FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Návrh a implementace hry pro výuku etického hackování
Student:	Mikuláš Hrdlička
Vedoucí:	Mgr. Jakub Růžička
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2018/19

Pokyny pro vypracování

Bakalářská práce se zabývá návrhem a implementací funkčního prototypu výukové počítačové hry /soutěže zaměřené na počítačovou bezpečnost a etické hackování, téže známé jako CTF (Capture the Flag), která bude využita jako podpůrný výukový nástroj předmětu BI-EHA (Ethical Hacking, FIT ČVUT).

Popište jaké přínosy může mít výuka informační bezpečnosti a etického hackování skrze interaktivní počítačové hry a zanalyzujte existující soutěže a řešení. Popište jakým způsobem se herní design a mechanismy dají využít pro výuku, a jaké výhody a nevýhody mají při využití pro edukativní účely. Navrhněte vlastní řešení a popište tento návrh z hlediska herního, softwarového a výukového designu. Prototyp svého řešení implementujte za použití nástrojů a jazyků zvolených během fáze návrhu. Řešení otestujte na vzorku studentů kurzu BI-EHA a zhodnoťte naplnění cílů práce.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 9. ledna 2018

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Návrh a implementace hry pro výuku etického hackování

Mikuláš Hrdlička

Katedra softwarového inženýrství
Vedoucí práce: Mgr. Jakub Růžička

14. května 2018

Poděkování

Na tomto místě chci poděkovat vedoucímu práce Mgr. Jakubovi Růžičkovi za jeho nadšení, upřímnost a metodické vedení při jejím zpracování, za poskytnuté důležité rady a podněty během konzultací, za jeho čas, vstřícnost a trpělivost.

Má neskonalá vděčnost patří také Krysovi a Míše s Dantesem, za tu nejlepší psychickou podporu v těch nejkrušnějších chvílích posledních několika měsíců.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 14. května 2018 .....

České vysoké učení technické v Praze
Fakulta informačních technologií
© 2018 Mikuláš Hrdlička. Všechna práva vyhrazena.
Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí a nad rámec oprávnění uvedených v Prohlášení na předchozí straně, je nezbytný souhlas autora.

Odkaz na tuto práci

Hrdlička, Mikuláš. *Návrh a implementace hry pro výuku etického hackování.* Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

Abstrakt

Tato bakalářská práce se zabývá návrhem, implementací a tvorbou úloh pro platformu na výuku etického hackování. Pro zatraktivnění interakce s platformou je využito poznatků z teorie herního designu, a pro úlohy je použitý tématický příběh založený na reálných událostech. Hlavním výsledkem této práce je implementovaná výuková platforma, která svými funkcemi reaguje na nedostatky ve zpětné vazbě, které jsou problémem existujících řešení. Na závěr je platforma otestována vzorkem studentů předmětu etického hackování.

Klíčová slova implementace, webová platforma, hacking, etické hackování, gamifikace, CTF, penetrační testování, tvorba her, herní design

Abstract

The main focus of this bachelor's thesis is design, implementation, and challenge design for a platform that teaches ethical hacking. Interaction with the platform is made more attractive by the use of game design theory, and a strong theme and story for the challenges. Main result of the thesis is the finished education platform, with features that solve the problematic lack of feedback and help in existing solutions. The thesis is concluded by a test run on students of ethical hacking course.

Keywords implementation, web platform, hacking, ethical hacking, gamification, CTF, penetration testing, game developement, game design

Obsah

Úvod **1**

1 Cíl práce **3**

2 Definice nejdůležitějších pojmů **5**
2.1 Hacking 5
2.2 Etické hackování 6
2.3 Capture the Flag 6
2.4 Gamifikace 6

3 Aktuální stav hacking soutěží **9**
3.1 Formáty Hacking Soutěží 9
3.2 Využití soutěží pro výuku 12

4 Srovnání vybraných soutěží **17**
4.1 Srovnávací kritéria 17
4.2 Vybrané soutěže 20
4.3 Interpretace Pozorování 21

5 Gamifikace **25**
5.1 Co je gamifikace 25
5.2 Co není gamifikace 27
5.3 Gamifikace v praxi 28
5.4 Gamifikace a výuka 29
5.5 Jak správně použít gamifikaci 31

6 Specifikace požadavků **35**
6.1 Úvod 35
6.2 Všeobecný popis 36
6.3 Specifikace požadavků 37

7 Analýza **41**
7.1 Modelování obchodních procesů 41
7.2 Případy užití 45
7.3 Analýza existujících CTF platforem 49

8 Návrh **51**
8.1 Gamifikace 51
8.2 Návrhová rozhodnutí 53
8.3 Architektura 53
8.4 Databázový model 56
8.5 Uživatelské rozhraní 58
8.6 Návrh úloh 60

9 Implementace a nasazení **65**
9.1 Vedení projektu 65
9.2 Praktická implementace 66
9.3 Tvorba úloh 67
9.4 Nasazení 67

10 Testování na studentech předmětu BI-EHA **69**
10.1 Statistiky interakce s platformou 69
10.2 Dotazník 69
10.3 Možná řešení 70

Závěr **73**

Literatura **75**

A Seznam použitých zkratek **85**

B Obsah přiloženého CD **87**

Seznam obrázků

4.1 CTFd Framework 19
4.2 Facebook CTF 19

7.1 Diagram aktivity zpětné vazby domácích úkolů 43
7.2 Diagram aktivity zpětné vazby domácích úkolů se systémem BI-EHA Task Froce 44

8.1 Ilustrace závislosti komponent mezi CTFd a vyvíjeným modulem . 54
8.2 Diagram komponent zásuvného modulu. Komponenty CTFd jsou z naprosté většiny vynechány. 55
8.3 Databázový model. Nerelevantní tabulky CTFd jsou z modelu vynechány. 57
8.4 Návrh základního navigačního menu 58
8.5 Návrh obrazovky seznamu zpráv 59
8.6 Návrh posílání zpráv a žádosti o pomoc. Vlevo je zobrazena konverzace, vpravo obrazovka žádosti o pomoc. 59
8.7 Návrh obrazovky tvorby postupů řešení 60

9.1 Plánování práce za použití platformy VSTS 66
9.2 Diagram nasazení vyvinuté platformy 68

Seznam tabulek

4.1 Vybrané soutěže 21

7.1 Porovnání funkcí CTF Frameworků 50

Úvod

Bezpečnost se v poslední době stává čím dál tím důležitější součástí informačních systémů. Lidé jim svěřují důvěrná a důležitá data, a tyto systémy se tím stávají velmi lukrativním cílem pro útočníky snažící se tyto data získat a zneužít. S růstem rozsahu a multifunkčnosti vyvíjených systémů začíná také ale být výrazně složitější zajistit dostatečnou bezpečnost před těmito útoky, a nároky na znalosti specialistů, již tuto bezpečnost zaručují a prověřují, rostou enormní rychlostí.

Jedním z populárních a moderních způsobů jak nahlížet na bezpečnost je zaujmout úhel pohledu útočníka, a tím způsobem rychleji a účinněji nalézat nedostatky vyvíjených systémů, které mohou být opraveny dříve, než je stihne někdo zneužít.

Tato práce je určena pro studenty, kteří mají zájem o tento úhel pohledu na informační bezpečnost, a kterým výstup této práce usnadní vstup do a seznámení s tímto složitým oborem. Zároveň je také určena pro vedoucí a vyučující kurzů Etického hackování, kterým nabízí platformu a způsob jak jednoduše prezentovat praktické úlohy svým studentům zábavnou a interaktivní formou.

Toto téma bylo zvoleno převážně z toho důvodu, že existuje veliké množství teoretických prací a studií o přínosu gamifikace ve výuce, ale není mnoho platforem, které by tuto teorii aplikovaly prakticky. A kombinace teoretických výhod gamifikace, která je podložena několikerými studii, a praktické výuky etického hackování, jehož výhody jsou také rozsáhle teoreticky prostudovány, se jevila jako nejpřínosnější, a také jako velmi zajímavé a atraktivní téma.

Práce se zabývá analýzou, návrhem a implementací gamifikované platformy pro výuku etického hackování. Vývoj byl vedený iterativní metodou, s týdenní délkou iterací.

Tato práce dále pokračuje v následující struktuře:

V první části této práce bude nejprve vysvětleno několik klíčových pojmů. Poté bude provedena analýza nedostatků, které plynou z přístupu soutěží k soutěžícím z edukativního hlediska, a také porovnání nejznámějších CTF soutěží které se po světě konají.

Poté následuje část o gamifikaci, jeho přínosů, možnosti využití v akademické sféře, a výběr nejvhodnějšího frameworku který bude implementován v dalších částech.

Třetí část práce se zabývá návrhem. Po ustanovení funkčních požadavků a návrhu aplikace z hlediska vzhledu a dostupných funkcí bude stanovena a zvolena architektura, a navržen základní set úloh, které budou studenti v rámci předmětu BI-EHA řešit.

Čtvrtá část je věnována způsobu, kterým probíhala implementace a nasazení platformy. Závěry, které vyplynuly z pozorování studentů, jimž byla hotová platforma spolu s úlohami v rámci výuky předložena na vyzkoušení, jsou sepsány v poslední, páté části.

Kapitola 1

Cíl práce

Hlavním cílem této práce je vytvořit počítačovou hru, platformu anebo soutěž, která interaktivní formou, a za využití prostředků gamifikace, představí a umožní uživatelům prakticky si vyzkoušet a procvičit základní témata z osnov kurzu Etického Hackování na FIT ČVUT. Cílem rešeršní části práce je prozkoumat jaké přínosy může mít výuka informační bezpečnosti a etického hackování skrze interaktivní počítačové hry a zanalyzovat existující soutěže a řešení. Popsat jakým způsobem se herní design a mechanismy dají využít pro výuku, a jaké výhody a nevýhody mají při využití pro edukativní účely. V praktické části je cílem navrhnout vlastní řešení gamifikovaného způsobu výuky, a popsat tento návrh z hlediska herního, softwarového a výukového designu. Navržené řešení implementovat, a na závěr prakticky vyzkoušet na vzorku studentů kurzu BI-EHA.

Kapitola 2

Definice nejdůležitějších pojmů

Hlavním tématem této bakalářské práce je spojení hackingu a gamifikace. Přesně definovat tyto dva pojmy ale nebude jednoduché, neboť v případě hackingu se jedná o pojem, kolem kterého se točí spousty dezinformací, a jehož známé definice se od sebe vcelku razantně liší, v závislosti na tom, koho se zeptáte. V této úvodní části se pokusím přiblížit čtenáři jaké definice existují, a vysvětlím co za význam jsem zvolil pro tyto termíny v kontextu této práce.

2.1 Hacking

Slovo hacking, a od něj odvozený hacker, má dva velmi se lišící významy. V původním významu mělo jít o někoho, koho baví zkoumat možnosti programovatelných systémů, a hledat nekonvenční způsoby jakým tyto technologie využít a vylepšit. V podstatě jde o nadšence, kteří se nespokojí pouze se standardním a zdokumentovaným způsobem používání technologií (ať už jde o hardware nebo software), a hledají nové, vlastní, cesty jakým tyto technologie zlepšit nebo použít. Většinou se jedná o způsob použití, který původní tvůrce technologie nezamýšlel. V masových mediích a populární kultuře je ale slovo hacking a hacker spojeno spíše s informačními systémy a nelegální činností, nežli s kreativitou a hardwarem – hackerem je někdo, kdo proniká do systémů jinou než standardní cestou, tedy obejitím nebo prolomením jeho bezpečnostní ochrany, a tím získává přístup k datům a funkcím ke kterým nemá být oprávněn, a to většinou za účelem zisku nebo s cílem způsobit škodu. Většinou bývá motivem snaha o krádež a následný prodej dat, přístupových hesel, nebo přímo převod financí (např. po získání přístupových údajů do něčí bankovní aplikace) [96].

Pro tuto práci jsou relevantní definice obě, neboť etické hackování (také známe jako white-hat hacking) je ve své podstatě kombinace obou zmíněných přístupů. Etickým hackerem je člověk, který po domluvě s vlastníkem cíleného informačního systému využije své znalosti o informačních systémech k tomu, aby prolomil nebo obešel bezpečnostní ochranu daného systému, a následně

mohl zdokumentovat a sepsat zprávu o způsobu jakým se mu to povedlo. Zprávu poté předá vlastníkovi prolomeného informačního systému, a na základě této zprávy může poté vlastník učinit opatření, které opraví chyby, jež umožnili prolomení jeho bezpečnostních systémů, aby k nim v budoucnosti nemohlo dojít znovu.

2.2 Etické hackování

Etické hackování je tedy sada znalostí, postupů a přístupů, jejichž cílem je získat schopnost prolomit nebo obejít bezpečnostní systémy a opatření kteréhokoliv informačního systému, a být schopen svůj postup důkladně zdokumentovat za účelem poskytnutí rad na zlepšení daného systému vlastníkovi, aby k prolomení nedocházelo v budoucnosti (a od subjektů s nekalými úmysly). Tyto postupy nemusí být pouze na rovině softwarové – mezi použité metody patří také například sociální inženýrství, při kterém se např. etický hacker pokusí získat přístupová hesla ze zaměstnanců společnosti, které do informačního systému mají přístup, a to třeba vydáváním se za zaměstnance poskytovatele telekomunikačních sítí, který přišel zapojit modem do kanceláře [82].

2.3 Capture the Flag

Capture The Flag (CTF) jsou soutěže zaměřené na kybernetickou bezpečnost a etické hackování. Zpravidla se jedná o soutěže týmové, kde každý tým dostane set úloh, většinou rozdělených do kategorií týkajících se určitého podoboru bezpečnosti (např. kryptografie, binární soubory, web, forensika atd.), za jejichž vyřešení dostávají týmy body. Cílem většiny úloh bývá získat tzv. Vlajku, což je textový řetězec (obvykle ve formátu flag{}), která bývá skryta způsobem souvisejícím s povahou úlohy [41]. Například pro kryptografickou úlohu může být řetězec s vlajkou zašifrován špatně nastavenou blokovou šifrou, která používá stejný klíč pro každou iteraci, nebo v případě webové úlohy může jít o webovou stránku, která si přístupová práva uživatele uchovává v cookies s tím, že vlajka se nachází v sekci pouze pro administrátory. Hlavní myšlenkou CTF soutěží je vyzkoušet si v simulovaném prostředí běžné zranitelnosti bezpečnostních systémů, a procvičit se v jejich obcházení.

2.4 Gamifikace

Gamifikace je použití herního designu, herní teorie a herních principů v kontextu který není hrou. Jedná se o v poslední době velmi populární techniku, která nalézá své uplatnění například v marketingu, školství, nebo i politice. Hlavní myšlenkou gamifikace je použít znalosti herního designu, a použít prvky hry pro motivaci a ozvláštnění neherních činností. Cílem hry je nejen bavit, ale také zaujmout a udržet pozornost hráče co nejdéle, motivovat ho k návratu

ke hře a zajistit co nejpříjemnější zážitek z interakce s hrou. Proto existuje spousty technik, jakými lze těchto efektů ve hře dosáhnout, a ideou gamifikace je přenést tyto postupy do jiných odvětví, a tím vyvolat stejně pozitivní efekty jaké doprovází hru, a dosáhnout pocitu u uživatele kdy úkoly spojené s odvětvím působí spíše jako zábava, než jako povinnosti [39]. V kontextu této práce se jedná o použití herního designu v odvětví školství a výuky, s cílem vytvořit učební materiál o etickém hackování, který bude působit spíše jako počítačová hra zatímco si zachová veškeré poučné a edukativní vlastnosti. Přesnější definicí gamifikace se bude práce zabývat v pozdější kapitole.

Kapitola 3

Aktuální stav hacking soutěží

Počítačová bezpečnost se stává čím dál tím více důležitou součástí Informačních Technologií. Ročně se ve světě pořádají stovky konferencí zaměřených na bezpečnost [23], na kterých tisíce nadšenců diskutují, prezentují, a v přátelské atmosféře sdílejí své nové poznatky z praxe. Na většině těchto konferencí se začínají stále častěji objevovat soutěže zaměřené na počítačovou bezpečnost, a obecně převládá názor, že tyto druhy soutěží poskytují unikátní příležitost, jak rozvíjet své schopnosti v oboru [18, 24]. Potenciál využití těchto již existujících soutěží pro výukové účely ale není příliš ideální, neboť kompetitivní povaha a téměř nulová zpětná vazba velmi limituje přínos, jaký může soutěž pro studenta mít [40]. V této kapitole se podíváme na již existující typy a způsoby vedení soutěží, a zanalyzujeme jejich přístup, mechaniky a možnost využití pro edukativní účely.

3.1 Formáty Hacking Soutěží

V současné době se většina soutěží drží jednoho z několika zaběhlých formátů, které si zde popíšeme. Formáty se obecně dají rozdělit následujícím způsobem: [40, 26]

- Individuální, s navazujícími úkoly (Wargames)
- Skórované, s tematicky rozdělenými úkoly (Jeopardy CTF)
- Týmové útok–obrana CTF
- Soutěže zaměřené pouze na obranu
- Soutěže zaměřené na fyzickou bezpečnost

Nejedná se o vyčerpávající seznam, neboť se občas ukáže nějaká unikátní soutěž, která pod žádný z těchto typů nespadá. Příkladem takovéto unikátní soutěže může být například každoroční soutěž Hackfortress [74], ve které týmy soutěžících soutěží v počítačové hře Team Fortress 2, a zároveň řeší soutěžní otázky týkající se bezpečnosti a hackování, za které jejich tým dostává výhody

do hry. V kontextu této práce se však soustředíme pouze na častěji se vyskytující typy soutěží. Dále následuje podrobnější popis každého ze zmíněných typů soutěží.

3.1.1 Individuální, s navazujícími úkoly

Jedná se o druh soutěží, ve kterých je účastníkům předložen jeden nebo více lineárních setů problémů s postupně se zvyšující obtížností. Problémy v daném setu navazují, a je potřeba je řešit v pevně stanoveném pořadí. Soutěže bývají dlouhodobé (v některých případech i časově neomezené [99]), což dovoluje účastníkům postupovat svým vlastním tempem. V tomto druhu soutěží bývá odměna za úspěšné vyřešení pouze symbolická, např. možnost zapsat se do tabulky řešitelů [85]. Příklady těchto druhů soutěží se dají nalézt v komunitách jako je OverTheWire.net [99], nebo smashthestack.org [86].

3.1.2 Skórované, s tematicky rozdělenými úkoly

Tento druh soutěží bývá často označován jako Jeopardy CTF, kvůli podobnosti s populární americkou znalostní soutěží Jeopardy [40], což je soutěž podobná tuzemské televizní soutěži Riskuj! [84]. Soutěžící, většinou týmy, dostávají několik soutěžních úkolů, které jsou rozděleny podle kategorií (jako např. web, reverzní inženýrství, forensika atd.). Každá kategorie obsahuje několik úloh, a týmy je mohou řešit, v jakémkoliv pořadí chtějí. Za každou správně vyřešenou úlohu dostávají daný počet bodů v závislosti na obtížnosti úlohy. Soutěže bývají krátkodobé (v rámci dnů, maximálně týdnů) [30], a vítězem se stává tým, který dosáhne největšího počtu bodů. Jedním z příkladů může být například kvalifikační kolo DEFCON CTF [27], jedné z největších CTF soutěží, které se v minulém roce účastnilo přes 350 týmů [31].

