Katedra informatiky

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH, PEDAGOGICKÁ FAKULTA

KATEDRA INFORMATIKY

POSUDEK KVALIFIKAČNÍ PRÁCE

posudek vedoucího bakalářské práce

Autor: Martin Svatoš

Název práce: Hesla zadávána hackery při pokusu o průnik do systému

Studijní obor: Informační technologie a e-learning

Datum odevzdání: 30.6.2022

Posudek vyhotovil: Mgr. Václav Šimandl, Ph.D.

Aktuálnost tématu:	A
Cíl práce a jeho naplnění:	B
Metodologická stránka práce:	A
Orientace v odborné literatuře:	C
Úroveň zpracování obsahu a interpretace výsledků:	C
Přínosy a aplikovatelnost v praxi:	B
Jazyková, formální a grafická úroveň práce:	C

Vlastní přínos autora:

- Student navrhl a vytvořil řešení umožňující analyzovat hesla zadávaná hackery do přihlašovacích formulářů pro přihlášení běžného uživatele i administrátora v rámci redakčního systému Joomla při pokusech o průnik do systému. Toto řešení ve spolupráci s vedoucím práce nasadil na produkční a testovací server Bobříka informatiky.
- Od nasazení uvedeného řešení v únoru 2022 do doby sepsání práce se studentovi podařilo zachytit přes 800 pokusů o průnik v rámci produkčního serveru a přes 300 tisíc pokusů o průnik v rámci testovacího serveru (v tomto případě šlo o jeden dlouhodobý útok). Zjištěné pokusy student analyzoval a svá zjištění popsal.

Hlavní nedostatky práce:

- Při realizaci praktické části práce, konkrétně návrhu a implementaci programových modulů, byla potřebná značná dopomoc vedoucího práce. Při implementaci vedoucí práce musel opakovaně (cca 5krát až 7krát) provádět nejen beta testování aplikace, ale i alfa testování a aktivně se podílet na odstraňování programových chyb.

- Teoretická část práce je psána poněkud chaoticky, jednotlivé podkapitoly nejsou provázané, což se projevuje především v kapitole 2. Některá kapitoly (3.2 až 3.5, 5, 8.x) souvisejí s cílovou problematikou spíše volně, naopak v kapitole 8 chybí problematika zebezpečení spojení pomocí SSL / TLS. Část kapitol (např. kapitola 6) je psána spíše populárně než odborně (resp. jsou citovány spíše populárně-naučné než odborné zdroje), což vede k nepřesnostem v textu (např. vyjádření na s. 32 „Hash (…) má podobu jedinečného shluku čísel a písmen“ není pravdivé). Celkově teoretická část práce nedává jistotu, že se student v odborné literatuře dobře orientuje a umí se zaměřit na zdroje zásadní pro jeho práci.
- Jazyková, stylistická a formální úroveň je spíše nižší:
  - V textu se objevují překlepy a chyby psaní (např. kapitola 10.3 začíná slovy „Bávrhu byl následující, …“), gramatických a pravopisných chyb (na řadě míst chybí ve větách interpunkce).
  - Stylistický úroveň textu je nižší (např. první odstavec kapitoly 1.1 nebo vyjádření „hacker, který se bude snažit prolomit do serveru“). K horší čitelnosti textu v teoretické části práce přispělo zřejmě užití strojového překladu anglických zdrojů (např. „ne každá havěť musí nutně vykrádat hesla“).
  - V praktické části práce student používá odkazy na obrázky a zdrojové kódy, ovšem uvádí pouze číslo cílového objektu, nikoliv jeho typ (např. na s. 49 odkaz „viz 6“ nedefinuje, zda se jedná o odkaz na Obrázek 6 nebo Výpis kódu 6).
  - Práce obsahuje typografické chyby (poměrně časté jsou jednopísmenné spojky a předložky na koncích řádků). Kapitoly 7 a 8 nezačínají na nové stránce, ale v pokračování předchozí kapitoly.
  - V seznamu literatury nejsou názvy zdrojů zvýrazněny kurzívou. U řady internetových zdrojů je místo názvu zdroje uveden název domény resp. subdomény (např. místo Český PHP manuál je uvedeno Php.baraja.cz).
- Praktická část práce obsahuje méně závažné faktické chyby:
  - Diagram na obrázku 5 neodpovídá textovému popisu a implementovanému řešení.
  - V kapitole 14.8 student uvádí, že „útoky hrubou silou jsou vždy krátký“, přičemž má patrně na mysli zjištěné útoky na server Bobříka informatiky. Dle mého názoru nejde v popsaných případech o útoky hrubou silou, ale slovníkové útoky s velmi omezenou sadou zkoušených kombinací přihlašovacích údajů.
  - V kapitole 14.3 student uvádí, že se útoků „zúčastnilo 103 hackerů“. Na přiloženém CD je však uvedeno cca 105 jedinečných IP adres, tedy připustíme-li možnost užití VPN při realizaci útoků, bude počet zúčastněných hackerů výrazně nižší.
  - V kapitole 13.3 student uvádí, že hacker zadává jako jeden z přihlašovacích údajů „ibobr2019“. V obrázku 10 dokumentující tento útok však takový záznam zachycen není a objevuje se až v obrázku 11 dokumentující jiný útok.
  - V kapitole 11.10.1 student uvádí možné hodnoty parametrů v souboru crontab. Hodnoty parametru den uvádí 0-31, ačkoliv jsou povolené hodnoty 1-31; obdobně u parametru měsíc.

