POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Využití OpenAI analýzy datových toků pro potřeby kybernetické bezpečnosti
Jméno autora:	Filip Pavel
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra telekomunikační techniky
Oponent práce:	Ing. Josef Koumar
Pracoviště oponenta práce:	Fakulta informačních technologií (FIT)

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Hlavním bodem tématu práce je zaměření se na problematiku kybernetické bezpečnosti malé a střední sítě. Jedná se o téma, které vyžaduje poměrně rozsáhlé studium existujících řešení. Úkolem je navrhnout asistovanou analýzu incidentů založenou na jazykovém modelu OpenAI. Jedná se o zajímavou oblast, která by mohla najít využití v praxi právě v malých a středních firmách. Téma považuji za náročnější kvůli množství informací k nastudování.

Splnění zadání **splněno s většími výhradami**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Student v textu práce adresuje všechny body ze zadání, a tak se na první pohled jeví, že je zadání splněno. Nicméně při bližším zkoumání zjišťujeme, že informace, které měl student nastudovat jsou pojaty na velice vysoké úrovni abstrakce. Student nejde do detailů v žádném v teoretických bodů, přičemž sepsané informace obsahují závažné chyby. Celkově práce působí dojmem, že student termínům nerozumí. Očekával bych v práci rozuzlení, co tedy je doporučeno malým a středním firmám, které nemohou mít SOC tým. Celá řada kapitol působí dojmem výkřiků do tmy. Celkově je práce velice chaotická. I když po formální stránce student adresuje vše ze zadání v dílčích kapitolách, tak na sebe kapitoly nenavazují a neinteragují spolu. I díky tomu je závěr práce pojatý jako: nastudoval jsem tyto věci v těchto kapitolách a s OpenAI jsem provedl tento experiment, který nemá významné výsledky. Proto v celkovém pohledu je sice zadání splněno, ale s velkými výhradami k tomu, jak jej student splnil.

Zvolený postup řešení **částečně vhodný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student studoval teoretickou část převážně z online zdrojů i přes to, že v této oblasti je publikováno velké množství publikací v mezinárodních konferencích a časopisech. Dále autor zmiňuje RFC dokumenty, což považuji za jeden z nejvíce vhodných zdrojů pro tuto problematiku, nicméně je necituje a informace z nich nejspíše nečerpal, což je veliká škoda a text práce tak utrpěl fatální chyby po odborné stránce. Jako praktickou část práce se student zaměřil na nástroje Suricata, Softflowd, a nProbe. Tyto nástroje byly zvoleny v hodně vzhledem k dnešním trendům, bohužel není přesně popsáno, jak tyto nástroje by měli být nasazeny do reálné sítě.

Odborná úroveň **E - dostatečně**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Začal bych citací ze studentovy práce: „Toto téma jsme zvolil z důvodu nedostatku veřejně dostupných doporučení zabezpečení.“ Takové tvrzení je velice zavádějící, protože se tomuto tématu věnuje obrovské množství příspěvků v nejrůznějších blozích, časopisech, výzkumných publikací i oficiálních dokumentech vydaných státní správou. Navíc tuto větu student napsal i přes to, že část jeho práce zabývajícím se „doporučeními“ (kapitola 4.Vhodný bezpečnostní standard) je čerpaná z jediného veřejně dostupného dokumentu: „Minimální bezpečnostní standard“ sepsaná organizacemi NÚKIB, NAKIT, a Ministerstvem vnitra České republiky. Student však v této kapitole navíc napsal: „Na základě rešerše jsem jako vhodné doporučení pro počáteční implementace vybral doporučení NÚKIB …“, ale žádné informace o této rešerši nám

nedal. Nevíme kolik, kde a jaké studoval materiály, ze kterých tento vybral, a hlavně nevíme proč jej vybral. Tato kapitola je také jediná, které nelze nic po odborné stránce vytknout, protože je celá převzatá (správně ocitovaná) právě ze zmíněného dokumentu. Zbytek práce obsahuje v odborné stránce značné chyby a vykazuje znaky nepochopení popisovaných termínů. Navíc mnohé termíny jsou často vysvětleny jedním kraťoučkým odstavcem, který termín příliš neosvětluje.

Například v kapitole 6. Místní infrastruktura, student do zabezpečení sítě chybně umístil antivirus a anti-malware software, a to i přes to, že ve stejném číselném seznamu má Zabezpečení koncových bodů.