3.1.3 CTF typu útok–obrana

Tento druh soutěží se od výše zmíněných výrazně liší, neboť v něm soutěžící neřeší předpřipravené úkoly, nýbrž každý tým dostane předem připravený systém, na kterém běží desítky až stovky služeb, které jsou úmyslně velmi špatně zabezpečené. Týmy v daném časovém limitu prolamují bezpečnostní systémy služeb na strojích ostatních týmů s cílem získat přístup k jejich vlajkám [36], zatímco se snaží opravit bezpečnostní nedostatky služeb na svém vlastním stroji, aby ubránili své vlastní vlajky. Vlajky jsou obvykle textové řetězce, které jsou uloženy jako data v různých službách spuštěných na strojích každého z týmů. Příkladem takovéto služby může být například SMTP server, na který dorazí vlajka ve formě elektronické zprávy. Přístup ke zprávě s vlajkou přirozeně vyžaduje řádnou autentizací uživatele, a náplní soutěže je tedy snaha týmů nalézt nedostatky v zabezpečení této služby (tyto nedostatky jsou do služby přidány organizátory soutěže, a u každého týmu jsou stejné), a

získat tím přístup k datům (vlajkám) ostatních týmů bez znalosti jejich přístupových hesel [27]. Zároveň také musí zamezit ostatním týmům získat přístup k datům na jejich vlastním stroji opravením bezpečnostních nedostatků, a tím ubránit své domácí vlajky. Týmy musí také po celou dobu soutěže udržovat veškeré tyto služby funkční, neboť součástí soutěže je i herní server, který disponuje validní autentizací a simuluje reálný provoz a využití těchto služeb legitimním uživatelem, čímž kontroluje jejich dostupnost. V případě že herní server zjistí u některého týmu nedostatek v dostupnosti některé ze služeb, jsou týmu automaticky ubrány body. Herní server tímto způsobem také pravidelně přidává nové vlajky týmům, které mohou ostatní týmy nacházet. Vítězem se stává tým, který má po uplynutí časového limitu nejvyšší skóre. Například na soutěži DEFCON CTF obsahuje soutěžní systém stovky služeb, a vlajky jsou kradeny po desítkách za použití předpřipravených skriptů, které si každý tým připravil předem [31, 27].

3.1.4 Soutěže zaměřené na kyberobranu

Soutěže zaměřené na obranu se na první pohled velmi podobají předchozím CTF typu útok–obrana. Ve své podstatě se také jedná o stejný styl soutěže, jen s jedním rozdílem – soutěžní týmy na sebe navzájem neútočí, nýbrž pouze brání svůj systém před útoky zprostředkované organizátory soutěže. Každý tým disponuje vlastní sítí, a cílem je ubránit ji před snahou hackerů (organizátorů) prolomit jeho bezpečnost, zatímco udržují všechny služby vyžadované soutěží (např. SMTP server, ftp server atd.) v chodu, aby na něj mohli bez problémů přistupovat běžní uživatelé, kteří jsou také simulováni organizátory soutěže. Dvojice významných [40] soutěží v kyberobraně zaměřených převážně na akademickou sféru jsou soutěže CCDC (National Collegiate Cyberdefence Competition) [78] a CDX (Cyber Defence Exercise) [77]. CCDC je soutěž pořádaná pro akademické instituce v Americe, a CDX je soutěž pořádaná NSA pro Americké vojenské školy. Hlavní rozdíl mezi těmito soutěžemi je v tom, že na CCDC dostanou účastníci předpřipravenou síť od organizátorů, kdežto na CDX dostanou účastníci pouze specifikace, které má síť splňovat, a staví si ji sami před začátkem soutěže [40].

3.1.5 Fyzická bezpečnost

Fyzická bezpečnost je často přehlíženým faktorem v mnoha informačních systémech [26]. Proto se některé ze soutěží soustředí na tento druh bezpečnosti. V tomto typu soutěží bývá cílem splnit určitý úkol týkající se obcházení fyzického zabezpečení, a týmy jsou posuzovány typicky podle rychlosti, za jakou daný úkol splní. Jedná se například o soutěže ve vyháčkování zámků, získávání informací ze zamčené kanceláře (včetně krádeže zapnutého pevného počítače aniž by došlo k přerušení přísunu proudu, a vymazání volatilní paměti [59]), nebo i úpravě zapečetěných přístrojů a dokumentů bez poznatelného poru-

šení pečeti [33]. Tento druh soutěží není pro naší výuku etického hackování relevantní, proto se jím nebudeme dále zabývat.

3.2 Využití soutěží pro výuku

3.2.1 Přínos existujících soutěží pro výuku

O přínosu hacking soutěží pro výuku informační bezpečnosti bylo napsáno již několik prací a článku, které se svými závěry v shodují na tom, že soutěže mají pro výuku bezpečnosti v naprosté většině případů pozitivní dopady. V této části se na tyto přínosy podíváme. Objevují se tyto přínosy soutěží:

- Pozitivní dopad na znalosti soutěžících. [25, 18]
- Inspirace účastníků k založení asociací a spolků na škole. [25, 18]
- Vznik dat pro výzkum které se těžce shání v reálném prostředí. [42, 26]
- Doplnění nedostatku ofenzivní bezpečnosti v osnovách univerzit. [41, 62, 104]
- Dosažení velkého rozsahu a rámce, který je těžké replikovat ve třídních podmínkách. [40, 18, 25]
- Zlepšení vztahu studentů k oboru, neboť studenty baví. [104, 18, 26, 25]

3.2.1.1 Přínos studentům

Studenti, kteří se v rámci osnov výuky bezpečnosti připravovali a účastnili soutěže CCDC [78] v rámci osnov výuky bezpečnosti tvrdí, že jim účast na soutěži velmi rozšířila znalosti a praktické dovednosti, a na jedné škole vedla k založení Information System Security Association (Asociace Bezpečnosti Informačních Systému, překlad autora) [25], která slouží k většímu propojení studentů s průmyslem, a má za cíl zvýšit úroveň znalostí a dovedností studentů v oboru informační bezpečnosti. Dokonce i v případě, že se tým studentů v soutěži umístí na posledních příčkách, popisují jeho členové jako přínos soutěže získání lepší představy o nedostatcích a mezerách v jejich znalostech, což vedlo k jejich lepšímu umístění v další soutěži [18]. Tito studenti také označili účast na soutěžích jako největší přínos celého kurzu, a u většiny z nich se zvedl zájem o bezpečnost v IT natolik, že na své škole založili studijní skupinu [18]. Jako další z přínosů účasti na CCDC popisují studenti uvědomění si reality okolo nedostatku dostupnosti detailních informací k problémům, jež nastávají, který je v reálném světě velmi častý [25]. Vedla k tomu skutečnost, že účastníci soutěže nejsou informováni v případě, že dojde k prolomení jejich systémů. Týmy si museli veškeré tyto informace zjišťovat sami, což je v přímém kontrastu s klasickými univerzitními zkouškami, kde jsou ve většině případů studentům všechna fakta týkající se problému vypsána přímo v zadání zkouškových úloh [25].

3.2.1.2 Přínos výzkumu

Kromě přínosu projevujícího se na znalostech studentů pozorují odborné články také přínos soutěží pro výzkumnou sféru. Data nasbíraná v jedné ze soutěží na HOPE konferenci [4] byla po jejím ukončení odevzdána do repositáře dat pro výzkum bezdrátových technologií univerzity Dartmouth, Crawdad [35], která mohou být využita pro výzkumy druhého a třetího řádu [26]. V článku *Gamification for Measuring Cyber Security Situatuational Awarness* [42] autoři popisují výhody sběru dat o chování účastníků hacking soutěží. Jako největší přínos spatřují ve snaze hacking soutěží co nejvíce se přiblížit ke scénářům z reálného světa, a možnosti sbírat a dále publikovat data o chování, metodách a přístupu účastníků bez nutnosti provádět příliš destruktivní anonymizaci dat. O takováto data je dle autorů ve výzkumné komunitě kyberbezpečnosti velký zájem, a je složité takováto data mimo soutěže získat, neboť v naprosté většině případů nelze používat reálná data z produkčních prostředí (kvůli citlivosti takových dat) [42].

3.2.1.3 Přínos výuce

Dívat se na bezpečnost z úhlu pohledu útočníka se osvědčuje jako velmi účinná učební metoda, která produkuje studenty se schopností psát bezpečnější aplikace a systémy než v případě čistě defensivního přístupu k výuce [62]. Článek *Capture-the-Flag: Learning Computer Security Under Fire* [41] nalézá v osnovách univerzit dva vyučované druhy přístupů k bezpečnosti, a tím jsou přístupy *protekční* a *konstrukční*. *Protekční* přístup se zaměřuje na obranu již existujícího systému, a vyučuje systémovou správu s cílem zajistit co nejvyšší bezpečnost. Přístup *konstrukční* se naopak používá v případě návrhu nového systému, a zabývá se postupy jak navrhnout informační systém tak, aby byl co nejvíce bezpečný již od spuštění. Dle článku se ale oba tyto přístupy zabývají již prověřenými a existujícími přístupy, které jsou schopny odhalit a předejít pouze již existujícím chybám. Student tedy není učen aktivně vyhledávat a rozpoznat bezpečnostní chyby a nedostatky dosud nenalezené. Autoři článku argumentují, že soutěže CTF typu útok–obrana jsou ideálním nástrojem pro vyplnění tohoto nedostatku v osnovách, neboť nutí účastníky rozpoznávat a vyhledávat nové bezpečnostní nedostatky. Vyučovat síťovou bezpečnost skrze cvičení ve formátu CTF soutěží zkoušela i Kalifornská univerzita Santa Barbara. Ve výsledku se jim tento přístup velmi osvědčil, neboť nejen že studenty bavil (a tím zajistil vysokou účast na předmětu), ale také se ukázal jako velmi efektivní metoda výuky [104]. Ke stejným závěrům došla i Massachusettská univerzita, která v rámci studie použila Challenge-Based Learning (CBL) [53] metodologii, nahrnutou společností Apple Computer Inc., pro výuku kyberbezpečnosti. Součástí doprovodných aktivit byla povinná účast na dvou CTF soutěžích typu útok–obrana, a dle odpovědí na dotazník po skončení studie byla zkušenost z CTF soutěží hodnocena studenty jako nejvíce přínosná akti-

vita [18].

CTF soutěže jsou ve své podstatě komplexní cvičení v oboru Informační Bezpečnosti, jež vyžadují přípravu a znalosti v rozličných oborech jako například forensika, systémová administrace, síťová bezpečnost, síťové inženýrství a architektura, týmové vedení nebo kooperace [41]. Během přípravy jsou většinou studenti vystaveni tématům, s nimiž by během svého studia nutně nepřišli do styku (resp. pouze v teoretické rovině). Naučí se spolupracovat, a protože jsou soutěže většinou chaotické, také pracovat dobře pod tlakem, zatímco efektivně komunikují a správně prioritizují úkoly [40]. Z toho důvodu se tyto soutěže jeví jako ideální doplněk k praktické výuce bezpečnosti na školách.

3.2.2 Nedostatky existujících soutěží

Na způsobu jakým jsou vedeny existující soutěže je stále co vylepšovat. Cílem kompetitivních soutěží většinou bývá primárně porovnat znalosti soutěžících mezi sebou, a jakýkoliv edukativní přínos je až vedlejší záležitostí. I přes to, že spousty soutěží jsou cílené pro studenty, nejedná se o nejlepší způsob jakým poprvé představit bezpečnost studentům. Je to způsobeno převážně vysokým nárokem na již získané znalosti studentů a nedostatkem dokumentace a zpětné vazby [15]. Naprostá většina těchto soutěží také neobsahuje žádné přípravné kurzy, a příprava týmů je přenechána na samotných účastnících [40]. Pokud účastník neví jakým způsobem se připravovat, účast na soutěži se pro něj stává velmi obtížnou. Také po skončení soutěže je pro týmy jedinou zpětnou vazbou jejich bodový zisk, a také jejich umístění v porovnání s ostatními týmy. Pokud nějaký z týmů během soutěže narazí na neznalost nějakého z kritických problémů, často to pro něj znamená konec soutěže. Ze soutěže se tím pádem stává pouze zajímavá zkušenost, a příležitost, která dává studentům a jejich týmům možnost k sebehodnocení, které ale musí studenti využít a zpracovat sami a mimo soutěž. Tím se zodpovědnost za znalostní přínos soutěže studentovi přesouvá na jeho tým, a záleží pouze na tom, zda této příležitosti využije. Pokud se student nebo tým dostane do situace, kdy takovéhoto druhu sebehodnocení není schopen (nebo neví jak k němu přistoupit), účast v soutěži pro něj bude mít výrazně menší přínos.

3.2.2.1 Možná řešení těchto nedostatků

Hlavním řešením těchto nedostatků je použít soutěže jako jednu z částí výuky, a postarat se o zajištění dobré a jasné přípravy před soutěží, a důkladné zpětné vazby jednotlivců po skončení soutěže. Tento přístup zvolila většina univerzit, jež se pokoušeli zapojit účast na soutěžích do osnov výuky bezpečnosti, a studie, které na toto téma byly napsány, poukazují na dobré výsledky [104, 41, 18].

V práci *Computer security competitions: Expanding educational outcomes* [40] porovnává Chris Eagle soutěže v kybernetické bezpečnosti s vojenskými cvičeními, a navrhuje možné zlepšení, jaké by mohli různé formáty soutěží zavést, aby se těmto cvičením přiblížili. Jako hlavní výhodu vojenských cvičení spatřuje v přípravě formou lekcí před cvičením, pevně stanoveném očekávání, které cvičení má na schopnosti účastníků (a se kterým jsou účastníci seznámeni), a přesně stanovené a velmi detailní zpětné vazbě, kterou každý účastník dostane po absolvování cvičení spolu s očekáváním, že všechny nedostatky do příštího cvičení napraví.

Některé z těchto navrhovaných řešení se již na soutěžích začínají objevovat. Například soutěž InCTF [15] byla rozdělena na několik kol, z nichž první bylo kolo naučné, při němž byli účastnící seznámeni se základními tématy, jimiž se soutěž zabývá, formou interaktivních online cvičení. V dalším kolem poté soutěžící prošli jednodušší CTF soutěží typu Jeopardy, jejíž řešení bylo po skončení soutěže zveřejněno pro studijní účely. Teprve poslední kolo soutěže bylo CTF typu útok–obrana, které je považováno za nejtěžší z disciplín [15]. To samé platí o soutěži MITCTF [72], jež byla hostována MIT Lincoln Laboratory, a která také obsahovala několik naučných kurzů, jejichž cílem bylo připravit účastníky na účast v soutěži [18].

Kapitola 4

Srovnání vybraných soutěží

V této části provedeme srovnání několika vybraných soutěží, které jsou pravidelně pořádány. Vzhledem k tomu, že během rešerše literatury nebyla objevena žádná odborná publikace nebo standard, který by se zabýval srovnávacími kritérii těchto soutěží, nejprve tyto kritéria navrhneme. Kritéria jsou vybrána v návaznosti na teoretické poznatky z předchozí kapitoly. U každé ze soutěží sledujeme a porovnáváme několik hlavních atributů, které budou popsány v následující části kapitoly a které byly vybrány s ohledem na jejich relevantnost k této práci. Soutěže byly vybírány ze seznamu pořádaných soutěží *CTF Time* [30], a z několika dalších seznamů nejpopulárnějších soutěží v oblasti informační bezpečnosti [1, 5].

4.1 Srovnávací kritéria

4.1.1 Typ soutěže

První atribut který u soutěží sledujeme je jeho zařazení do jedné z kategorií, které byly představeny v předchozí kapitole.

4.1.2 Počet soutěžících

Počet účastníků slouží jako dobrý ukazatel popularity a rozsahu soutěží, a také se jedná o údaj který je jednoduché o soutěži zjistit.

4.1.3 Prezenční/Distanční

U soutěží také rozlišujeme zda je od účastníků vyžadována jejich fyzická přítomnost na místě soutěže, nebo zda celá soutěž probíhá online formou.

4.1.4 Cílové publikum

Dalším důležitým atributem při porovnávání soutěží je cílové publikum. Zde hlavně rozlišujeme, zda je soutěž pouze pro studenty, amatéry, nebo zda je účast povolena všem, včetně expertů z bezpečnostní praxe.

4.1.5 Zpětná vazba účastníkům

Zde sledujeme jaká zpětná vazba je předávána účastníkům soutěže. Zjišťujeme, zda organizátoři zveřejňují po soutěži referenční postupy řešení, zda během soutěže mají týmy, kterým se příliš nedaří, možnost nápovědy, a jaká všechna data jsou k dispozici po skončení soutěže.

4.1.6 Přípravné workshopy

Porovnáváme také přístup k přípravě na soutěž. Sledujeme, zda soutěž nabízí přípravné kurzy, či obsahuje nějaký druh rozehřívacích kol/lekcí, aby byl zájemcům, kteří nejsou v oboru příliš zběhlí, o něco ulehčen vstup do soutěže.

4.1.7 Použití některé ze známých soutěžních platforem

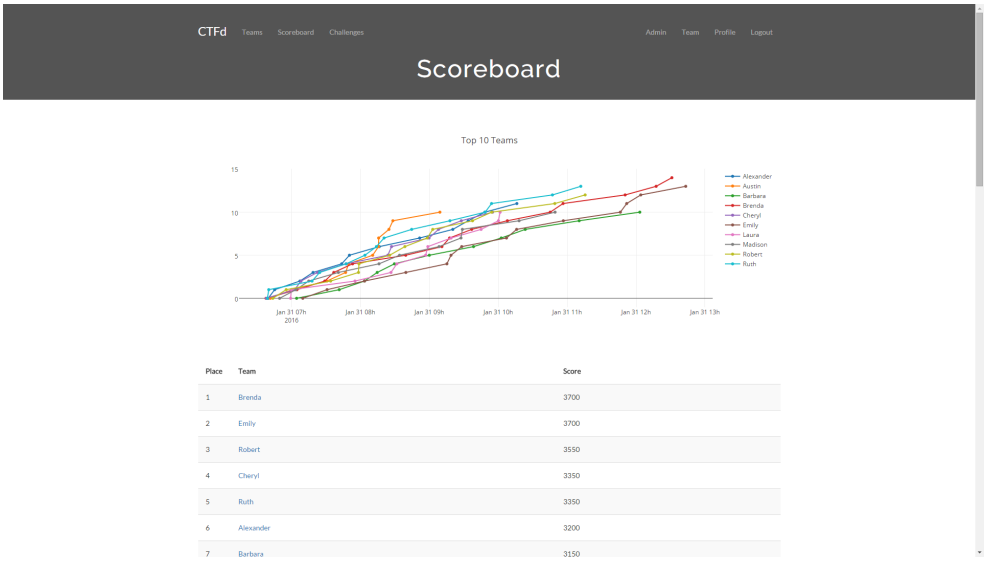
Existuje několik populárních platforem, za jejichž pomoci se dá jednodušeji organizovat a skórovat soutěže těch nejpopulárnějších typů. Toto kritérium sledujeme převážně z toho důvodu, abychom mohli v pozdějších kapitolách posoudit atraktivnost a popularitu jednotlivých platforem. Rozlišujeme tyto platformy:

4.1.7.1 CTFd

CTFd [22] je framework pro Jeopardy CTF soutěže, zaměřený na jednoduchost použití a přizpůsobitelnosti. Mezi jeho hlavní funkce patří registrace a evidence týmů, zprostředkování přístupu týmům k soutěžním otázkám, nabízení nápověd, přijímání správných řešení (odevzdaných vlajek), bodování týmů, skóre tabulky, vyhodnocení soutěže a další.

4.1.7.2 Facebook CTF

FBCTF [63] je platforma zaměřená na hostování Jeopardy CTF soutěží. Skrze jednoduché rozhraní mohou organizátoři soutěže zprostředkovat účastníkům soutěžní úkoly, evidovat týmy a organizovat soutěž. Hlavním rozdílem oproti ostatním platformám a frameworkům je unikátní visuální styl, který má podobu mapy světa. Jednotlivé úkoly se pojí s existujícími státy, což soutěžím dodává unikátní vzhled.



Obrázek 4.1: CTFd Framework

Obrázek 4.2: Facebook CTF

4.1.7.3 picoCTF Platform 2

picoCTF [45] je další platforma zaměřená na Jeopardy CTF soutěže. Jedná se o platformu založenou na infrastruktuře, jež byla použita pro soutěž picoCTF [17], což je CTF soutěž zaměřená na studenty základních a středních škol. Platforma je navrhnuta tak, aby byla co nejjednodušeji modifikovatelná, a aby se dala použít na skórování různých soutěží.

4.1.7.4 Další platformy

Existuje několik desítek různých platforem a frameworků pro jednoduché skórování a hostování soutěží. Podrobněji jsme si popsali ty nejpoužívanější z nich. Dále následuje pouze stručný seznam dalších platforem jež existují.

