



## POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

**Jméno studenta:** Bc. Aleš Lajvr  
**Název práce:** Simulace síťových útoků za využití Kali Linux  
**Autor posudku:** doc. Mgr. Josef Horálek, Ph.D.  
**Cíl práce:** Cílem práce bylo provést analýzu a podrobný popis nástrojů pro síťové útoky dostupných v prostředí Kali Linux a navrhnout a sestavit sadu úloh pro ověření zabezpečení sítě.

Povinná kritéria hodnocení práce	Stupeň hodnocení (známka)					
	A	B	C	D	E	F
Práce svým zaměřením odpovídá studovanému oboru	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vymezení cíle a jeho naplnění	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování teoretických aspektů tématu	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování praktických aspektů tématu	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adekvátnost použitých metod, způsob jejich použití	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hloubka a správnost provedené analýzy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Práce s literaturou	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logická stavba a členění práce	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jazyková a terminologická úroveň	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Formální úprava a náležitosti práce	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vlastní přínos studenta	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Využitelnost výsledků práce v teorii (v praxi)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 13%. Po analýze výsledků konstatuji, že se jedná zejména o citované definice legislativy a norem.

### Dílní připomínky a náměty:

Vedoucí práce nemá žádné závažné připomínky k předložené práci.

### Celkové posouzení práce a zdůvodnění výsledné známky:

Téma diplomové práce v oblasti etického hackingu je aktuální a setkáváme se s ním na každodenní bázi. Autor práci rozdělil do teoretické a experimentální části. V kapitole 2 autor představuje aktuální stav kybernetické bezpečnosti, kdy nejdříve představuje vybrané výzkumné práce související s tématem kybernetické bezpečnosti a vysvětlí základní pojmy. V další části se pak zabývá situací z pohledu národní i evropské legislativy, včetně porovnání se situací v USA. Dále představuje přehled hackerských taktik a technik. V následující kapitole pak představuje přehled nejvyužívanějších nástrojů distribuce Kali Linux, které je možné využít k simulaci síťových útoků s cílem ověření skutečného stavu zabezpečení drátových i bezdrátových sítí. Konkrétně byly představeny nástroje Nmap, Wireshark, Aircrack-ng, Wifite, Ettercap, Yersinia, Scapy a Macof. Kapitola 4 se pak věnuje aktuálním vědeckým pracím na téma síťových útoků vůči drátovým i bezdrátovým sítím. V podkapitolách je nejprve uvedena

vybraná zranitelnost následovaná popisem způsobu, jakým lze danou zranitelnost zneužít, a v závěru podkapitol jsou doporučeny možnosti obrany před zneužitím. Experimentální ověření bezpečnostních rizik v laboratorním prostředí je pak podrobně popsáno v kapitole 5. S pomocí nástrojů představených v kapitole 3 autor provedl simulaci útoků představených v kapitole 4. Podrobné shrnutí výsledků pak autor uvádí v kapitole 6.

Autor naplnil všechny vytyčené cíle a práce naplnila požadavky kladné na diplomovou práci.

**Otázky k obhajobě:**

Nejsou

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: A**

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

---

**podpis**