Jeho popis VPN začíná větou „VPN je síť, přes kterou prochází zašifrovaná komunikace, tato síť není viditelná pro ostatní.“. Tato věta indikuje, že student neví, co přesně je VPN. Což dokazuje i jeho další tvrzení o VPN: „Každé zařízení má šifrovací kódy“, což mi připomnělo spíše špiónský film Mission: Impossible - Rogue Nation (2015) než VPN.

Dalším tvrzením je „Intrusion Prevention System je mechanismus, …“, což je nepochopitelné zadefinování IPS, jelikož se jedná o systémy. Zároveň student zmiňuje k IPS „Zároveň při detekování podezřelého chování vytváří upozornění a loguje veškeré chování systému.“, což je zavádějící. IPS aktivně potlačuje detekovaný útok. Další zavádějící věta porovnání IPS a IDS je „Intrusion Detection System je na druhé straně levnější řešení, …“.

Dále u popisování portů na transportní vrstvě TCP/IP modelu, student zmiňuje: „Čísla portů jsou od 0 do 65535, nejznámější jsou TCP porty (0 až 1023), které jsou využívány pro systémové služby [17].“. Toto tvrzení je naprosto špatně. Navíc v citovaném zdroji [17] (což je https://www.avast.com/business/resources/what-is-port-scanning#pc) je to popsané správně a úplně jinak, než student sepsal. Není možné, aby z tohoto zdroje student získal tyto informace.

V textu se třeba je i věta „Pro mé použití jsem zvolil nástroj Suricata.“, přičemž není vysvětleno, co je to „mé použití“.

Dalším nepřesným a zavádějícím popisem je DoS a DDoS, u kterých student tyto pojmy zaměňuje viz: „DoS neboli odepření služby. Jedním z možných způsobů realizace tohoto útoku je například využití botnetů.“ a „DDoS – Distributed Denial of Service probíhá na základě zahlcení cílového serveru nebo sítě velkým množstvím požadavků.“

Taktéž kapitola 9.1 Síťový datový tok je plná nepřesností, zavádějícími až nepravdivými informacemi. Například: „UDP a TCP jsou protokoly pro přenos dat v sítích. Nejzákladnější data těchto datagramů jsou: IP adresa odesílatele a adresáta, Port odesílatele a adresáta, Číslo protokolu“, ale UDP datagram, tzn. segment transportní vrstvy TCP/IP modelu neobsahuje IP adresy. Tato část dokonce není ocitovaná, a pokud bychom uvažovali, že citace [23], která se objevuje ve dvou odstavcích pod tímto tvrzením, je zdrojem, tak bychom byli zklamáni, protože tento zdroj takové informace samozřejmě neobsahuje.

Opět zavádějící tvrzení je v odstavci: „Prozatím poslední verze je NetFlow verze 9, která byla vydána v roce 2004 a již podporuje IPv6 či možnost sběru informací o využívání šířky pásma pro jednotlivé aplikace. Technicky je poslední verze 10, která byla vydána roku 2013. Je taktéž často označována jako IPFIX, nicméně jsou to dva rozdílené standardy. [24]“. Studentovo tvrzení, že poslední verze NetFlow je technicky 10 je zavádějící, protože IPFIX je otevřený standard jenž vzniknul z NetFlow v9 a pouze se v komunitě čas od času označuje jako NetFlow v10. Což by student zjistil kdyby si svůj vlastní zdroj [24] lépe prostudoval, protože se v něm doslova píše: „IPFIX is an IETF standard flow record format that is very similar in approach and structure to NetFlow v9 (see more on NetFlow version numbering below). It is sometimes called “NetFlow v10” since IPFIX plays a key role in coalescing all NetFlow variants and equivalents as the standards process evolves the IPFIX specifications over time.“

Dále student uvádí „NetFlow umožňuje odhalit potencionálně slabá místa sítě, jakožto nezabezpečené porty či zařízení.“, ale takové tvrzení je zavádějící. Analýza NetFlow záznamů může sice takové odhalení přinést, ale sám osobě bez další analýzy toto neumožňuje.

Praktická část práce po odborné stránce je v pořádků, ale jedná se pouze o seznam kroků, jak zprovoznit software Suricata. Nicméně není diskutována volba parametrů, pouze je oznámeno, že tyto parametry student zvolil.