- HackTheArch [54] - Platforma pro skórování CTF soutěží
- Mellivora [75] - CTF engine napsaný v PHP
- NightShade [89] - Jednoduchý framework pro CTF soutěže
- OpenCTF [106] - Minimalistická CTF platforma
- PyChallFactory [34] - Malý framework na tvorbu a správu úkolů pro Jeopardy CTF soutěže.
- RootTheBox [73] - Hra na hackery, framework pro skórování CTF soutěže spolu s předpřipravenou hackovací minihrou
- Scorebot [46] - skorovací platforma vytvořena pro účely konference Defcon
- SecGen [100] - Aplikace na tvorbu náhodných zranitelných Virtuálních Strojů.

4.1.8 Další sledované atributy

Mezi další sledované atributy, které nepotřebují podrobnější popis, patří:

- Velikost týmů
- Délka soutěže

4.2 Vybrané soutěže

Výběr soutěží probíhal na základě váhy, jenž soutěžím připisuje seznam soutěží *CTF Time* [30], a mého přehledu o populárních soutěžích dle průzkumu subkultury okolo informační bezpečnosti a hacking konferencí. Vybral jsem také soutěže, které jsou zmiňované v akademických článcích, jež jsem používal jako reference k této práci, soutěže pořádané velkými korporacemi jakými jsou například *Google* [49] nebo *Blizzard Entertainment* [13], a také soutěže kterých jsem se osobně účastnil.

Během sbírání dat se ukázalo, že retrospektivně dohledávat konkrétní data jako pravidla, počet soutěžících, či jakou zpětnou vazbu dostali účastníci je

velmi časově náročné, neboť soutěže velmi často nearchivují výsledkové tabulky, nezveřejňují počet účastníků, či jsou organizovány jako součást konference. Velmi často se webové stránky soutěže změní v moment ukončení soutěže, a místo konkrétních pravidel posledního ročníku pouze děkují za účast, a zobrazují jména vítězů (jako například [61]). Informace je tedy nutné dohledávat ze sekundárních zdrojů, webových archivů a různých článků popisujících účast na soutěži. Z toho důvodu jsem pro ilustraci zpracoval pouze 20 soutěží, u kterých se podařilo měřená data získat ze spolehlivých zdrojů.

Vybrané soutěže, spolu s jejich typem a počtem účastníků jsou shrnuté v Tabulce 4.1. Kompletní data jsou k nalezení na přiloženém datovém CD.

Tabulka 4.1: Vybrané soutěže

Soutěž	**Typ**	**Počet soutěžících**
Defcon CTF	Útok-Obrana CTF	15 týmů
picoCtf	Jeopardy CTF	16570 učastníků
National CCDC	Kyberobrana	10 univerzit
Cyber Defence Excercise	Kyberobrana	8 vojenských univerzit a akademií
CSAW CTF	Jeopardy CTF	55 týmů
Ghost in the Shell Code	Jeopardy CTF	321 týmů
Plaid CTF	Jeopardy CTF	1292 týmů
iCTF	Útok-Obrana CTF	317 týmů
Electrolux CTF	Jeopardy CTF	4 týmy
Hack.lu CTF	Jeopardy CTF	242 týmů
ruCTFE	Útok-Obrana CTF	358 týmů
Google CTF	Jeopardy CTF	10 týmů
Accenture CTF	Jeopardy CTF	32 týmů
Hack the Nexus - Blizzard CTF	Jeopardy CTF	Není zveřejněno
H1-702	Jiné	50 týmů
Nuit du hack CTF	Útok-Obrana CTF	10 týmů
Global Cyberlimpics	Jeopardy CTF + Hardware	11 týmů
Hack the World	Bughunting	Není zveřejněno
LASA CTF	Jeopardy CTF	1200 týmů

4.3 Interpretace Pozorování

Je nutno brát v potaz velmi malý vzorek dat, na kterém toto pozorování provádíme. Výběru samotných zástupců soutěží, jejich reprezentativitě a zastoupení každého typu soutěže stejně velikým vzorkem jsem věnoval zvýšené úsilí. Vzhledem k tomu, že větší část pořádaných soutěží jsou soutěže typu Jeopardy CTF, vybrané srovnávané soutěže nemusí nutně reprezentovat celkové zastoupení jejich typu mezi všemi hacking CTF soutěžemi. Z důvodu malého vzorku dat jsem se také rozhodl statistická pozorování týkající se kritérií, jež má tato práce společné s kritérii sledovanými v archívu *CTF Time* [30] zakládat na větším vzorku dat z tohoto archívu, místo na datech získaných v této

práci. S archívem *CTF Time* [30] má tato práce společná pouze kritéria délky soutěže, rozřazení na prezenční/distanční formu účasti, a typ soutěže.

4.3.1 Typy CTF

Dle archivu soutěží které byly organizovány v roce 2017, a které byly zapsány do internetového kalendáře soutěží *CTF Time* [29], proběhlo v daném roce 139 soutěží. Z nich byla naprostá většina (125/139) typu Jeopardy CTF. Nejspíše je to způsobené tím, že soutěže CTF typu Útok-Obrana jsou náročnější na požadovanou infrastrukturu [104] a na znalosti účastníků [15]. Z dvacítky analyzovaných soutěží, dvě, jenž byly pořádané na populárních hacking konferencích, byly CTF typu Útok-Obrana. Obě z těchto soutěží ale měly malý počet účastníků, a kvalifikační kolo, jenž bylo typu Jeopardy CTF.

4.3.2 Zpětná vazba

Zpětná vazba byla analyzována pouze u dvacítky výše vybraných soutěží. V naprosté většině (17/20) případů byla jediná zpětná vazba od pořadatelů zveřejnění tabulky bodů, kterých tým dosáhl. U soutěží pořádaných univerzitami se často objevují akademické práce, které popisují vznik a dopad soutěže [25, 15]. U naprosté většiny soutěží (17/20) využili účastníci možnosti zveřejnit postup, jakým úlohy řešili, ve článcích nazvaných *writeups*. V některých soutěžích je dokonce psaní těchto writeups vyžadováno od vítězných týmů, aby dostali nárok na ceny za své vítězství [83], nebo je za ně poskytována finanční či bodová odměna [48]. Často tyto writeups bývají jediným způsobem pro neúspěšné účastníky soutěží jak zlepšit své dovednosti, a jak se dozvědět jak měli postupovat.

4.3.3 Příprava

Z analyzovaných soutěží neměla naprostá většina (19/20) žádnou speciální přípravu před soutěží. Pouze jediná soutěž obsahovala přípravný set úloh s nápovědou, ke kterým měli studenti přístup před zahájením soutěže [3]. Za jistý způsob přípravy by se také mohla dát považovat existence kvalifikačních kol, která byla přítomna u 6 z 20 soutěží. Účelem kvalifikace ale nebylo připravit účastníky na zvládnutí soutěže, nýbrž vybrat z obrovského počtu zájemců ty nejlepší (a již schopné) účastníky, kteří mohou ve finále zvýšit atraktivitu soutěže.

4.3.4 Počet účastníků

Počet účastníků u analyzovaných soutěží byl dohledáván podle zveřejněných výsledkových tabulek. Data se ale ukazují jako nevypovídající, neboť ve většině případů jsou soutěže týmové, a u žádné týmové soutěže nebyla zveřejněna

velikost týmů. Dalším problémem se ukázal fakt, že na online soutěže se registruje velké množství zájemců, z nichž se jich nezanedbatelný počet nedostaví. Z výsledkových tabulek navíc zpravidla nelze poznat, zda se tým nedostavil, vzdal soutěž, anebo prostě skončil s nulovým počtem bodů. Například na *picoCTF* se dle výsledkových tabulek přihlásilo 16570 týmů. Pokud tento počet vynásobíme maximálním počtem soutěžících za tým, což je 5, získáme tím horní strop 82850 účastníků. Vezmeme-li v potaz že se jedná o soutěž pro studenty středních škol, číslo se jeví být velmi zavádějícím. I do kvalifikace na nejprestižnější CTF soutěž, jenž je pořádána na konferenci DEFCON [37], a na které účast byla odměnou za první místo v množství analyzovaných soutěží, se přihlásilo pouze 368 týmů [2]. Tento obrovský rozdíl mezi přihlášeným počtem účastníků na soutěž pro studenty střeních škol oproti počtu účastníků na celosvětově nejprestižnější CTF soutěži se jeví jako velmi podezřelý, a z toho důvodu si myslím, že způsob, jakým byla data odhadnuta, nebyl vypovídající, a nemůžeme z něj vyvozovat významné závěry.

4.3.5 Závěr pozorování

Vzhledem k rozmanitosti organizovaných soutěží, a velmi obtížnému způsobu sběru dat, není v možnostech této práce vypozorovat statisticky významná data. Zvolená velikost vzorků se ukázala jako nedostatečná, což je nejlépe vidět na počtech soutěžících, a délkách soutěží, ve kterých nelze pozorovat žádný trend. Soutěže jsou opravdu rozmanité.

Ukázalo se ale, že k naprosté většině (17/20) pozorovaných soutěži lze na internetu jednoduše vyhledat řešení (writeups) některý úloh, které se na ní objevily, a že některé soutěže tvorbu a zveřejnění těchto postupů přímo vyžadují od vítězů [83]. Naopak samotné přípravě soutěžících před soutěží se nevěnovala téměř žádná ze zkoumaných soutěží. Všechny pozorované soutěže kladly hlavní důraz na poměřování znalosti účastníků.

Kapitola 5

Gamifikace

Idea gamifikace se ve světě vyskytuje již dlouho. Věrnostní programy, jež se dají v omezené míře považovat za gamifikaci [58], se na světě vyskytují již od 18. století, kdy američtí prodavači přidávali ke každému nákupu měděné mince, které se při dalších nákupech u toho samého prodejce dali proměnit v odměny a jiné produkty [65]. Stále se ale jednalo o velmi povrchní použití idejí, které jsou dnes známy jako gamifikace. V poněkud interaktivnější formě, která je dnešnímu pohledu na gamifikaci o něco bližší, tyto techniky použila v 60 letech firma Weight Watchers [107], jež pomáhala lidem hubnout. V té době ale samotný pojem gamifikace známý nebyl, a trvalo ještě mnoho let, než se uchytil. Teprve v prvních deseti letech nového tisíciletí začal být tento fenomén herního přístupu rozeznáván, a pod klíčovými slovy jako *herní dynamika*, *participační jádro* [participation engine], *herní taktiky* [game tactics] nebo *osvědčená praxe účasti* [engagement best practices] zapojován do řady věrnostních programů a podnikání [58].

5.1 Co je gamifikace

Přesná definice gamifikace se jen složitě hledá, neboť při pokusech o jednoznačné vyjádření celé složité idey gamifikace je naráženo na stejné problémy, jako při pokusu definovat co je přesně hra. Ještě v roce 2012, bylo kolem 25 až 45 procent času na konferencích o gamifikaci věnováno diskuzím o tom, co vlastně je a co není gamifikace [88]. Nejprve je ale potřeba definovat, co je tedy přesně hra.

5.1.1 Definice hry

V knize *Art of Game Design: A Book of Lenses* [94], která je uznávaná jako jedno z nejlepších literárních děl na téma herního designu [10], věnuje Jesse Schell pokusu o definici *hry* [game] a *hraní si* [play] celou kapitolu, jejímž výsledkem jsou tyto definice:

- Zábava je potěšení s překvapením.
- Hraní si je manipulace jenž uspokojuje zvědavost.
- Hračka je objekt se kterým si hrajeme.
- Dobrá hračka je objekt se kterým je zábava si hrát.
- Hra je aktivita řešení problémů, ke které přistupujeme s hravým postojem.

Dalším z uznávaných autorů na poli herního designu [47] je autorka Jane McGonigal, která ve své knížce *Reality is Broken: Why Games Make Us Better and How They Can Change the World* [68], definuje pojem *hra* těmito čtyřmi vlastnostmi:

- Každá hra má cíl, kterého se hráči snaží dosáhnout.
- Každá hra má pravidla, která omezují způsob jakým mohou hráči cíle dosáhnout.
- Každá hra má systém zpětné vazby, který hráčům naznačuje jak blízko jsou dosažení cíle.
- Každé hry se účastníci účastní dobrovolně.

Jsou-li tyto definice od uznávaných autorů na poli herního designu porovnány, je vidět, že společného toho na první pohled nemají mnoho, přitom ale oboje popisují to samé. Lze tím ilustrovat obtížnost, s jakou se dá abstraktní pojem jako je *hra* definovat, a nakonec se dochází k tomu, že naprosto přesná a neprolomitelná definice není potřeba, neboť v umění (kterým herní design nepochybně je) záleží velmi na subjektivní definici autora, a u každé definice se dá najít nějaký okrajový případ, který by ji vyvracel [94].

5.1.2 Definice gamifikace

S definicí gamifikace je to ještě složitější. Samotný pojem *gamifikace* byl poprvé použit Britským programátorem Nickem Pellingem v roce 2002, ale do populárního povědomí se dostal až kolem roku 2010 [55]. Velmi rychle se z něj stal trend, a již v roce 2011 byl pořádán první Gamification Summit v San Francisku [44].

Samotných definic gamifikace koluje po konferencích a vědeckých pracích několik. Za ty nejcitovanější z nich vybral Craig Miller v článku *Gamification of Education* [71] tyto definice:

- Gamifikace je proces použití *herního myšlení*[1] [game thinking] a herních mechanik pro řešení problémů. [39]
- Gamifikace je použití herních mechanik, dynamik a frameworků pro vyvolání požadovaného chování. [60]

[1] „Použití her a hrám-podobných přístupů k řešení problémů a tvorbě lepších zážitků.“ [64]

- Gamifikace je použití herních mechanik, estetiky a *herního myšlení* pro zaujmutí lidí, motivaci k činu, podpoření učení a řešení problémů. [56]

Tyto definice jsou ale velmi obecné, a velmi těžko se pod nimi představuje něco konkrétního. O něco přímočařejší definice se nachází v přednášce autora gamifikačního frameworku *Octalysis* [20]:

- Gamifikace je převzetí zábavných elementů z her, a jejich použití na nudnou práci [21].

A co se týče významu a budoucnosti gamifikace, názory se na to liší. Diskuze okolo tohoto tématu se dají shrnout do dvou pohledů. První pohled je zastáván designéry jako Jesse Schell nebo McGonigalová, *„jenž věří, že výsledek gamifikace bude, že se všichni proměníme v obrovské koule světla, a bezstarostně se vzneseme do kosmu ve věčném štěstí a úžasu.“* [88] Tyto slova pronesl Scott Rigby ve své přednášce [88] na konferenci *GDC Online 2012* [102], a snažil se tím shrnout tento úhel pohledu na gamifikaci. Poněkud formálněji jde o pohled, jenž v gamifikaci spatřuje řešení spousty problémů lidstva, a zastává svým způsobem utopickou vizi budoucnosti, kde bude vše gamifikované (a tudíž zábavné), místo práce bude vše hra a lidé budou své povinnosti plnit dobrovolně, a ještě se při tom dobře bavit [66, 95].

Druhý pohled je o něco více negativní. Dle něj, je gamifikace zákeřná manipulace, jenž zneužívá znalostí psychologie a herního designu k tomu, aby donutila uživatele investovat více času nabízené (a často prodávané) službě za virtuální odměny, které nemají žádnou hodnotu [14]. Varují před budoucností kde *„Svět je plný triků, i digitálních lží,“* [16] a spatřují v ní velký etický problém [88].

5.2 Co není gamifikace

Gamifikace se velmi rychle stala trendem. Podnikatelé nabízející zapojení gamifikace do podnikání slibovali zákazníkům zdánlivě nevídané věci. Na stránkách nabízejících gamifikované platformy se v roce 2010 nacházely sliby jako „O 200% více sociálních doporučení“ [social refferals], nebo „o 75% větší účast [engagement] uživatelů“. V některých případech se také dalo narazit na termíny jako „672% nárůst účasti uživatelů“ [88].

Netrvalo dlouho, a objevil se první problém, který otázku „Jak implementovat gamifikaci?“ velmi zkomplikoval. Tento problém nebyl v počátcích patrný, neboť se jednalo o problém dlouhodobý, který začal být patrný až v momentě kdy se tento trend gamifikace rozmohl, a stal víceméně všudypřítomným [88]. S rychlostí s jakou se gamifikace stávala čím dál tím populárnější, a s její pověstí „magického“ řešení veškerých business problémů, začalo velké množství podnikatelů hledat co nejjednodušší a zaručený postup, jak

gamifikaci implementovat. A tak vznikla idea „Bodů, Odznaků a Žebříčků“[2] [Points, Badges and Leaderboards], která se na několik let stala synonymem pro praktickou gamifikaci, k velké nelibosti herních designerů a akademické sféry [38]. Stalo se tak převážně proto, že použití vnějších [extrinsic] odměn (jejichž opakem jsou vnitřní [intrinsic] odměny) má následující výhody [88]:

- Jednoduše implementovatelné.
- Zdánlivě univerzální přístup, který lze přizpůsobit různým druhům podnikání.
- Rychle viditelné krátkodobé výsledky - rychlý nárůst účasti uživatelů.

Jedním z hlavních argumentů proti tomuto přístupu ke gamifikaci, je jeho krátkozrakost. Herní designérka Margaret Robertson popsala ve svém článku *„Can't play, won't play“* [90] tento přístup citátem: „*To, co momentálně nazýváme gamifikací je ve skutečnosti proces, ve kterém používáme ty nejméně důležité věci na hrách, a předvádíme je jako základ herního zážitku.*“ (překlad z originálu [90]) Základem her (a tudíž i gamifikace) není tato vnější zpětná vazba ve formě bodů, odznaků a žebříčků, nýbrž možnost provádět zajímavá rozhodnutí, při pronásledování zajímavě složitých cílů.

Toto zneužití a nepochopení gamifikace [38] bylo hlavním tématem konferencí a akademických článků vycházejících na téma gamifikace následujících několik let. Prezentace s názvy jako *„Gamification: That Word Doesn't Mean What You Think...“* [88], nebo *„We Don't Need No Stinkin' Badges: How to Re-invent Reality Without Gamification“* [67], se staly běžnou součástí konferencí, a téměř každá práce která vycházela na toto téma v sobě obsahuje zmínku o tom, že „Odznaky, Body a Žebříčky“ nejsou pro implementaci gamifikace dostatečné [20, 60, 38, 88, 67].

5.3 Gamifikace v praxi

V dnešní době lze nalézt případy gamifikace téměř všude. Jedním z dosud nejvíce citovaných použití gamifikace, které spustilo tento celý trend, byla aplikace *Foursquare* [43], jež k obrovskému úspěchu využila herní mechaniky, a vnější odměny [extrinsic rewards], čímž zvedla míru účasti uživatelů a velmi rychle se stala jednou z nejpopulárnějších aplikací na své části trhu [110]. *Foursquare* byl zajímavý převážně svou historií. V roce 2003 založila dvojice studentů mobilní službu s názvem *Dodgeball*, jenž zastávala funkci sociální sítě, která spojovala uživatele na základě jejich aktuální polohy, a upozorňovala je na přátele, přátele přátel a zajímavá místa v okolí. O dva roky později byla společnost vlastnící *Dodgeball* odkoupena firmou *Google LLC* [49], a za dalších

[2] Zjednodušeně se jedná o přiřazení odměny ve formě virtuálních bodů jako odměnu za účast uživatelů, ocenění ve formě odznaků za dosažení větších cílů, a žebříčků porovnávajících uživatele mezi sebou.

několik let byl projekt zrušen, a nahrazen službou *Google Latitude*. Původní autoři služby *Dodgeball* ale neváhali, a v okamžiku, kdy to bylo právně možné, vytvořili nový pokus o sociální sít založenou na aktuální poloze - *Foursquare*. Tentokráte ale, na rozdíl od původní iterace *Dodgeball*, sociální sít gamifikovali, což vedlo k jejich rychlému růstu a popularitě [110], jenž trvá dodnes [11].