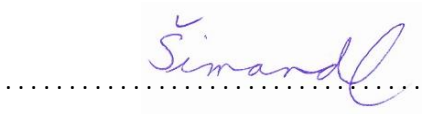
Otázky pro obhajobu a náměty do diskuze:

- Upravil byste na základě realizovaného výzkumu pravidla pro stanovení, zda konkrétní neúspěšný pokus o přihlášení je součástí útoku hackera (např. změnil byste časové intervaly, minimální počet pokusů o přihlášení apod.)? Pokud ano, jak?

Práci doporučuji k ústní obhajobě.

Navrhuji hodnocení stupněm: C dobře

Místo, datum: České Budějovice, 9.8.2022



. . . . . .

Vysvětlivky:

A – vysoká úroveň (precizní teoretická část, kvalitní rešerše, bohatá a správně citovaná literatura, bez chyb psaní, výstižné formulace, kvalitní grafika, velký rozsah prací, velice inovativní práce, správná volba metody výzkumu, kvalitně zpracované výsledky výzkumu)

B – standard (teoretická část bez chyb, správně a přesně popsán cíl a metoda práce, průměrná odborná úroveň, standardní rozsah práce, s málo překlepy, vzhledem k rozsahu přiměřený počet drobných chyb, správné popisy v grafech, nepřesné citace v textu, chudší literatura – použití převážně 1- 2 zdrojů)

C – slabší úroveň (cíle a metody popsány nepřesně nebo neodpovídají realitě práce, menší rozsah práce, nepřesná terminologie, chybějící vysvětlení hlavních pojmů, malý rozsah práce, nepříliš inovativní a nosné, nedostatečné zdroje, použití převážně jednoho hlavního zdroje, chudá literatura, četné překlepy a slabší grafická úroveň, větší množství méně podstatných chyb, nejasná metoda a analýza výzkumu)

N – nevyhovující (chybějící nebo velmi stručné a formální popsání cílů a metod, malý rozsah práce, částečně opsáno v teoretické části, slabá terminologie, není patrný vlastní přínos, slabá úroveň vyjadřování, nejasné používané pojmy, malý rozsah praktické složky práce, závažné chyby ve výzkumu, nevyhovující grafická úroveň, mnoho hrubých chyb a překlepů, odbyté)