověření scénářů pro penetrační testování bezdrátových sítí.

Celkové posouzení práce a zdůvodnění výsledné známky:

Diplomová práce je svým tématem velice aktuální, neboť problematika penetračního testování v rámci etického hackingu je vzhledem k nárůstu kybernetických útoků v posledních letech akcentována. Autor nejprve představuje základní pojmy z oblasti kybernetické bezpečnosti, včetně organizačních a technických opatření a nového zákona o kybernetické bezpečnosti. Součástí druhé kapitoly je i přehled

taktik a technik dle MITRE ATT&CK matice, která je uznávaným standardem v oblasti identifikace taktik a technik využívaných v oblasti penetračního testování a etického hackingu.
Kapitola 3. obsahuje přehledný a vyčerpávající seznam široce využívaných nástrojů pro simulaci kybernetických útoků v prostředí bezdrátových sítí. 4. kapitola obsahuje popisy možných útoků na bezdrátové sítě. Kapitola je přehledně zpracována. Oceňuji zpracování této kapitoly, kde autor nejprve představuje typ útoku, možnost zneužití zranitelnosti pro úspěšné provedení útoku a doporučení mitigačních opatření úspěšné provedení útoku.
V praktické části práce se autor na věnuje simulaci útoků na bezdrátové sítě s využitím nástrojů představených v teoretické části práce. Jednotlivé scénáře jsou přehledně zpracovány včetně prezentace výsledků testů. Praktická část práce je dále široce využitelná v rámci výuky na FIM UHK v oblasti kybernetické bezpečnosti se zaměřením na penetrační testování a bezpečnost bezdrátových sítí.

Závěrem lze konstatovat, že práce naplnila požadavky kladné na diplomovou práci.

Otázky k obhajobě:

Nejsou

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové**, dne 6. května 2024**

podpis