Ve své prezentaci o gamifikačním frameworku *Octalysis* [21] uvádí Yu-Kai Chou několik dalších příkladů služeb, které gamifikaci úspěšně implementovali:

- *Pain Squad* [52], mobilní hra, která pomáhá dětem s rakovinou pravidelně zaznamenávat své bolesti. Děti v rolích agentů speciální *Jednotky Bolesti* pravidelně sledují a zaznamenávají, kde cítí bolest, a tím před ní zachraňují svět.
- *Nike+* [79], jenž implementuje gamifikaci do fitness a cvičení. Za pomoci fitness náramku uživatelé monitorují své výsledky, za něž získávají zpětnou vazbu v aplikaci, ve které se také mohou porovnávat s přáteli, či sdílet své pokroky na sociálních sítích.
- *Foldit* [103], počítačová hra, jež je součástí výzkumného projektu Washingtonské univerzity. Hráči v ní pomocí různých pomocných metod vytvářejí struktury vybraných bílkovin. Nejpovedenější výsledky jsou dále zkoumány výzkumníky.
- *Speed Camera Lottery* [87], rychlostní radar, který přidává řidiče, jenž kolem něj projíždí bezpečně a pomalu, do slosovaní o peněžní odměny, které jsou financovány z pokut řidičů, které radar přistihne při překračování maximálně povolené rychlosti.
- *Zombies, Run!*, fitness mobilní aplikace, ve které se hráč dostane do role přeživšího při zombie apokalypse. Při běhu si uživatel z aplikace přehrává audioknihu, ve které je mu poutavě popisováno, jaké je kolem něj množství zombie, a jak rychle musí utíkat aby nebyl chycen a zkonzumován.

5.4 Gamifikace a výuka

Výuka je jedno z odvětví, kterému je přisuzována velká míra uplatnění gamifikace, neboť má potenciál zvyšovat motivaci studentů. Zároveň se také jedná o odvětví, které názorně demonstruje, že nestačí pouze vzít herní prvky jako body, odznaky a žebříčky, a nekoncepčně je propojit s činnost pro dosažení pozitivní motivace a pocitu hry místo práce. Škola je totiž v určitých ohledech ideálně gamifikovaná zkušenost. Studenti dostávají body za splnění úkolů, jež se mění na herní měnu ve formě známek. Studenti jsou odměňováni za vhodné chování, a trestáni za nevhodné použitím známek (herní měny) a odznaků ve formě vyznamenání a pochval. Pokud jsou studenti dostatečně pilní, na konci roku se jim „zvýší úroveň“ a dosáhnou vyššího stupně vzdělání. I přes existenci těchto herních mechanik školy ve studentech mohou vzbuzovat negativní chování jako např. podvádění a naučenou bezmocnost. Většina studentů by

aktivity ve škole nepopsala jako hru. Z toho plyne, že pouhá existence herních elementů nevede k zvýšení zapojení studentů a samo o sobě nestačí [60].

5.4.1 Gamifikace ve výuce v praxi

I přes tuto zdánlivou složitost praktické aplikace byla gamifikace ve výuce použita již na několika místech. Objevují se případy předmětů, jenž jsou s velkým úspěchem vedeny jako masivní multiplayer hry. Studentům jsou např. přidělovaní *„zkušenostní body“* místo známek, získávají úrovně nebo mají své školní alter-ego s vlastním virtuálním vybavením, jež jim poskytuje výhody [98]. Toto téma je ale ještě málo rozšířené, neboť systém jakým je vedena a uzákoněna výuka ve veřejném školství není dostatečně flexibilní na to, aby se tyto techniky daly prakticky využít ve větším měřítku.

Vysokoškolský učitel medicíny *Dr. Christopher See* [97] si během své kariéry všiml, že fenomén her známých jako *úniková místnost*[3] a zkušenost, jež studenti zažívají při řešení zkouškových úloh ve škole, jsou si velmi podobné. Při řešení únikové místnosti hráči:

- Řeší imaginární problémy
- Zapamatovávají si informace
- Hledají vzorce v datech
- Komunikují o svých nápadech
- Pracují pod tlakem
- Mají omezený čas

Což je dle *Dr. See* téměř identický soubor aktivit, které student zažívá u zkoušky. Hlavní rozdíl mezi zkouškou a únikovou místností je fakt, že data, se kterými hráči pracují v únikové místnosti, jsou smyšlená a mimo hru nevyužitelná. Ve snaze udělat učení anatomie atraktivnější, použil autor koncepty jako je anatomie a fyziologie, na jejich základě postavil únikovou místnost, ve které studenti pracují s reálnými informacemi [97]. Výsledkem například bylo, že třída studentů strávila nezanedbatelnou část času u tabulky, ve které byla hádanka pracující s názvy hormonů v těle, a diskutovala o tom, co dělá který hormon, jak funguje, a navzájem si předávali znalosti a fakta, ve snaze vymyslet další postup.

Dalším praktickým případem, při kterém byla gamifikace prakticky použita ve výuce, bylo využití herních mechanik k zatraktivnění e-learningové platformy určené k výuce elektrotechniky v Ukrainské Technické Univerzitě v Kluži [101]. Témata úkolů e-learningu byla rozdělena do kategorií. Postup spolu s dosaženými výsledky každého studenta byl zveřejněný v abstraktní formě odznaků, které značily studentův stupeň dokončení dané kategorie.

[3] Úniková místnost je aktivita, při které je tým několika lidí zamčen do místnosti plné tematických hádanek, a cílem hry je do vypršení časového limitu vyřešit danou posloupnost hádanek, a tím otevřít východ a z místnosti uniknout.

Toto rozdělení a nezávislé hodnocení podle kategorií způsobilo, že studenti rychle demonstrovali to, co umí, a následně sháněli pomoc u jiných studentů jiného zaměření (a tedy s lepším skórem v odlišné kategorii úkolu). Studenti také byli odměňováni odznaky za významné úspěchy, jako například „První řešitel“, nebo „Nejrychlejší řešitel“. Tento přístup zvětšil zájem studentů o e-learning a také způsobil zvýšení zpětné vazby od studentů, kteří přicházeli s nápady a návrhy jak platformu vylepšit, aby byla zajímavější [101].

5.5 Jak správně použít gamifikaci

Dle poznatků v předchozí části této kapitoly se nezdá, že by existoval jeden zaručený způsob, jakým gamifikaci aplikovat. Kapitola nás téže vede k závěru, že hlavním faktorem v úspěchu aplikace gamifikace je návrh designu, který je potřeba přizpůsobit problému, jež se prostřednictvím gamifikace pokoušíme vyřešit. Existuje však celá řada ucelených softwarových frameworků, které přístup k tomuto problému zjednodušují a rozdělují na konkrétnější dílčí problémy. V této podkapitole budou popsány některé systémy, jež podávají konkrétnější představu o tom, jaké jsou klíčové vlastnosti gamifikovaných systémů, a na co se při jejich návrhu zaměřit.

5.5.1 Octalysis Framework

Jedním z ucelených přístupů ke gamifikaci je *Octalysis Framework* [20], který byl navržen průkopníkem gamafikace, Yu-kai Chou. Základní ideou tohoto přístupu je zaměření se na osm klíčových motivací, které udržují hráče investované do her, jež hrají. Veškeré mechaniky, které používá gamifikace, se, podle Chou, dají rozdělit do těchto kategorií. Ideálním výsledkem je produkt navržený tak, aby obsahoval mechaniky pro každou z těchto oblastí motivace [21].

Správně implementovaný gamifikační systém tedy využívá všechny tyto klíčové motivace, což návrháři poskytuje dobrý výchozí bod. V této práci budeme tento systém používat při návrhu funkčních požadavků.

Níže naleznete seznam těchto osmi klíčových oblastí motivace, na který navazuje podrobnější vysvětlení každého z nich:

- Grandiózní smysl a poslání [Epic Meaning and Calling]
- Vývoj a úspěchy [Development and Accomplishment]
- Posílení kreativity a zpětná vazba [Empowerment of Creativity and Feedback]
- Vlastnictví a majetek [Ownership and Possession]
- Sociální vliv a sounáležitost [Social Influence and Relatedness]
- Nedostatek a netrpělivost [Scarcity and impatience]
- Nepředvídatelnost a zvědavost [Unpredictability and Curiosity]
- Ztráta a předcházení [Loss and Avoidance]

5.5.1.1 Grandiózní smysl a poslání

Tato klíčová motivace je způsobena lidskou touhou a potřebou být součástí něčeho většího. Uživatelé jsou díky této klíčové motivaci ochotni interagovat se systémem nikoliv proto, že by z toho měli nějaký přímý zisk, ale proto že tím pomáhají nějaké dobré myšlence. Vzorovým příkladem této motivace v praxi je internetová encyklopedie *Wikipedia* [109], pro kterou jsou tisíce uživatelů ochotni bez jakékoliv kompenzace moderovat, upravovat, psát a aktualizovat informace na miliónech stránek o různorodých tématech a pojmech, neboť z nich toto přispívání dělá *„hrdiny, jež ochraňují kolektivní znalosti lidstva“* [19]. Jimi odvedená práce je důležitější než jakýkoliv jednotlivec a pozitivně se dotkne milionů lidí po celém světě. To je jejich grandiózní smysl a poslání.

5.5.1.2 Vývoj a úspěch

Klíčová motivace touhy po vývoji a úspěchu motivuje hráče dokončovat začaté úkoly skrze pocit postupu k dosažení kýženého cíle. Pro využití této klíčové motivace je potřeba uživatelům dávat výzvy, jež pro ně nejsou ani příliš složité (hráč je frustrován), ani příliš jednoduché (hráč se nudí). Tyto výzvy by tedy měly být optimalizovány podle postupu a znalostí každého uživatele, s postupně stupňovanou obtížností. Tím, že uživatelé uvidí svůj postup v plnění dané výzvy, jsou motivováni k tomu toho nezanechat a pokračovat dál.

5.5.1.3 Posílení kreativity a zpětná vazba

Lidé mají potřebu se kreativně projevovat. Tato motivace je založena právě na této potřebě. Na této motivaci je založena idea *LEGO* produktů, jež jsou pouze kostičky, se kterými si hráči mohou postavit, co chtějí. Dát hráčům možnost kreativně se projevovat, a zkoušet si své nápady, je jedním z dobrých způsobů jak si udržet jejich zájem. Uživatel bude se systémem interagovat, protože naplňuje jeho potřebu tvořit, a cítí se díky tomu dobře.

5.5.1.4 Vlastnictví a majetek

Tato motivace je založena na potřebě lidí ochraňovat, zlepšovat a získávat více virtuálních předmětů, o kterých se domnívají, že je vlastní. Nejedná se pouze o touhu akumulovat bohatství (i když ta pod tuto motivaci spadá), může se jednat například o motivovaného manažera, který se stará o „svůj“ projekt. Této motivace lze využít nejen ve formě odměn ve virtuální měně a věcí, ale také například tím, že svěříme uživateli zodpovědnost. Tato touha něco ochránit uživatele udrží motivovaného.

5.5.1.5 Sociální vliv a sounáležitost

Sociální vliv je jednou z motivačních sil, které fungují velmi dobře. Nikdo nechce být tím nejhorším v okruhu svých přátel. Když někomu ukážete, že jejich průměrná spotřeba elektřiny za měsíc je o pět procent vyšší než průměrná spotřeba v celé jeho ulici, v následujícím měsíci může být více motivován tuto spotřebu snížit. Tento přístup vyzkoušel projekt *OPOWER*, jenž každý měsíc posílal svým klientům výpis se statistikami, ve kterých porovnával, jak nakládá zákazník s elektřinou, vodou a dalšími službami v porovnání se svými sousedy. Do roku od spuštění tohoto projektu ušetřily domácnosti přes 250 milionů dolarů na ceně za služby [21].

5.5.1.6 Nedostatek a netrpělivost

Motivační síla za tímto bodem spočívá ve faktu, že člověk vždy chce to, co nemůže ihned mít, nebo co je vzácné. Na tomto principu jsou postaveny crowdfunding řešení jakým je například *Kickstarter* [57], které většinou nabízí produkty, jež jsou jedinečné, a pouze pro zákazníky kteří přispějí na projekt. Tato rarita přidává v očích uživatele hodnotu produktu a je motivační silou za tím, proč si produkt nakonec pořizuje.

5.5.1.7 Nepředvídatelnost a zvědavost

Jelikož lidé nevědí, co bude následovat, stále o tom přemýšlí. Jedná se o motivační sílu, která je nejvíce používaná v odvětví gamblingu, ale také o sílu, jež nás nutí dokončit čtení knihy či sledování filmu. Překvapení vyvolává příjemnou reakci, a to i když se jedná o překvapení nepříjemné [94], a proto je klíčovou motivační silou gamifikace.

5.5.1.8 Ztráta a předcházení

Tato motivační síla je přímočará - člověk je motivován konat, aby předešel nějaké hrozící ztrátě. Například může jít o hráče kontrolujícího a zalévajícího několikrát denně květiny na své virtuální farmě ve hře *Farmville* [111], aby předešel ztrátě virtuální úrody.

5.5.2 Gameful design

Gameful design je pohled na použití gamifikace prezentovaný *Jane McGonigalovou* [67]. Dle ní, se při návrhu gamifikovaných systémů nelze dívat pouze na herní mechaniky, ale je potřeba mluvit o „duši“ her, o tom co dělá hry dobré, a z jakého důvodu. Tomuto přístupu říká *„gameful design“*. Podobně jako *Octalysis* identifikuje 4 kategorie, na které je potřeba se při návrhu zaměřit. Dobrý gameful design je hodnocen podle těchto 4 aspektů:

- Positivní emoce [Positive Emotion] - Zvyšuje hra štěstí, zdraví a kvalitu života hráčům?
- Vztahy [Relationships] - Buduje hra pozitivní vztahy mezi účastníky?
- Smysl [Meaning] - Zapojuje hra hráče do něčeho, co je větší než oni? Smysl, mise, kolektivní cíl.
- Úspěchy [Accomplishment] - Dává hra hráčům možnost budit se každé ráno s pocitem, že dosáhli něčeho smysluplného?

Dle McGonigalové je třeba se zaměřit na tyto 4 hodnoty, spíše než na „body, odznaky a žebříčky“, a sice z důvodu, že tyto 4 hodnoty se zaměřují na vnitřní hodnoty, které jsou pro lidi zajímavější než vnější hodnoty (jimiž jsou výše zmiňované body a žebříčky). Vnitřní hodnoty se promítají v aktivitách, které děláme pro ně samé, aniž bychom za to vyžadovali nějaké vnější odměny. Jedná se také o 4 aspekty šťastného a smysluplného života [67].

Tyto 4 aspekty korespondují se 4 silnými stránkami a schopností hráčů her, které jsou následující [66]:

- Blažená produktivita [Blissful Productivity] - Hráči jsou ochotni trávit hodiny řešením problémů při hraní her a brát to jako zábavu.
- Sociální struktury [Social Fabric] - Hrát s někým hry vyžaduje velké množství důvěry a buduje silnější vztahy mezi lidmi.
- Urgentní optimismus [Urgent Optimism] - Extrémní sebe motivace, chuť konat okamžitě, vyřešit problém, spojená s vírou, že hráč má šanci na úspěch.
- Grandiozní smysl [Epic Meaning] - Touha po větším smyslu života. Spojení se s něčím, co má smysl mimo jednotlivce.

V praxi je gameful design velmi podobný frameworku Octalysis. Na první pohled je vidět podobnost mezi některými body Octalysisu a gameful designu. Samotné použití gameful designu může vypadat například takto [67]:

- Pro vyvolání pozitivních emocí a využití urgentního optimismu potřebují hráči nějaký cíl, který se dobrovolně rozhodnou řešit. Nabízet hráčům dobrovolné cíle a probouzet v nich zvědavost je jedním ze způsobů jak těchto vlastností využít.
- Pro tvorbu dobrých vztahů mezi hráči je nejlepším přístupem nechat hráče využívat silné stránky své osobnosti, a na jejich základě pomáhat druhým. Příkladem jsou léčitelé v masivních mutliplayer online hrách, za něž často hrají altruističtí hráči.
- Pro přidání *grandiózního smyslu* do svého designu je potřeba přemýšlet ve velkém měřítku, mít jasný cíl svého projektu a mít dobrý příběh, který hráče upoutá.
- Pro naplnění touhy po vývoji a výsledcích je důležité dát hráčům nějaké konkrétní a nové schopnosti, začít s něčím malým, co se postupně rozroste a zlepšuje do něčeho velkého.

Kapitola 6

Specifikace požadavků

6.1 Úvod

V předchozí části práce byl uskutečněn průzkum současného stavu, ve kterém se nachází myšlenky gamifikace a výuky systémové bezpečnosti skrze interaktivní simulace, soutěže a počítačové hry. V této kapitole bude využito získaných poznatků, a navrhnut systém, který se zaměří na zmírnění negativních dopadů gamifikace zmíněných v předchozích kapitolách, a co největšího využití aktivního praktického přístupu k výuce systémové bezpečnosti a etického hackingu.

Specifikace požadavků byla vytvořena na základě šablony dle standartu *ISO/IEC/IEEE 29148:2011* [6], která byla mírně upravena pro potřeby této práce. Z šablony byly vynechány některé části, které se zabývají definicemi a referencemi, neboť se jedná o informace, jež jsou zmíněné v předchozích kapitolách. Také došlo k vynechání detailnějších částí šablony, neboť požadavky na systém nedosahovali dostatečné úrovně detailů. Vzhledem k volnosti ve výběru a návrhu řešení, iterativní metodě vývoje a obšírností tématu, se kterou byla tato práce zadána, docházelo k postupnému aktualizování a úpravě specifikace požadavků v průběhu životního cyklu vývoje práce. V této kapitole se nachází finální podoba specifikace požadavků, jež byla výsledkem několikerých schůzek s vedoucím práce.

6.1.1 Účel

Účelem této kapitoly je představit detailní popis vyvíjeného systému s názvem *BI-EHA Task Force*. Bude zde vysvětlen účel a rozhraní systému, jeho funkce a omezení, pod kterými bude systém provozován. Kapitola je určena pro uživatele a administrátory systému a potencionální vývojáře, jež budou systém rozšiřovat.

6.1.2 Rozsah systému

BI-EHA Task Force je webová platforma, která uživatelům zábavnou formou (za použití gamifikace) zpřístupňuje praktické úkoly z oboru hackování. Uživatelům představuje zadání úloh, dává jim možnost odevzdávat a zveřejňovat své postupy řešení, a navzájem se mezi sebou kontaktovat s dotazy ohledně úkolů. Hlavní zaměření funkce systému je na podporu sociálního aspektu výuky, zatraktivnění úkolů za použití silného tématu a příběhu, a jednoduchého přístupu ke zpětné vazbě, jenž je nejdůležitější součástí praktické výuky.

Systému bude použit při výuce kurzu *Etického Hackování*, jenž je vyučován na *Fakultě informačních technologií ČVUT* [112].

Součástí systému je i set několika úloh, jenž obsahují nejdůležitější okruhy ze sylabu kurzu *Etického Hackování*, na kterých si uživatelé mohou ozkoušet své znalosti.

6.2 Všeobecný popis

6.2.1 Kontext produktu

BI-EHA Task Force systém je vyvíjen pro studenty a vyučující se zájmem o ofenzivní systémovou bezpečnost, hackování, penetrační testování a hacking CTF soutěže.

Skrze webové rozhraní umožňuje administrátorům spravovat zadané úlohy, uživatele, a hodnotit odevzdané postupy řešení. Běžní uživatelé mohou skrze webové rozhraní přistupovat k úlohám, odevzdávat řešení, odevzdávat postupy řešení a navzájem se kontaktovat. Gamifikační složka slouží jako dodatečná motivace uživatelům více interagovat se systémem.

Systém je vyvíjen pro populární webové prohlížeče *Firefox*, *Chrome*, *Internet Explorer*, *Opera* a *Safari*, při zobrazení na stolním počítači. Podpora mobilních zařízení není vyžadovanou součástí tohoto systému.

Úlohy, jež jsou součástí systému, jsou zaměřeny na sylabus kurzu *Etického Hackování* ze školního roku 2017/2018, a jsou vyvinuty pro vypracovávání na systému *Linux*.