Formální a jazyková úroveň, rozsah práce **D - uspokojivě**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Jazykově je práce velice zvláštní. Podstatné části, především v prvních 30 stránkách působí dojmem, že jsou buď špatně přeložené z angličtiny nebo napsané umělou inteligencí. Taktéž kapitoly na sebe příliš nenavazují a špatně se sleduje myšlenkový pochod studenta.

Některé kapitoly vypadají natolik uměle, že jsem zkusil nástroje pro odhalení jazykového modelu. Je nutné poznamenat, že tyto nástroje samy o sobě nemůžou prokázat, že by student skutečně použil jazykového modelu pro napsání práce, jelikož se jedná o DL klasifikátor, která samozřejmě obsahuje chybovost, jak se píše i zde: https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text v sekci Limitations. Nicméně při použití tohoto modelu (https://platform.openai.com/ai-text-classifier) u podstatných částí práce tento klasifikátor vypíše výsledek „The classifier considers the text to be likely AI-generated.“.

Výběr zdrojů, korektnost citací **C - dobře**

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Studijní materiály studenta jsou vesměs online články na různých blozích. Nicméně k samotné citační etice studenta mám výhrady. Při namátkové kontrole u termínů, které byly na první pohled špatně či podány zavádějícím způsobem bylo zjištěno, že student u nich danou citaci pouze umístil, ale nečerpal z ní, protože dané závěry či definice zdroj neobsahuje.

Příkladem je již zmíněná citace [17] u textu: „Čísla portů jsou od 0 do 65535, nejznámější jsou TCP porty (0 až 1023), které jsou využívány pro systémové služby [17].“. V citovaném zdroji [17] (což je https://www.avast.com/business/resources/what-is-port-scanning#pc) je to popsané správně a úplně jinak, než student sepsal. Není možné, aby z tohoto zdroje student získal tyto informace.

Dalším příkladem je porovnání IPS a IDS, kde student napsal „Intrusion Detection System je na druhé straně levnější řešení, které nedokáže aktivně zastavit útok, ale dokáže upozornit podezřelé chování [16]“. Nicméně v [16] se vůbec nepíše nic o tom, že by IDS byly levější řešení, jejich závěrem je, že se mají IPS a IDS kombinovat, což student v textu zmiňuje v jiném odstavci, ale už to tvrzení neocitoval.

Další spíše špatnou práci s citacemi je „Umožňuje TCP skenování, UDP skenování, SYN skenování, ARP skenování či další [18]“ kde student odkazuje na specifickou stránku o základním fungování NMAP, ale na této stránce není pospané, že by umožňoval například ARP skenování. Student by měl citovat přesně stránku kde se zmiňují o ARP skenu nebo celou dokumentaci NMAP (https://nmap.org/book/toc.html).

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Úroveň teoretické části práce je mizerná. Praktická část o Surikata nepřináší nic nového. Praktická část o využití OpenAI pro alerty ze Surikata je zajímavá, ale bohužel krátká (2 A4 experimentů). Rozsah práce (Od úvodu po závěr) je 44 stran, nicméně dohromady přibližně 11 stran (sečteme-li i nepopsané půl a čtvrt stránky) není popsáno. I tak je, ale rozsah bakalářské práce v normě.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Závěrečná práce je z mého pohledu podprůměrná. Obsahuje skoro bych řekl kritické chyby v teoretické části a vypovídá dojmem, že student klíčové termíny nepochopil. Navíc obsahuje špatnou práci s citacemi, které neobsahují citovaný text. Navíc praktická část i přes věcnou správnost a zajímavost je poněkud kratší a nezachraňuje celkový pohled na závěrečnou práci. Proto jsem nucen hodnotit klasifikačním stupněm D.

Otázky k obhajobě, které by měl student zodpovědět:

1) Měla by firma používat cloudové řešení nebo své vlastní? Popište pro malou i střední firmu odděleně a své závěry zdůvodněte.
2) Jsou všechna doporučení NÚKIB v dokumentu „Minimální bezpečnostní standard“ pro malou i střední síť proveditelná?
3) Věříte, že bude v budoucnu možné využít jazykový model OpenAI Vámi popsanou metodou využít v praxi pro kybernetickou bezpečnost malých a středních firem? A jak jej firmy nejspíše budou využívat?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **D - uspokojivě.**

Datum: 31.5.2023 Podpis: