Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Martin Mičkech

Název práce: Analýza využitelnosti simulačních nástrojů pro síťovou bezpečnost

Autor posudku: doc. Mgr. Josef Horálek, Ph.D.

Cíl práce: Cílem práce bylo zmapovat možnosti využitelnosti simulačních nástrojů pro testování síťové bezpečnosti a na vybraných řešeních navrhnout a realizovat sadu laboratorních úloh zaměřených na síťovou bezpečnost.

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: 1%.

Dílčí připomínky a náměty:

Vedoucí práce nemá žádné závažné připomínky k předložené práci.

Celkové posouzení práce a zdůvodnění výsledné známky:

Bakalářská práce se zabývala problematikou testováním a simulací počítačových sítí s důrazem na jejich zabezpečení. V teoretické části práce autor seznámil čtenáře s konkrétními nástroji určenými pro simulaci, či testování efektivity provozu a bezpečnosti počítačových sítí, přičemž byli zdůrazněny jejich přednosti a praktické využití. Další kapitola práce byla věnována kybernetickým útokům, kdy autor nejdříve seznamuje s danou problematikou představením několika nejčastěji se vyskytujících typů útoků a popisuje způsoby jejich provedení. Dále podrobněji seznamuje s několika konkrétními hrozbami dle vrstev ISO/OSI. U každé z vrstev byli nejprve popsány protokoly a slabiny, které bývají častým cílem kybernetických útoků. Dále se práce zaměřila na konkrétní útoky, které cílí na identifikovaná slabá místa jednotlivých vrstev sítě. Tyto útoky byly detailně popsány včetně jejich

metodiky, cílů, potenciálních dopadů a v neposlední řadě byli zmíněny způsoby, jak se proti daným útokům bránit.
V praktické části práce se autor zaměřil na analýzu možností nástroje společnosti Fortinet Security Fabric, kdy autor podrobně popisuje funkčnosti nabízených nástrojů a možnosti jejich konfigurace. Autor mimo jiné zkoumá prvky určené pro správné fungování síťové infrastruktury ze strany firewallu, které zahrnují konfiguraci jednotlivých rozhraní a firewall politiky, nebo nastavení DNS. Dále se autor věnuje nástroji pro centrální monitorování a správu počítačové sítě pomocí firewallu FortiGate. Pal navazují kapitoly FortiSwitch a FortiAP zaměřené na možnosti nabízené těmito zařízeními v rámci Security Fabric. Přepínač FortiSwitch pak nabízel především možnost segmentace pomocí VLAN a NAC, zatímco přístupový bod FortiAP poskytl možnost bezpečného bezdrátového připojení k počítačové síti. Posledním probíraným tématem bylo podrobné popsání bezpečnostních profilů poskytujících testované počítačové sítí co nejlepší možné zabezpečení.
Práce poskytuje ucelený pohled na problematiku kyberbezpečnosti, simulačních a testovacích nástrojů počítačových sítí a jejich zabezpečení. Zahrnuje důkladné seznámení s teoretickými základy těchto oblastí, včetně konkrétních nástrojů, detailního popisu kybernetických útoků a možností obrany proti nim. Nabízí také detailní pohled na možnosti Security Fabric. Důkladně zkoumá funkčnost a možnosti konfigurace poskytovaných nástrojů s důrazem na efektivní zabezpečení počítačové sítě.
Je nutné ocenit, nadstandardní čas, který student věnovat praktickému testování nástroje Fortinet Security Fabric, kdy všechny uvedené testy a konfigurace byly několikanásobně testovány a analyzovány. Autor tak zcela naplnil vytyčené cíle a přeložená práce splňuje požadavky kladené na bakalářskou práci.

Otázky k obhajobě:

Jaké nástroje a možnosti Security Fabric byste doporučil využít např. v prostředí univerzitní sítě?

Práci doporučuji k obhajobě.

Navržená výsledná známka: A

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

podpis