6.2.2 Profil uživatelů

- Běžní uživatelé, jako např. studenti, již systém používají v rámci kurzu. Jejich hlavním cílem je vyřešení zadaných úloh, a získání zpětné vazby.
- Administrátoři, jako např. učitelé, jež systém využívají k vedení kurzu. Jejich hlavním cílem je zpřístupnit svým studentům zadání úkolů, a hodnotit jejich interakce a postupy řešení.
- Vývojáři, kteří mají zájem o rozšíření systému o další funkce. Jejich hlavním požadavkem je jednoduchost modulace systému.

6.2.3 Přehled omezujících podmínek

Vzhledem k nedostatku softwarových nástrojů používaných k řešení úloh etického hackování pro operační systémy *Windows* a *MacOS* je nutné pro úlohy používat prostřední OS *Linux*.

Krátké časové okno dostupné pro implementaci, a velký rozsah projektu vylučuje možnost vytvářet novou webovou platformu, a vynucuje použití a úpravu nějakého z existujících řešení.

Kurz *Etické Hackování* je vyučován v anglickém jazyce, tudíž je volba jazyku obsahu aplikace omezena na AJ.

6.3 Specifikace požadavků

6.3.1 Požadavky na rozhraní

- Interakce se systémem probíhá za použití webového prohlížeče na stolním počítači.
- Administrátorské rozhraní je znatelně odděleno od uživatelského.
- Uživatelské rozhraní využívá některé z technik gamifikace.

6.3.2 Požadavky na funkce

6.3.2.1 Úlohy

Systém poskytuje uživatelům přístup k zadání úloh, souborům, a datům potřebným k jeho řešení. Uživatelé mohou zadání číst, a odevzdávat odpovědi na otázky v úlohách. Systém jejich odpovědi zkontroluje, a v případě správnosti přiřadí danému uživateli body dle obtížnosti úlohy.

Úlohy jsou rozděleny do celků zvaných „případ“, a v rámci případu jsou uživatelům zpřístupněny v pořadí určeném v zadání.

K úlohám je možné připojit nápovědu. Přístup k nápovědám je uživatelům omezen, aby byl omezen počet případů, ve kterém uživatel ihned po přečtení zadání úlohy přečte také všechny nápovědy.

Součástí systému je také ukázkový set zadání úloh, který je zaměřený na osnovy kurzu *Etického Hackování*.

6.3.2.2 Bodování a uživatelské účty

Pro interakci se systémem je vyžadován uživatelský účet. Systém obsahuje následující funkce spojené s těmito účty:

- Registrace nového uživatele: Registrace je omezena pouze na účty studentů a zaměstnanců vysoké školy *České Vysoké Učení Technické*.
- Autentizace již registrovaného uživatele za použití hesla a uživatelského jména zvoleného při registraci.

- Bodování uživatelem splněných úloh.
- Žebříček uživatelů dle počtu bodů a splněných úloh.
- Zajištění přístupu k úlohám uživateli.
- Funkce zpětné vazby a sociální interakce mezi uživateli, které jsou popsané níže.
- Rozdělení rolí uživatelů na administrátory, a běžné uživatele

6.3.2.3 Administrace

Uživatelé s rolí administrátora mají přístup k následujícím funkcím:

- Administrace úloh, přidávání, úprava a mazání zadání úloh. K úlohám lze připojit soubory, nápovědy, a více možných řešení.
- Administrace uživatelů, možnost přidávat, mazat a upravovat uživatelské účty.
- Součástí administračního rozhraní jsou statistiky, které sledují počet správných a špatných odpovědí uživatelů, počet řešení jednotlivých úloh, počet uživatelů, a IP adresy ze kterých se uživatelé připojují.
- Administrátor má přístup ke čtení, správě a hodnocení postupů řešení, které uživatelé odevzdávají v rámci funkcí zpětné vazby popsané níže.

6.3.2.4 Zpětná vazba

Funkce zpětné vazby zajišťují uživatelům přístup ke zpětné vazbě ohledně způsobu, jakým zadané úkoly řešili.

- Uživatelé mohou odevzdat zprávu o způsobu jakým řešili jednotlivé úlohy v rámci případu.
- Administrátoři mohou odevzdané zprávy hodnotit, a posléze je zpřístupnit ostatním uživatelům.
- Přístup ke zprávám ostatních uživatelů je uživatelům umožněn.
- Přístup ke zprávám ostatních uživatelů je omezen, aby nebylo možné vyřešit všechny úlohy pouhým zkopírováním postupu ostatních uživatelů.

6.3.2.5 Sociální interakce uživatelů

Systém zpráv a žádosti o pomoc umožňuje uživatelům kontaktovat ostatní uživatele v rámci jednotlivých úkolů s žádostí o radu a pomoc s řešením. Systém umožňuje:

- Uživatel si zvolí oblasti specializace, ve kterých je ochotný nabízet ostatním pomoc.
- Uživatel má možnost pří řešení úkolu kontaktovat ostatní uživatele, kteří mají zvolenou oblast specializace úkolu.

- Po poskytnutí pomoci dostane uživatel žádající o pomoc možnost ohodnotit interakci s uživatelem, který mu poskytoval pomoc, a tím poskytnou zpětnou vazbu.

6.3.3 Požadavky na výkonnost

- Počet podporovaných uživatelů je větší než maximální počet studentů účastnících se kurzu *Etického hackování*. Z toho vyplývá nutnost podpory více než 150 uživatelů.

6.3.4 Požadavky na vlastnosti

- Dostupnost systému v průběhu semestru nesmí dosáhnout méně než 90%.
- Systém odevzdávání řešení bude chráněn proti útoky hrubou silou.

Kapitola 7

Analýza

V předchozí kapitole byl představen soubor požadavků kladených na navrhovaný systém. Další součástí životního cyklu software vývoje je analýza, které je věnována tato kapitola.

Nejprve bude provedeno modelování případů užití a obchodních procesů které se v požadavcích nacházejí, načež bude navazovat analýza existujících technologií, které mohou být při implementaci použity.

7.1 Modelování obchodních procesů

Hlavní obchodní proces na který je tato práce zaměřena je proces zadání, kontroly a vyhodnocení úloh pro studenty v kurzu výuky etického hackování. Dalším důležitým procesem je způsob, kterým studenti získají přístup k pomoci v případě, že si s úlohou neví rady. V následující části budou tyto procesy analyzovány, a porovnán současný stav se stavem po realizaci systému *BI-EHA Task Force*.

7.1.1 Zadání a kontrola úkolů

7.1.1.1 Současný stav

Při výuce programu *BI-EHA* již probíhá v omezené míře praktická výuka ve formě dobrovolných domácích úkolů zadávaných vyučujícím během laboratorních cvičení. Aby student, jehož cílem je zlepšení vlastních znalostí v oboru, získal zpětnou vazbu za vypracovaný domácí úkol, musí následovat následující proces:

Student musí nejprve být přítomen na laboratorním cvičení, na kterém je vyučujícím představeno zadání domácí úlohy. Pokud na cvičení přítomen není, musí si obstarat zadání jinou cestou. Poté následuje omezená doba, během které má možnost úlohu vypracovat, a odeslat své řešení a postup vyučujícímu, za použití emailových služeb. Vyučující musí řešení od každého

studenta zkontrolovat, postup okomentovat, a odpovědět studentovi s hodnocením a limitovanou zpětnou vazbou. Pokud termín vypracování student nestihne, přístup ke zpětné vazbě se stává z důvodu vytíženosti časových možností vyučujícího výrazně složitějším. Po přečtení odpovědi od vyučujícího je student seznámen se zpětnou vazbou, a jeho znalosti jsou na jejím základě zlepšeny. Celý proces je modelován na obrázku 7.1.

7.1.1.2 Stav po realizaci

Po spuštění systému *BI-EHA Task Force* se proces získání zpětné vazby a zadání stane jednodušším, neboť studentům vznikají další možnosti jakým způsobem tuto zpětnou vazbu získat. Proces se změní v následující:

Student musí být zaregistrován v systému *BI-EHA Task Froce*. Po registraci mu je umožněn přístup k veškerým úlohám, které byly v daném semestru zadány a zveřejněny. Student může úlohu vypracovat, a ihned si ověřit zda je jeho řešení správné. Po dokončení úlohy má možnost v systému odevzdat postup řešení, které je ohodnoceno vyučujícím. Další možností je podívat se na již ohodnocené postupy řešení ostatních studentů, jež mohou být také považovány za zpětnou vazbu. Diagram na obrázku 7.2 tento proces modeluje.

7.1.2 Žádost o pomoc

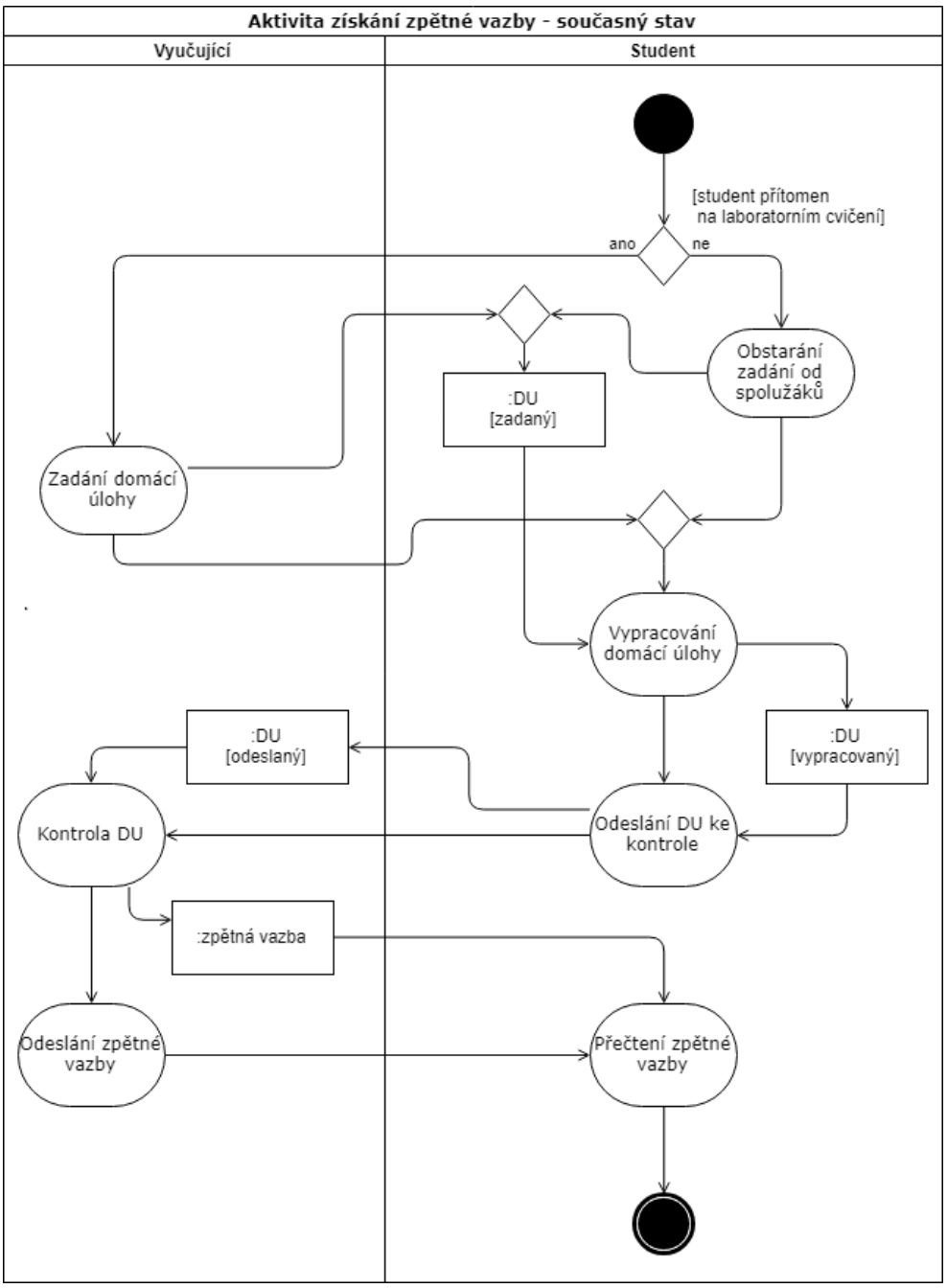
V případě že si student s domácím úkolem neví rady, má v současnosti dvě možnosti jak získat pomoc. Může kontaktovat své spolužáky, nebo vyučujícího. Proces kontaktu s vyučujícím je přímočarý, a obsahuje pouze odeslání emailové zprávy s dotazem, a následné čekání na odpověď.

Proces kontaktu se spolužáky je o něco komplexnější, neboť do něj vstupuje velké množství vnějších faktorů, od sociálního kapitálu tazatele, až po různé komunikační kanály, na kterých účastníci kurzu komunikují, z nichž z velké pravděpodobnosti žádný není dostupný všem. V současné době proces kontaktování spoluúčastníků kurzu probíhá následovně:

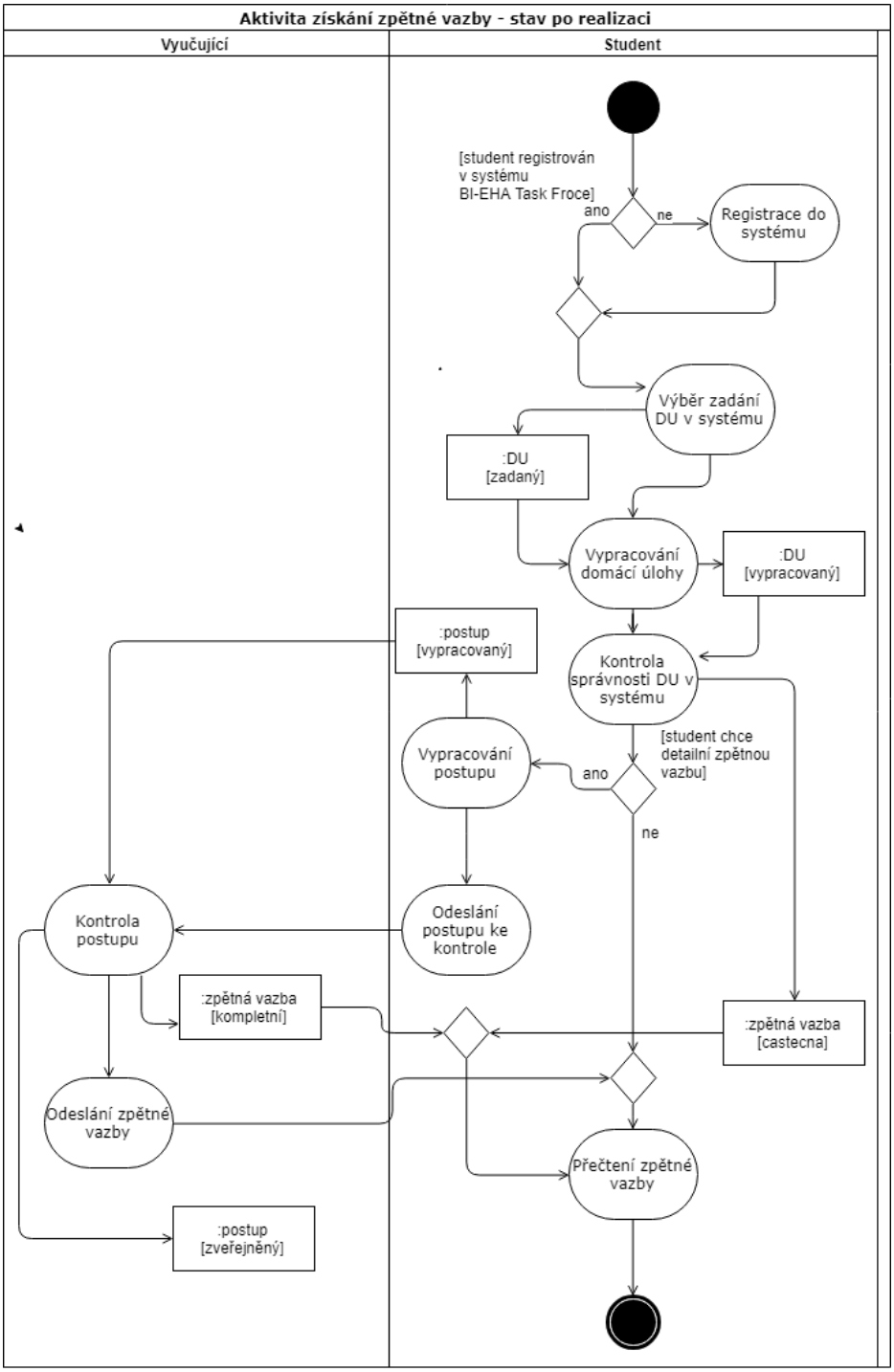
Student, jenž si neví rady s částí zadané domácí úlohy, nejprve zvolí komunikační kanál, skrze který bude komunikovat. Zda otázku položí veřejně, jednotlivci či zvolené skupině známých záleží čistě na zvoleném kanálu a sociálním kapitálu tazatele. Na zvolený komunikační kanál položí svou otázku, a počká na odpověď. Zda odpověď dostane či ne záleží pouze na dobré vůli kontaktovaných studentů, a složitosti otázky.

7.1.2.1 Stav po realizaci

V případě že student má k dispozici systém *BI-EHA Task Force*, proces komunikace je do jisté míry zjednodušen. Součástí funkcí vyvíjeného systému je i komunikační platforma, jež poskytuje studentům způsob jakým ostatní kontaktovat v případě, že potřebují radu. Proces dotazování bude vypadat následovně:



Obrázek 7.1: Diagram aktivity zpětné vazby domácích úkolů



Obrázek 7.2: Diagram aktivity zpětné vazby domácích úkolů se systémem BI-EHA Task Froce

Student registrovaný do systému *BI-Eha Task Force* se přihlásí, zvolí úlohu, se kterou si neví rady, a je mu systémem doporučen seznam studentů, jež se na problematiku úlohy specializují. Student si vybere na základě hodnocení koho kontaktovat, a svůj dotaz pošle za použití uživatelského rozhraní systému. Příjemce dotazu je na zprávu upozorněn, a je motivován bodovým ziskem v případě, že se rozhodne odpovědět. Po obdržení odpovědi má tazatel možnost ohodnotit kvalitu konverzace, a tím se odměnit studentovi, který jeho dotaz zodpověděl.

7.2 Případy užití

Hlavní případy užití se týkají zadávání, čtení, a plnění úloh. V této části bude pro každou skupinu funkcí z funkčních požadavků rozepsán hlavní případ užití. Případy užití, které se jeví jako dostatečně přímočaré a intuitivní, zde rozepisovány nejsou, prostor je věnován pouze případům užití které jsou primární interakcí se systémem, nebo se svým průběhem odlišují od běžných případů užití standardních webových aplikací.

7.2.1 Úlohy

7.2.1.1 Zadání nové úlohy

1. Případ užití začíná, jestliže se administrátor rozhodne vložit do systému novou úlohu.
2. Administrátor se přihlásí do administračního rozhraní, a zobrazí si formulář na přidání úlohy, jenž obsahuje název úlohy, specializaci úlohy, název celku úloh, ke kterému úloha patří, pořadí v celku, cíl úlohy, příběh úlohy, správnou odpověď a bodovou hodnotu. Také umožňuje připojit soubory potřebné k řešení.
3. Administrátor vyplní všechny údaje, z nichž jediný nepovinný je přiložení souboru. Systém zkontroluje, zda jsou zadané údaje v pořádku, a úlohu uloží do systému.
4. Po uložení úlohy má administrátor dále možnost připojit k úloze nápovědu, další soubory, nebo více správných odpovědí.
5. Úloha je poté zveřejněna, a přístupna ostatním uživatelům.

7.2.1.2 Přístup k zadání

1. Pro přístup k zadání se nejprve musí uživatel přihlásit do svého uživatelského účtu.
2. Poté je mu zobrazen seznam úloh, které jsou rozděleny do navazujících případů. Úlohy jsou barevně odlišeny. Zeleně jsou již splněné úlohy, šedivé jsou přístupné úlohy, a černě úlohy, pro které uživatel nemá splněné předpoklady k zpřístupnění.

3. Uživatel vybere úlohu, kterou chce řešit, a systém mu zobrazí zadání úlohy, spolu s příběhem, jenž jej doprovází, a nabídne mu možnost stažení přiložených souborů, nebo odevzdání odpovědi.

7.2.1.3 Odevzdání řešení

1. Pro odevzdání řešení se uživatel musí nejprve přihlásit do svého uživatelského účtu.
2. Poté si zobrazí zadání, jehož součástí je formulář na odevzdání odpovědi na úkol.
3. Po vyplnění formuláře a odeslání odpovědi je uživatel informován systémem, zda jeho řešení je správné.
4. V případě správné odpovědi je uživateli přičtena bodová hodnota úlohy k celkovému skóre.
5. Systém označí úlohu pro uživatele jako vyřešenou, a tím aktualizuje seznam dostupných úloh.

7.2.1.4 Nápověda k řešení

Pokud se přihlášený uživatel rozhodne zpřístupnit si uzamčenou nápovědu u daného úkolu, postupuje následovně:

1. Zobrazí si zadání úlohy, u které chce nápovědu zobrazit.
2. Vybere nápovědu, kterou chce zpřístupnit.
3. Systém zobrazí varování, zda si je uživatel jistý, a upozorní uživatele na fakt, že zpřístupnění nápovědy snižuje skóre.
4. V případě že se uživatel rozhodně pokračovat, systém sníží uživateli hodnotu skóre o cenu nápovědy, a zpřístupní mu nápovědu.

V případě, že je nápověda již uživatelem zaplacena a zpřístupněna, postup užití je následující:

1. Uživatel si zobrazí zadání úlohy, u které se chce znovu podívat na nápovědu.
2. V zadání vybere nápovědu, kterou chce zobrazit. Zpřístupněné nápovědy jsou odlišeny od uzamčených rozdílným textem.
3. Po zvolení nápovědy systém uživateli nápovědu zobrazí.

7.2.2 Bodování a uživatelské účty

7.2.2.1 Registrace nového uživatele

1. Návštěvník systému má možnost projevit zájem o registraci otevřením registračního formuláře, do kterého vyplní své uživatelské jméno, emailovou adresu a heslo.

2. Systém provede kontrolu, zda emailová adresa pochází z domény *čvut.cz*. Pokud ano, uživatel je zaregistrován do systému.

7.2.3 Zpětná vazba

7.2.3.1 Zobrazení seznamu zveřejněných postupů řešení skupiny úloh

1. Uživatel si zobrazí seznam úloh.
2. U každé skupiny úloh je zobrazen odkaz na seznam postupů řešení dané skupiny úloh od ostatních uživatelů.
3. Po kliknutí na odkaz zobrazí systém uživateli seznam zveřejněných postupů řešení dané skupiny úloh. U každého postupu řešení je zobrazena cena pro zpřístupnění postupu, uživatelské jméno autora a hodnocení, jež postup řešení získal od administrátora.

7.2.3.2 Tvorba postupu řešení

V případě že se uživatel rozhodne odeslat zpětnou vazbu ke skupině úloh, postupuje následujícím způsobem:

1. Uživatel si zobrazí seznam zveřejněných postupů řešení skupiny úloh.
2. V seznamu postupů řešení ostatních uživatelů vybere možnost umožňující začít psát vlastní postup.
3. Systém ho odkáže na formulář, který zobrazí název skupiny úloh a seznam úloh v dané skupině, a u každé úlohy zobrazí textové pole, do kterého uživatel zapíše svůj postup řešení dané úlohy. Pod formulářem se nachází tlačítka na odeslání postupu k hodnocení, nebo uložení rozepsaného postupu.
4. Jakmile je uživatel hotov s tvorbou postupu, zvolením tlačítka na odeslání potupu k hodnocení je formulář odeslán k hodnocení.
5. Jakmile dojde k ohodnocení postupu řešení administrátorem, uživatel je notifikován zobrazením krátké zprávy v panelu hlavního menu systému.

7.2.3.3 Přístup k postupům řešení ostatních uživatelů

Postup zobrazení ohodnocených a zveřejněných postupů řešení skupin úloh psaných ostatními uživateli zachycuje následující případ užití:

1. Uživatel si zobrazí seznam zveřejněných postupů řešení skupiny úloh.
2. Vybere postup řešení, který chce zpřístupnit.
3. Systém zobrazí varování, zda si je uživatel jistý, a upozorní uživatele na fakt, že zpřístupnění postupu mu snižuje skóre o cenu, jež byla postupu přiřazena administrátorem.
4. V případě že se uživatel rozhodně pokračovat, systém sníží uživateli hodnotu skóre o cenu postupu, a umožní mu přístup zobrazit a přečíst.

7.2.3.4 Hodnocení postupů řešení

Administrátor, který se rozhodne hodnotit odevzdané postupy řešení uživatelů, postupuje tímto způsobem:

1. Administrátor zvolí v hlavním panelu možnost hodnocení odevzdaných postupů řešení.
2. Systém zobrazí seznam postupů řešení, které jsou odeslány k hodnocení, a nebyly nikým ohodnoceny.
3. Administrátor vybere postup řešení, který chce hodnotit. Systém mu zobrazí text postupu řešení, a administrátor se na jeho základě rozhodne, jaké hodnocení udělí.
4. V seznamu postupů řešení administrátor použije možnost hodnocení, jež zobrazí formulář, do kterého vyplní hodnocení na stupnici od 0 do 100, komentář k hodnocení, a cenu za jakou bude postup řešení přístupný ostatním uživatelům.
5. Po odeslání formuláře je postup řešení považován za veřejný a ohodnocený, a uživateli, jež je autorem postupu, je poslána notifikace.
6. Autorovi je také zvýšeno skóre v závislosti na hodnocení, které administrátor udělil.

7.2.4 Sociální interakce uživatelů

Hlavním případem užití z této kategorie funkcí je možnost kontaktovat ostatní uživatele s žádostí o pomoc nebo radu v řešení úlohy. Tento kontakt probíhá následujícím způsobem:

1. Uživatel, jenž se rozhodne kontaktovat ostatní uživatele, si zobrazí zadání úlohy, které se žádost týká.
2. Součástí obrazovky se zadáním úlohy je odkaz na obrazovku se seznamem uživatelů, kteří se specializují na okruh zobrazené úlohy. U každého uživatele je zobrazeno jejich skóre, průměr hodnocení konverzací s ostatními uživateli, a tlačítko umožňující uživatele kontaktovat.
3. Po zvolení uživatele, kterého kontaktovat, kliknutím na tlačítko u jeho jména je zobrazen formulář, do kterého má uživatel možnost zapsat svoji zprávu spolu s dotazem.
4. Po odeslání formuláře je zahájena konverzace, a zpráva doručena adresátovi, kterému je zobrazena notifikace. V případě, že není v daný moment v systému aktivní, je adresátovi poslána emailová zpráva, upozorňující ho na novou konverzaci.

7.2.4.1 Hodnocení konverzace

Uživatel, jenž zahájil konverzaci, má možnost tuto interakci s jiným uživatelem ohodnotit udělením hodnocení od 1 do 5. Za hodnocení dostane hodnocený

uživatel odměnu ve formě skóre, a průměr hodnocení uživatele je veřejně zobrazen v tabulkách uživatelů.

Hodnocení probíhá následujícím případem užití:

1. Uživatel, který obdržel alespoň jednu odpověď v konverzaci, jež inicioval, má možnost tuto konverzaci ohodnotit.
2. Pro ohodnocení konverzace nejprve otevře formulář s konverzací skrze panel hlavního menu.
3. Na obrazovce konverzace použije tlačítko hodnocení, které zobrazí formulář, do kterého vyplní hodnocení na stupnici od jedné do pěti, a krátký komentář.
4. Systém provede kontrolu zadaných údajů, v případě že hodnocení není v rozmezí 1 až 5, konverzace již byla ohodnocena, nebo neobsahuje žádnou odpověď, hodnocení není uloženo. V opačném případě je formulář odeslán.
5. Po odeslání formuláře je uživateli oznámeno úspěšné ohodnocení, a hodnocený uživatel obdrží notifikaci, a je mu přičteno skóre v závislosti na výši hodnocení.

7.3 Analýza existujících CTF platforem

Součástí specifikace požadavků je i požadavek na použití existujícího CTF frameworku/platformy. V této části budou vybrána kritéria které u frameworků budou pozorována, a existující řešení budou porovnány, aby mohl být zvolen framework který bude pro potřeby této práce nejvhodnější.

7.3.1 Srovnávací kritéria

U každé z nalezených platforem sledujeme přítomnost funkcí, jež jsou vyžadovány funkčními požadavky vyvíjeného systému. V nejlepším případě bude nalezena platforma, která splňuje co nejvíce požadavků, a nebude nutné vyvíjet doplňkové funkce.

Kromě kritérií přímo plynoucích ze specifikace požadavků jsou důležité také následující vlastnosti:

- Licence, jež umožní použití platformy v této práci a následně ve výuce.
- Podpora zásuvných modulů, jež zjednoduší implementaci chybějících funkcí.
- Technologie na kterých je platforma postavena.
- Osobní preference, jenž je kombinací autorova dojmu z vizuální stránky frameworku, použitých technologií a osobních zkušeností ze soutěží které absolvoval.

Vzhledem k faktu, že některá z kritérií jsou pro potřeby této práce nezbytně nutné (jako například licence), platformy které požadavky na tuto vlastnost nesplňují nejsou zmiňovány, a jsou rovnou vyřazeny z analýzy.

7.3.2 Výsledky analýzy

Porovnáno bylo celkem 7 nalezených CTF frameworků, které splňovali minimální funkční specifikace potřebné pro tento projekt. Výsledky analýzy jsou shrnuty v tabulce 7.1. Sloupec technologií je obarven dle množství zkušeností autora práce s danou technologií.

Tabulka 7.1: Porovnání funkcí CTF Frameworků

Name	Plugins	Technologie	Napověda	Zprávy	Zpětná vazba	Osobní preference
CTFd	A	Flask	A	X	X	A
fbctf	X	PHP	X	X	X	X
HackTheArch	X	Ruby on Rails	A	A	X	X
Mellivora	X	PHP	A	X	X	A
NightShade	X	Python	X	X	X	X
OpenCTF	X	Go	X	X	X	X
picoCTF	X	Python	X	X	X	A

Existující řešení podporující odevzdávání postupů řešení, a následné zpětné vazby nebylo ani ve sféře otevřeného, ani proprietárního software nalezeno. Z toho důvodu se podpora zásuvných modulů a snadné rozšiřitelnosti bez nutnosti zásahu do zdrojového kódu samotné platformy jeví jako nejdůležitější požadavek na funkce potencionální platformy.

Jediná platforma *CTFd* [22] nativně podporuje zásuvné moduly, a tudíž umožňuje tvorbu funkcí zpětné vazby, gamifikace a messagingu , aniž by došlo k potížím s aktualizacemi na novější verze původního frameworku. Tím se jeví jako nejlepší volbou pro potřeby vyvíjeného systému.

Kapitola 8

Návrh

V této části bude proveden návrh dodatečných funkcí aplikace a gamifikace, praktická aplikace poznatků o výukových hrách a gamifikaci z literární rešerše, a návrh architektury a komponent ze kterých se bude vyvíjený systém skládat.

8.1 Gamifikace

Z rešeršní části o gamifikaci vzešlo několik poznatků o správných postupech při implementaci gamifikace. Do návrhu tohoto systému se tyto poznatky promítly následujícím způsobem:

8.1.1 Octalysis Framework

Při návrhu funkcí vyvíjeného systému byl použit gamifikační framework *Octalysis*, jemuž je věnována podkapitola 5.5.1. Každá z funkcí zamýšlených pro vyvíjený systém byla navrhována v souladu s tímto frameworkem, nebo upravena aby do frameworku zapadala, a využívala jeho přednosti.

Navrhované funkce zapadají do osmi klíčových oblastí motivace následujícím způsobem:

- Téma příběhu a vzhledu webové platformy je zasazené do prostředí speciálních policejních jednotek, jež verbují ty nejlepší studenty kurzu *BI-EHA* k tomu, aby jim pomáhali s bojem proti zločinu za pomoci hackingu. Studenti řeší úlohy ve formě případů inspirovaných reálnými žalobami v Českém právním systému, což dodává úlohám atraktivitu a je v souladu s motivací *grandiózního smyslu a poslání*, popsané v podkapitole 5.5.1.1.
- Rozdělení jednotlivých případů na více jednodušších úloh, jež na sebe navazují, ale dají se řešit jednotlivě, využívá klíčové motivace *vývoje a úspěchu* (Podkapitola 5.5.1.2). Nemožnost přístupu k zadání a příběhu

úloh jenž v případu následují dříve, než jsou dokončeny všechny předchozí úlohy pracuje s motivací *nepředvídatelnosti a zvědavosti*, popsané v podkapitole 5.5.1.7.

- Přidání možnosti odevzdávat a zveřejňovat své vlastní postupy řešení případů, jež si mohou ostatní uživatelé zpřístupňovat, je zaměřeno na posílení klíčové motivace *posílení kreativity a zpětné vazby*, které je věnována podkapitola 5.5.1.3.
- Možnost pomáhat ostatním, a veřejný žebříček účastníků jsou cíleny na soubor motivací jež nese název *sociální vliv a sounáležitost*. Více o této klíčové motivaci je popsáno v podkapitole 5.5.1.5.
- Nutnost platit za zpřístupnění nápověd a postupů řešení ostatních uživatelů virtuální měnou která je přímo svázaná s hodnotou skóre uživatele využívá motivace *nedostatku a netrpělivosti* a *ztráty a předcházení* k tomu, aby motivovala uživatele řešit úlohy bez jejich použití. Tím je posílen výukový přínos platformy. Motivace je popsána v podkapitolách 5.5.1.8 a 5.5.1.6.

8.1.2 Gameful Design

Vzhledem k podobnosti frameworku *Octalysis* a *gameful designu* nebude v této části do podrobnosti rozepisováno kterému z aspektů gameful designu přísluší která funkce. Bude zde pouze stručně shrnuto, jakým způsobem byla myšlenka *gameful designu*, jež je podrobně popsána v kapitole 5.5.2, použita při návrhu funkcí implementovaného systému.

Hlavní myšlenka *gameful designu* je nezaměřit se pouze na herní mechaniky a vnější odměny, ale na vnitřní hodnoty hráčů které za nimi stojí. Z toho důvodu bylo při návrhu funkcí implementovaného systému rozhodnuto zaměřit gamifikační část a nemalou část implementačního času na vybudování systému podpory komunikace mezi uživateli, jenž motivuje studenty navzájem sdílet znalosti. Z praktického zapojení gamifikace *Dr. Christopherem Seem*, popsaného v kapitole 5.4.1, se komunikace mezi studenty řešícími tematické hádanky v únikové místnosti ukázala být jednou z důležitějších součástí experimentu, a měla pro studenty velký přínos.

Zamýšleným výsledkem návrhu implementovaných funkcí není tedy pouhé předání a ohodnocení úloh studentů, ale snaha motivovat k větším sociálním interakcím, a tvůrčí aktivitě při psaní a sdílení postupů. Tyto myšlenky jsou v souladu s *gameful designem*, a vychází z rešerše na téma gamifikace.

8.1.3 Existující CTF soutěže

V analýze provedené v kapitole číslo 3.2.2 byl jako největší slabá stránka existujících CTF soutěží identifikován nedostatek zpětné vazby, a možnosti účastníků získat přístup k pomoci, či radě v případě, že nejsou schopni úlohu vyřešit. Navrhované funkce, jejichž implementací se tato práce zabývá, jsou

zamýšleny jako potencionální řešení těchto nedostatků, a jsou navrhnuty s cílem nedostatky existujících soutěží vyřešit. Z tohoto důvodu, spolu s ideou *gameful designu*, je návrh funkcí zaměřen převážně na sociální a komunikační aspekty stavěného systému.

8.2 Návrhová rozhodnutí

Nejdůležitějším návrhovým rozhodnutím, které bylo přímo požadováno specifikací požadavků, byla volba vhodného CTF Frameworku na kterém bude systém vystaven. Vzhledem k nedostatku vhodných alternativ nebylo možné příliš dbát na preference a zkušenosti autora práce v rozhodnutích ohledně použitých technologií, a bylo nutné přizpůsobit se technologiím, jež jsou používány zvoleným frameworkem.

Z analýzy vzešel jako nejvhodnější volba *CTFd Framework* [22], z důvodu jednoduchosti nasazení, škálovatelnosti, a hlavně podpory zásuvných modulů.

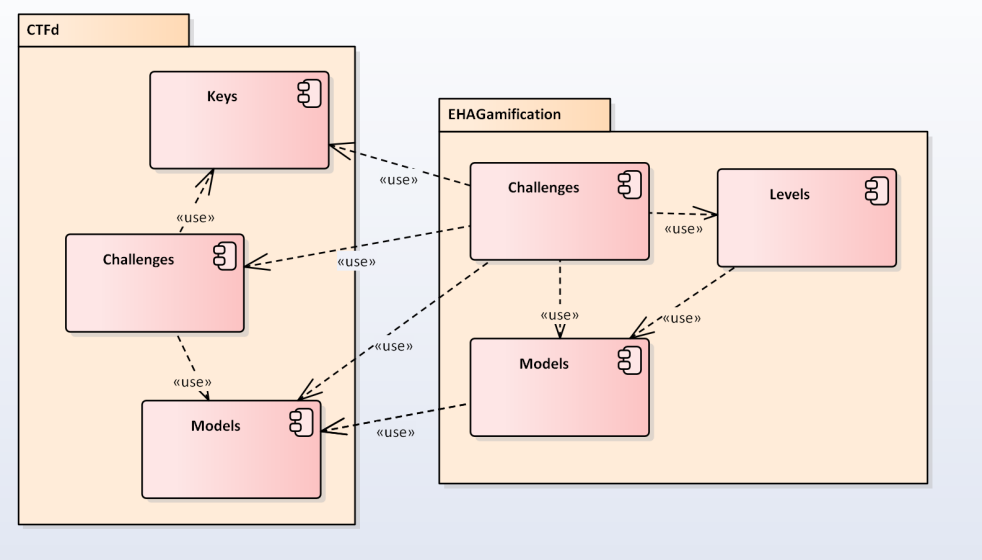
Důsledkem volby frameworku byla také nutnost použití následujících technologií, neboť je na jejich základě *CTFd Framework* vystaven:

- Implementační jazyk: Python3, HTML a jQuery
- Webový framework: Flask [91]
- Databázový systém: SQLite [50]
- ORM: SQLAlchemy [12]

8.3 Architektura

Nejdůležitějším architektonickým rozhodnutím bylo implementovat chybějící funkce jako jeden zásuvný modul do frameworku *CTFd*. Způsob, kterým *CTFd Framework* pracuje s moduly, neumožňuje implementaci modulu, který nezasahuje přímo do komponent frameworku, neboť nevystavuje žádné rozhraní kromě inicializačního a konfiguračního. Místo toho umožňuje modulům přístup ke všem vrstvám své architektury, a přímo k rozhraním frameworků, které používá. Implementovaný zásuvný modul je tedy v některých místech závislý na konkrétní implementaci *CTFd*, a v případě že dojde k nějaké větší změně ve frameworku bude nutné modul aktualizovat. Příklad takovéto závislosti je ilustrován na diagramu komponenty na obrázku číslo 8.1. V celém modulu se ale jedná pouze o závislosti do stejné nebo nižší vrstvy, tudíž není porušena idea třívrstvé architektury.

Pro zásuvný modul byla zvolena třívrstvá architektura, neboť se jedná o stejnou architekturu, jež používá framework *CTFd*. Architektura je znázorněna na modelu komponent, který je na obrázku číslo 8.2. Nutno dodat, že na obrázku není zobrazena většina komponentů frameworku *CTFd*, neboť jejich návrh a zobrazení není pro dostatečnou ilustraci zvolené architektury nezbytné.



Obrázek 8.1: Ilustrace závislosti komponent mezi CTFd a vyvíjeným modulem

8.3.1 Theme

Tato komponenta uchovává HTML šablony, které *CTFd Framework* zobrazuje za použití frameworku *Jinja2* [92]. Poskytuje *themes* rozhraní, se kterým *CTFd Framework* pracuje a na jeho základě upravuje vzhled základních obrazovek, které jsou uživatelům prezentovány.

8.3.2 Writeups

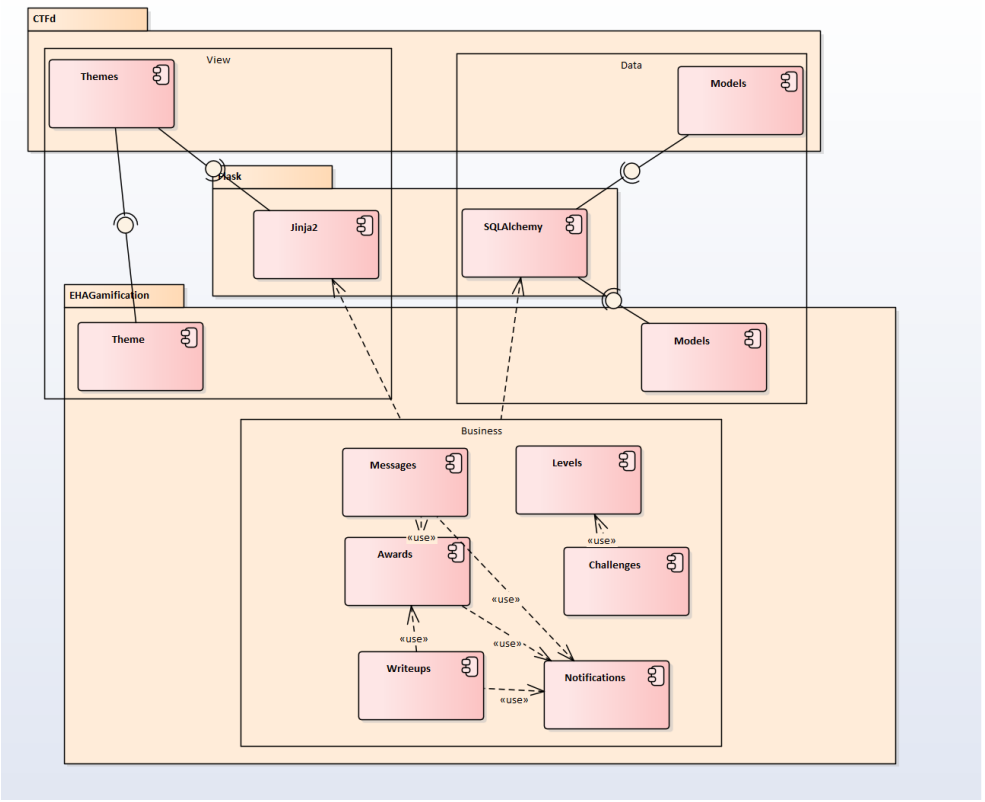
Writeups komponenta obstarává dotazy okolo přidávání, kontroly, hodnocení, zpřístupnění a editaci odevzdaných popisů postupů, které mohou uživatelé odevzdávat na ohodnocení. Jedná se o hlavní modul funkcí zpětné vazby.

8.3.3 Levels

Tato komponenta rozšiřuje *CTFd Framework* o možnost určovat kategorie, na které se uživatelé specializují. Zajišťuje počítání a práci se specializačními body, které uživatelé dostávají za plnění úloh, výběr a administraci specializací, a možnost počítat skóre za úspěchy v každé specializaci zvlášť.

8.3.4 Challenges

V komponentě *Challenges* je implementována logika okolo typu úlohy *gamified challenge*, jež využívá funkce rozhraní pro vlastní typy úloh vystavené *CTFd Frameworkem* v rámci rozhraní *CTFdPlugin*. Jedná se o typ úloh, který na



Obrázek 8.2: Diagram komponent zásuvného modulu. Komponenty CTFd jsou z naprosté většiny vynechány.

rozdíl od základního typu *CTFd* úlohy využívá funkce přidávané modulem který je v této práci vyvíjen, jako je například specializace, či možnost požádat o pomoc ostatní uživatele při řešení.

8.3.5 Messages

Komponenta zajišťuje veškerou logiku okolo posílání zpráv mezi uživateli, žádosti o pomoc, hodnocení konverzací, a většinu funkcí sociální interakce.

8.3.6 Awards a Notifications

Tato dvojice komponent umožňuje posílání upozornění uživatelům, že došlo k nějaké významné akci. *Awards* obstarává logiku předávání ocenění za významné úspěchy, nebo utracení skóre za nápovědy, a *Notifications* oznamuje uživateli důležité akce, jako například příchod zprávy či ohodnocení jim odevzdaného postupu řešení.

8.3.7 Models

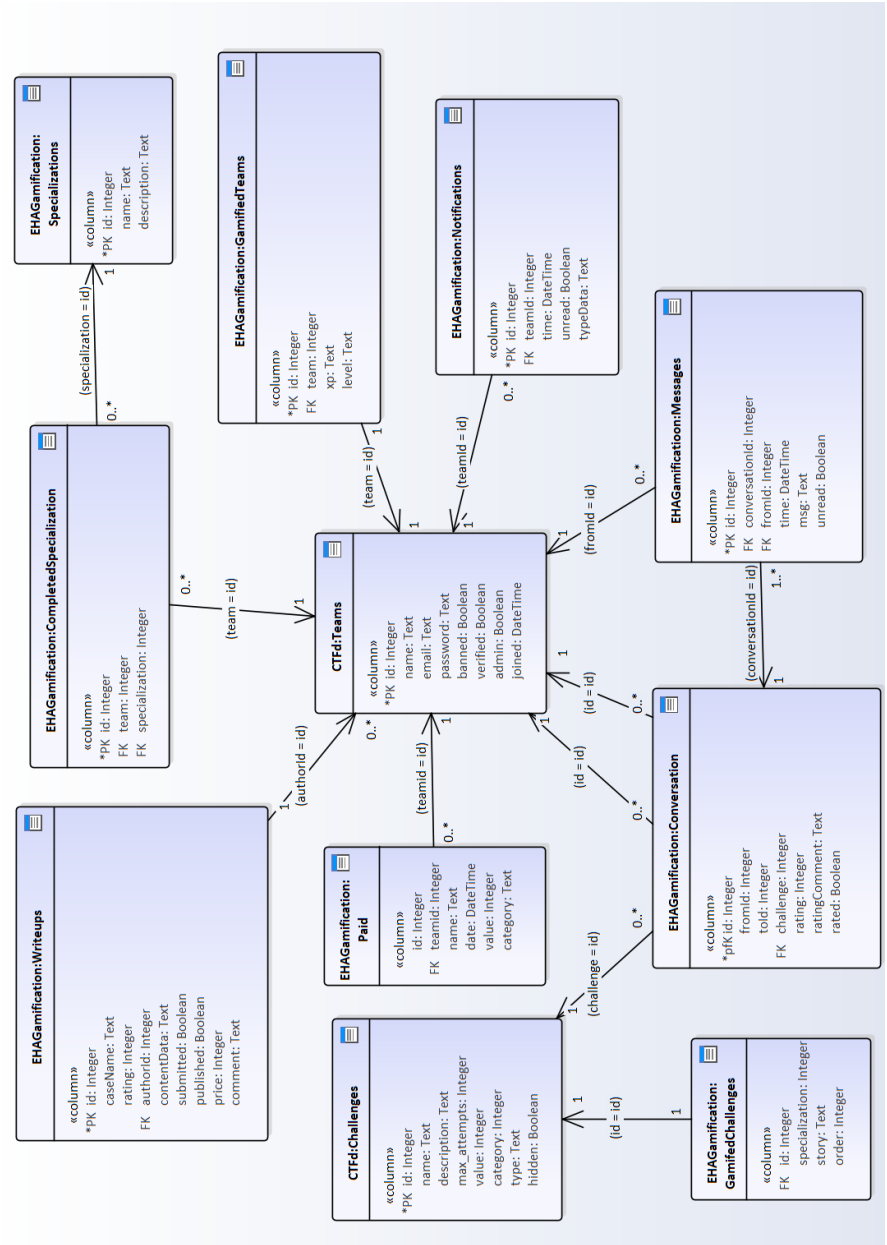
Komponenta ORM, jež je napojena přímo na *SQLAlchemy* rozhraní poskytované *CTFd Frameworkem.* Zajišťuje definice ORM v datové vrstvě.

8.4 Databázový model

Další důležitou součástí návrhu je návrh databáze. Vzhledem k použití frameworku, který s databází pracuje, není potřeba navrhovat databázovou strukturu celou. Tabulky pro uživatelské účty, úkoly, nápovědu, správná a špatná odevzdaná řešení apod. jsou již součástí *CTFd Frameworku*, a není nutné je navrhovat. Je ale nutné navrhnout část databáze pro vyvíjený zásuvný modul, a napojit tyto tabulky na již existující model.

Vzhledem k faktu, že dokumentace frameworku *CTFd* neobsahuje databázový model, je nutné tento model pro potřeby diagramu vytvořit. Protože framework obsahuje velké množství funkcí, které nejsou pro implementaci vytvářeného zásuvného modulu relevantní, jsou z přiloženého databázového modelu z důvodu přehlednosti vynechány. Jakékoliv tabulky, na které je z tabulek modulu odkazováno, jsou ale do modelu zahrnuty.

Názvy tabulek jsou dostatečně intuitivní, tudíž není nutné dodávat podrobnější popis. Model je zobrazen na obrázku 8.3.



Obrázek 8.3: Databázový model. Nerelevantní tabulky CTFd jsou z modelu vynechány.

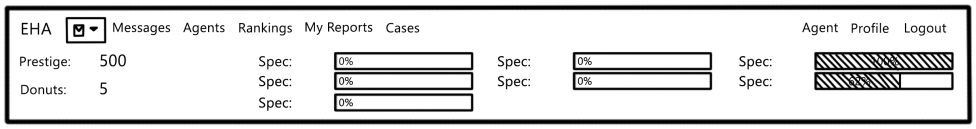
8.5 Uživatelské rozhraní

Velká část uživatelského rozhraní je již součástí *Frameworku CTFd*. Od registrace, přes administrátorské rozhraní až po zobrazení žebříčků uživatelů. Žádnou z těchto obrazovek není potřeba navrhovat. V některých případech dochází k menším úpravám pro potřeby modulu, nejedná se ale o dostatečně velké změny na to, aby bylo nutné se jim zde věnovat.

Součástí implementovaného zásuvného modulu je několik nových obrazovek, pro které je nutné navrhnout vzhled. V této části budou představeny návrhy těch nejdůležitějších nových obrazovek.

8.5.1 Hlavní menu

Na každé obrazovce zobrazuje *CTFd Framework* hlavní navigační menu. Pro potřeby implementovaného modulu je nutné toto menu pozměnit, např. přidáním ikony pro notifikace. Z důvodů větší viditelnosti prvků gamifikace, a lepšímu přístupu k rychlé zpětné vazbě, bylo rozhodnuto do tohoto menu přidat informace o současném postupu uživatele, a jeho skóre. Návrh nového menu je zobrazen na obrázku 8.4



Obrázek 8.4: Návrh základního navigačního menu

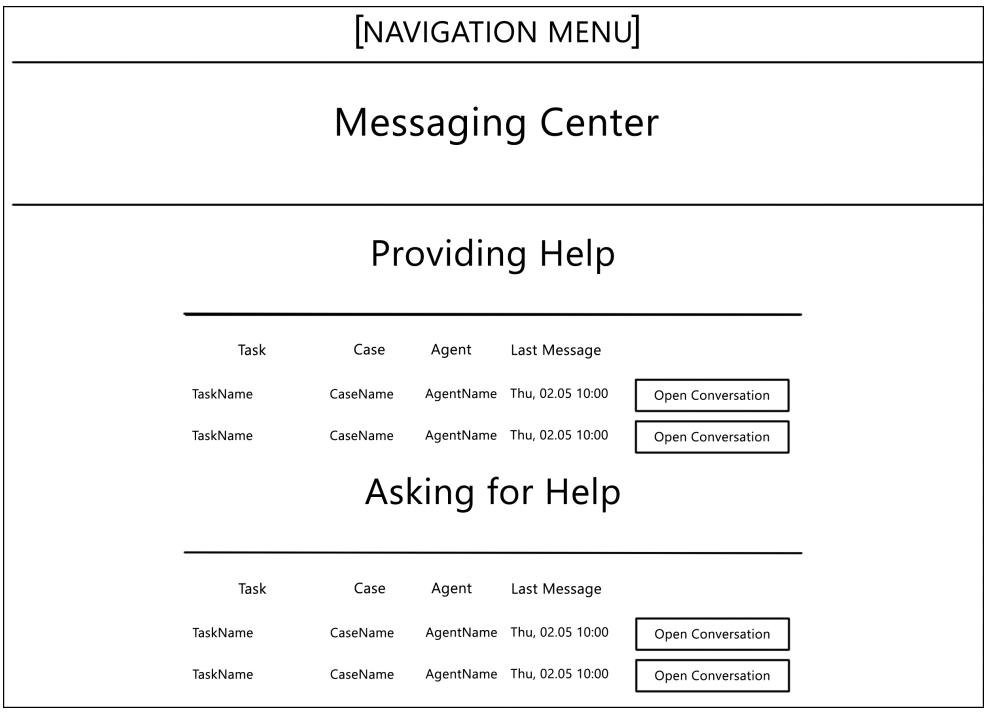
8.5.2 Zprávy

Jednou z hlavních funkcí je možnost požádat ostatní o pomoc. Obrazovka jež tuto funkci zpřístupňuje je navrhnuta na obrázku číslo 8.5.

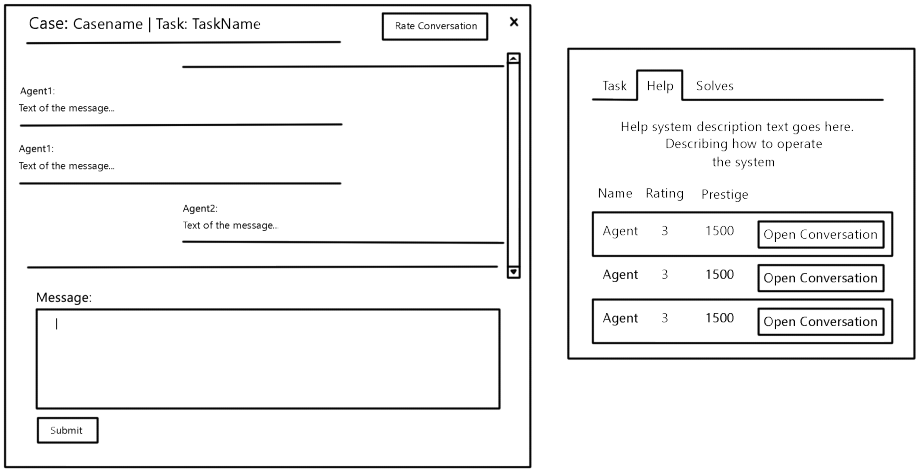
Samotné posílání zpráv a konverzací probíhá ve vyskakovacích oknech, jejichž návrh je načrtnut na obrázku číslo 8.6.

8.5.3 Editor postupu řešení

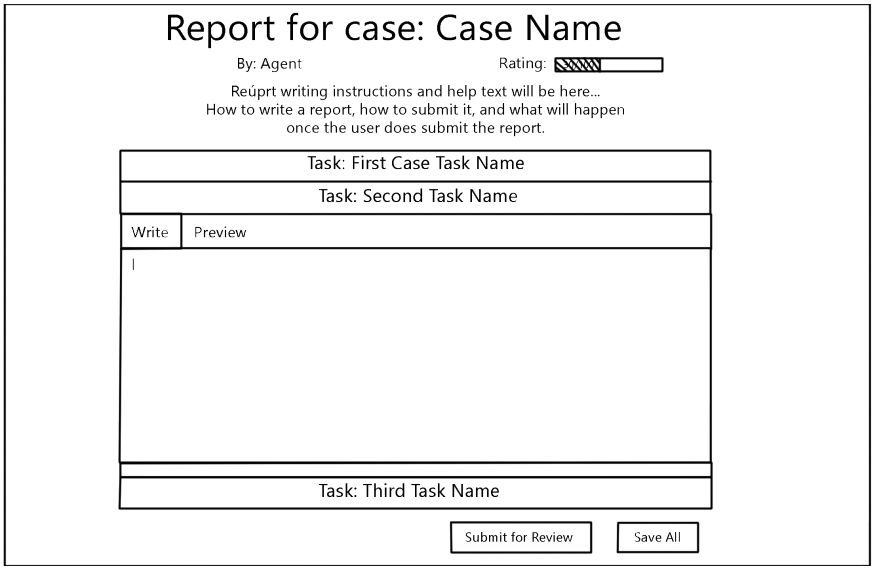
Možnost psát a odevzdávat postupy řešení jednotlivých skupin úloh je další obrazovkou, jež byla navržena od základu. Na obrázku číslo 8.7 je tato obrazovka navržena. Obrazovka obsahuje seznam úloh v dané skupině, a po kliknutí na název úlohy zobrazí editor, do kterého je možné psát postup za použití markdown syntaxe. Na obrázku je tímto způsobem zobrazený editor pro druhou úlohu.



Obrázek 8.5: Návrh obrazovky seznamu zpráv



Obrázek 8.6: Návrh posílání zpráv a žádosti o pomoc. Vlevo je zobrazena konverzace, vpravo obrazovka žádosti o pomoc.



Obrázek 8.7: Návrh obrazovky tvorby postupů řešení

8.5.4 Úlohy

Obrazovka výběru a zobrazení úloh pro řešení byla oproti původnímu frameworku změněna pouze minimálně. Místo seskupování do kategorií jsou úlohy řazeny podle případu, což je na sebe navazujících set úloh týkající se jednoho příběhu. Také již není možné zobrazit jakoukoliv úlohu, a tudíž je nutné od sebe odlišovat, které úlohy jsou a nejsou přístupné. K tomu bylo zvolenou použití jiné barvy, a ikony zámečku.

Vzhledem k faktu že tyto změny jsou z velké většiny pouze funkční, a na výsledném vzhledu obrazovky nic nemění, není přiložen wireframe návrh této obrazovky.

8.6 Návrh úloh

Součástí funkčních požadavků je také tvorba setu úloh, které pokryjí hlavní témata kurzu *BI-EHA*. Jedná se o následující témata:

- Průzkum, mapování cílů, shromažďování informací, síťové skenování
- Návrh vektorů útoku (různých způsobů infiltrace systému)
- Obcházení vybraných bezpečnostních mechanismů (firewall, antivirus, DEP atp.)
- Prolamování hesel
- Vyhledávání, testování a zneužití síťových zranitelností

- Vyhledávání, testování a zneužití zranitelností softwarového balíku, operačního systému, databázového systému, webové aplikace, prostřednictvím fuzz testování, prostřednictvím auditu zdrojového kódu a nebo skrze debuggování a reverzní inženýrství
- Analýza systému „zevnitř“, pillaging (sběr dat z infiltrovaného systému relevantních k cíli útočníka) a eskalace privilegií
- Zajištění persistence útočníka / škodlivého softwaru v systému
- „Zahlazování stop“ po aktivitě útočníka
- Pivoting - přistupování k doposud nedostupným systémům skrze první infiltrovaný systém

8.6.1 Příběh

Celkem bylo navrženo 13 úloh, které jsou rozděleny do 5 tematických případů. Každý případ obsahuje sadu několika navazujících úkolů, které simulují fiktivní situace do kterých se dostává fiktivní policejní složka složena ze studentů předmětu *BI-EHA*, jež nese název *BI-EHA Task Froce*. Každý z případů je volně inspirovaný reálnými případy z trestního práva v oblasti kyberzločinu, a byla provedena snaha zranitelné virtuální stroje sestavovat způsobem, který toto téma co nejvíce podporuje.

Příběh a téma jednotlivých úloh je následující:

- Případ *Basic Training* - V průběhu tří úloh je studentovi představena idea a příběh *BI-EHA Task Force* jednotky a systém *ForensicLink*. Součástí je také návod na instalaci Linux distribuce *Kali Linux* [7], a použití virtuálních appliancí, které jsou součástí většiny ostatních úloh.
- Případ *Commorragh* - Studentova asistence je vyžadována v případu nelegální pirátské obchodní sítě s názvem *Commorragh*. K serveru ale není možné připojit se přímo, a je nutné nejprve získat přístup do zabaveného počítače hacktivistky Lelith, který je do sítě napojen. Cílem případu je nainstalovat persistentní zadní vrátka na server, který umožní pozdější sběr důkazů. Případ je volně inspirován obchodní sítí *Silk Road* a zatčením Rosse Ulbrichta [108].
- Případ *Windmill Co.* - V tomto případu řeší studenti sběr důkazů z nalezeného serveru, který byl údajně použit pří páchání trestného činu, při kterém zaměstnankyně firmy *Windmill Co.* získala za použití hackingu přístupové údaje do sociálních sítí od svých kolegů, a napáchala na nich škodu.
- Případ *Damimier Substances* - Studentův úkol v tomto případě je získat administrátorský účet na webové aplikaci, jež je používána drogovým kartelem pro přijímání objednávek, a sledování svých kurýrů. Tento případ je inspirován nedávnou událostí, ve které policie odhalila drogový kartel využívající velké množství informačních technologií pro nelegální činnost [32].

- Případ *Home Defense* - Tento případ se zabývá úkoly, které jsou inspirované interním chodem běžných oddělení. V první úloze je prováděn audit zdrojového kódu pro potencionální interní webovou aplikaci, a v druhé student dešifruje důležitá data, která byla místnímu sekretáři zašifrována ransomware malwarem.

8.6.1.1 ForensicLink

Hlavním cílem všech úloh je získat přístup k textovému řetězci ve formátu *„FLAG{TEXT}“*, který je poté odevzdán do webového rozhraní systému, čímž student dokáže splnění zadaného úkolu. Výhodou tohoto přístupu je fakt, že student může dojít k řešení vlastním postupem, a za použití vlastních nástrojů, a vždy dojde ke stejnému řetězci, který se nemění.

Protože pouhé hledání textových řetězců není dostatečně tematické, a narušuje možnost dostatečného ponoření se do příběhu a role policejních složek, je uživatelům představen systém *ForensicLink*. *ForensicLink* je fiktivní systém, který je schopný sběru relevantních důkazů v případech, a to za použití *„Forensic Link Access Gateway“* (FLAG) přístupových bodů. Uživatelé tedy zdánlivě hledají místo textových řetězců virtuální přístupové body, což je z pohledu herního designu zajímavější a zábavnější, a podporuje důslednější ponoření do fantasie policejních složek.

8.6.2 Zranitelné virtuální stroje

Součástí většiny případů je virtuální appliance ve formátu *.ova*, na které se nachází zranitelný stroj. Úkolem všech úloh je prolomit bezpečnost sytému zneužitím zranitelností, které jsou na stroji úmyslně zanechány, a získat přístup k souborům obsahujícím *FLAG* řetězec. Všechny virtuální stroje používají jako operační systém minimální instalaci linuxové distribuce *ArchLinux* [105], a neobsahují žádné grafické rozhraní. Jediný možný způsob interakce se zranitelnými stroji je skrze otevřené síťové porty. Přihlašovací hesla na uživatelské účty na strojích nejsou zveřejněna.

8.6.3 Zranitelnosti v případech

Každý případ obsahuje jeden virtuální stroj, na kterém je nutno pro vyřešení případu a přístupu k souboru s *FLAG* řetězcem využít některé ze zranitelností. Každý stroj obsahuje více než jeden *FLAG* řetězec, neboť součástí případů je vždy několik na sebe navazujících úloh.

Zranitelnosti v případech, spolu se zamýšlenou návazností úloh a řešení bude popsán v této podkapitole.

8.6.3.1 Případ Commorragh

Pro úspěšné řešení tohoto případu je nejprve nutné získat přístup na první ze dvou virtuálních strojů. Na prvním stroji je spuštěno několik služeb, a jednou z nich je služba *msfd*. Tato služba zpřístupňuje *Metasploit Framework* skrze TCP socket, její zranitelnost se nalézá ve faktu, že je možné spouštět *Ruby* kód. Tímto kódem je možné otevření reverzní shell konzole, čímž je získán přístup do systému.

Dalším krokem je pivoting na druhý server. Server obsahuje přihlašovací službu, která přijímá připojení pouze od prvního počítače. Pro úspěšné vyřešení je nutné získat heslo, které je obsaženo v jednom z 12 000 archivovaných emailů na již prolomeném počítači. Je tedy nutné nějakým způsobem emailové konverzace profiltrovat, a nalézt heslo.

Po získání hesla je posledním krokem získání persistence na serveru. Na serveru je reboot skript, který stroj restartuje, zakáže přihlašovací službu (tudíž není možné znovu se připojit stejným způsobem), a zapíše *FLAG* řetězec. Pro získání řetězce je tedy nutné zajištění perzistence. Zamýšlený způsob řešení je skrze službu *cron*, a reverzní shell připojení na nyní volném otevřeném portu přihlašovací služby.

8.6.3.2 Případ Windmill Co.

V tomto případu je studentovi předán virtuální stroj serveru, a také *.pcap* soubor na kterém je zachycena část komunikace serveru. Virtuální stroj má nastavený firewall způsobem, že přijímá pouze připojení vycházející z portu 1804, a žádná jiná. Po zjištění tohoto faktu lze nalézt službu, která na náhodném portu přijímá data, a odpovídá *FLAG* řetězcem.

Druhá úloha vyžaduje získání přístupu na server. Služba, která je na serveru spuštěna, restartuje připojení každé dvě vteřiny, tudíž je nutné pracovat rychle. V případě, že je službě poslán řetězec delší než 512 znaků, program, jež tato data ukládá, je ukončen chybovou hláškou *SegFault*, a jakákoliv další poslaná data jsou vyhodnocena programem */bin/bash*. Po dvou vteřinách je ale připojení restartováno, a program ukládání dat znovu spuštěn. Pro vyřešení této úlohy je nutné za použití skriptů nejprve odeslat dlouhý řetězec, a poté příkaz, kterým je spuštěna reverzní shell konzole, která již nebude každé dvě vteřiny restartována. Tím je získán přístup, a vyřešena další úloha.

Finálním úkolem je získat přístup k *.log* souborům do kterých služba ukládá získaná data. Uživatel, který tuto službu spouští, nemá dostatečná oprávnění ke čtení tohoto souboru, a je tedy nutné použít eskalaci privilegií. Toho se dá dosáhnout špatně nakonfigurovanou *$PATH* proměnnou, jež obsahuje „.“ symbol na svém začátku, a *cron* práce spouštěné cíleným uživatelským účtem, která každých pět minut zálohuje *.log* soubory. Zneužitím způsobu jakým systém *Linux* pracuje s *$PATH* hodnotou lze dosáhnout eska-

lace privilegií, a tím získat přístup k *.log* souborům, které obsahují poslední *FLAG* řetězec.

8.6.3.3 Případ Damimier Substances

Přílohou u tohoto případu je virtuální stroj, na němž je spuštěna *Flask* webová aplikace s jednoduchým přihlašováním a registrací uživatelů, jež obsahuje možnost zobrazit a filtrovat recenze fiktivních uživatelů služby. Webová aplikace obsahuje staré verze použitých frameworků *Flask* a *SQLAlchemy*, které trpí SQL-Injection zranitelnosti v některých funkcích [93].

Cílem první úlohy je vytvoření uživatelského účtu. Po registraci je studentovi sděleno, že nové účty musí být potvrzeny administrátorem. Pokud se student pokusí přihlásit bez uživatelského jména, je mu zobrazena chybová hláška, ve které je zobrazen *SELECT* příkaz, čímž je student seznámen s modelem databáze a přítomných tabulek. Této znalosti, spolu s SQL Injection zranitelností, je nutné využít a aktivovat svůj účet v databázi, a tím získat první *FLAG* řetězec.

Dalším úkolem je získat přístup do administrátorského rozhraní. To je možné pouze získáním hesla na jeden z existujících účtů administrátorů. Za použití directory fuzzing techniky je možné nalézt soubor *backup.zip*, který obsahuje zálohu databáze. Použitím bruteforce techniky na hash hesla administrátora je možné heslo získat do několika minut. Po získání hesla je potřeba nalézt administrátorské rozhraní, které se nachází na url *\admin*, a tím úlohu dokončit.

8.6.3.4 Případ Home Defense

V tomto případě se nachází dvojice úloh. První úloha se zaměřuje na reverzní inženýrství ransomware malware, kterým byl zašifrován důležitý soubor. Ransomware používá ke generování hesla pro šifrování uživatelské jméno, tudíž není příliš složité heslo získat a soubor dešifrovat.

V druhé úloze provádí student auditing zdrojového kódu pro přihlašovací rozhraní napsané v jazyce PHP. Vzhledem k subjektivní povaze názoru na bezpečnost v informačních technologiích je úloha řešena formou aktivní kontroly od administrátora - řešení této úlohy, spolu s odůvodněním je nutné odeslat administrátorovi, který řešení zkontroluje a studentovi přičte body.

Kapitola 9

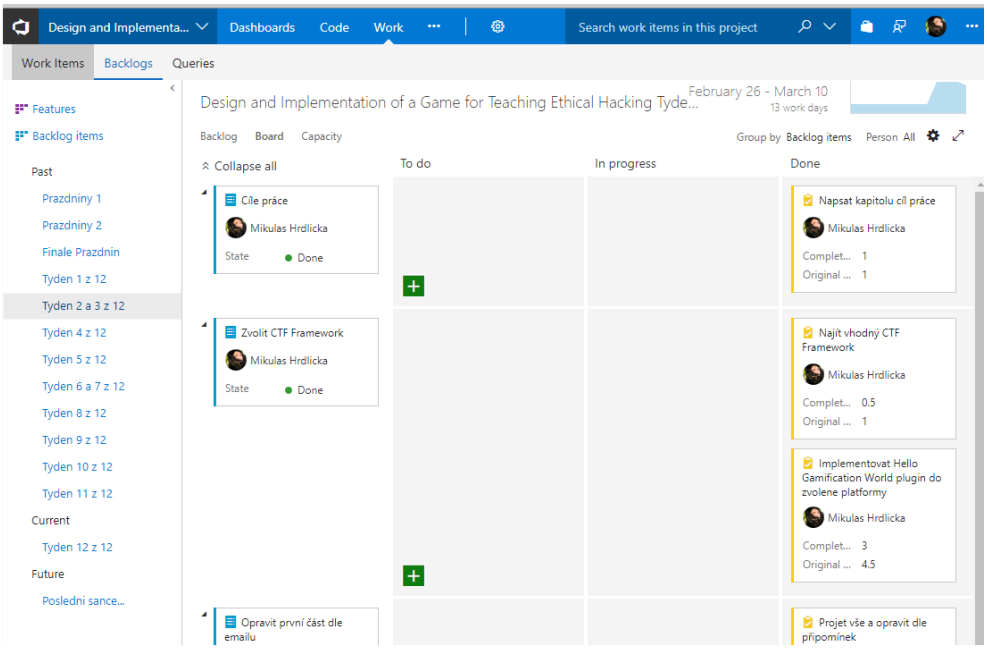
Implementace a nasazení

V této kapitole bude napsáno pár slov o způsobu, jakým byla praktická část práce realizována. Bude zde popsán systém, jakým byla implementace vedena, jaké nástroje byly použity, a jakým způsobem byla práce nasazena do produkce pro potřeby kurzu.

9.1 Vedení projektu

Projekt byl veden iterativní metodou vývoje, s týdenní délkou iterací. Na konci každého týdne byla finalizována rozpracovaná textová a návrhová část práce, zkompilována a poslána vedoucímu práce na schválení. Na základě zpětné vazby byla textová část upravena. V momentě kdy životní cyklus projektu dosáhl implementační části, byl praktikován stejný týdenní postup. Návrh a funkční požadavky byly s každou iterací mírně pozměněny, aby lépe vyhovovaly novým požadavkům, jež vyplynuly z nových informací, které postupný vývoj přinášel.

Projekt byl veden za použití platformy *Microsoft VisualStudio Team Services* [70], jež obsahuje veškeré potřebné funkce pro vedení týmu, jako je například podpora průběžné integrace včetně automatických testů, privátní verzovací repozitář, a systém na plánování práce stavěný pro potřeby agilního vývoje. Platforma je určena pro vedení rozsáhlých projektů velkých týmů, a je používána převážně v komerční sféře velkými korporacemi. Z četných funkcí této platformy bylo vzhledem k velikosti týmu využito pouze systému rozvržení a plánování úkolů a práce, a verzování. Platforma byla zvolena z důvodů osobní preference autora práce, a jeho dobrými zkušenostmi s touto platformou. Příklad plánování práce je zobrazen na obrázku číslo 9.1.



Obrázek 9.1: Plánování práce za použití platformy VSTS

9.2 Praktická implementace

Projekt byl implementován za použití vývojového prostředí *Microsoft Visual Studio* [69], z důvodů preferencí autora, a propojení nástroje s platformou vedení projektu *Visual Studio Team Services*. Verzování bylo zajištěno *Git* repozitářem poskytnutým jako součást platformy *VSTS*.

9.2.1 Podíl vlastní implementace

Většina sociálních funkcí a funkcí zpětné vazby byla implementována autorem práce. Naprostá většina kódu, který je součástí vizuálního tématu (*EHA-Gamification theme*) a zásuvného modulu *EHAGamification*, který obsahuje veškeré nové funkce, byla psána autorem práce. Na přiloženém CD se nachází zdrojový kód projektu, ve kterém jsou všechny soubory, které byly upraveny nebo psány autorem práce znatelně označeny formou komentáře na začátku souboru. V naprosté většině se jedná o soubory ve složkách s názvem *EHA-Gamification*. Do samotného *CTFd frameworku* bylo zasahováno minimálně, jediný zásah který byl proveden byl z důvodu neexistujícího rozhraní na export úloh a databázových tabulek které jsou součástí zásuvných modulů.

9.3 Tvorba úloh

Tvorba úloh probíhala za použití hypervizoru *Oracle VM VirtualBox* [80], a vytvořením virtuální appliance na které byl nainstalován systém *ArchLinux*. Po úspěšné instalaci a základní konfiguraci byl nainstalován a nakonfigurován zranitelný software potřebný pro řešení úloh. V některých případech bylo nutné zranitelné služby naprogramovat. Použité technologie pro vývoj se lišily dle potřeb vyvíjené služby. Při tvorbě zranitelných appliancí bylo celkem použito následujících technologií:

- Programovací jazyk *C* a *C++*, pro tvorbu dvojice server aplikací, jedné klientské přihlašovací aplikace, a programu na zjištění persistence v úloze *Commorragh*.
- Skriptovací jazyk *bash*, převážně pro tvorbu skriptů pro práce služby *cron*, jež zajišťuje start potřebných služeb po spuštění zranitelných strojů.
- Programovací jazyk *Python*, *SQL*, a *jQuery* při tvorbě webové aplikace pro úlohu *Damimier Substances*.
- Programovací jazyk *C#*, jež byl spolu s *Windows Forms* frameworkem použit při tvorbě ransomware aplikace v úloze s názvem *BetterTear*.
- Programovací jazyk *PHP*, při tvorbě úlohy auditingu zdrojového kódu.
- Programovací jazyk *Ruby*, použitý při tvorbě simulované komunikace mezi zranitelným serverem a klienty, která byla ve formě *.pcap* souboru součástí zadání.

9.4 Nasazení

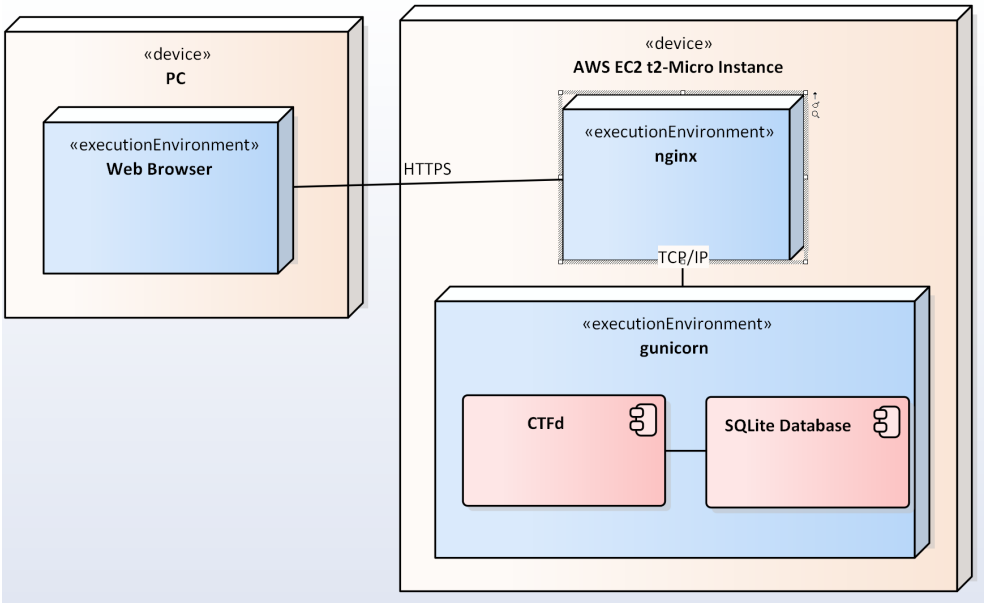
Pro potřeby praktického testu implementované platformy bylo nutné zařídit hosting, který splňuje požadavky na počet aktivních uživatelů, a bude schopný zajistit bezproblémový přístup studentů kurzu *BI-EHA*. Vzhledem k faktu, že vyvíjený produkt je součástí již kompletního frameworku *CTFd*, možnosti a způsob nasazení je dostatečně důkladně popsán v dokumentaci frameworku [28]. Vyvíjený modul je pouze zásuvným modulem do tohoto frameworku, a na způsobu nasazení nic nemění. Ucelený návod ukázkového postupu nasazení je obsažen na přiloženém digitálním médiu.

9.4.1 Praktické nasazení

Z důvodu nutnosti otestovat vyvíjené řešení na studentech kurzu *BI-EHA*, byla platforma nasazena a zveřejněna na internetové adrese `http://bieha.fun`, která byla pořízena za použití registrátora domén *Namecheap.com* [76]. Na obrázku číslo 9.2 je zobrazen diagram nasazení, který byl pro tento případ zvolen. Bylo využito služby *Amazon Elastic Compute Cloud* [8], pro zajištění Linuxové instance na které je spuštěna webová aplikace, a DNS služby *Amazon Route 53* [9], která zajišťuje propojení získané domény s instancí na které

je platforma spuštěna. Pro zajištění *SSL* šifrování a možnosti použití *https* protokolu byla použita certifikační služba *LetsEncrypt* [51], která umožňuje získání potřebných certifikátů zdarma, a automatizovanou cestou.

Z několika možností nasazení *CTFd Frameworku* byla zvolena možnost nasazení za použití kombinace reverzního proxy *nginx*, a WSGI (Web Server Gateway Interface) serveru *gunicorn*, na kterém je spuštěna *CTFd* aplikace. Během prvních dnů testování byla platforma hostována za použití web serveru vestavěného do *Flask* frameworku. Tato možnost nasazení ale není doporučována [81], neboť sebou přináší problémy se škálovatelností. Přesměrování portů bylo realizováno za použití *iptables*, což se ukázalo jako problémové v momentě, kdy bylo nutné nasadit podporu SSL, a zajistit přesměrování z *http* verze stránky na šifrovanou verzi užívající protokol *https*. Z toho důvodu byl po několika dnech provozu zvolen *nginx* + *gunicorn* způsob nasazení.



Obrázek 9.2: Diagram nasazení vyvinuté platformy

Kapitola 10

Testování na studentech předmětu BI-EHA

Výsledek implementace, spolu s úlohami, byl po dobu několika týdnů zveřejněn na webové adrese `https://bieha.fun`. Odkaz byl rozeslán studentům předmětu *BI-EHA*, kteří měli možnost se zaregistrovat a řešit zadané úlohy.

Po uplynutí doby dvou týdnů byl registrovaným studentům rozeslán dotazník, ve kterém hodnotili svou interakci s platformou, a řešením problémů. Vzhledem k faktu, že ani jedna z úloh nebyla úspěšně vyřešena, byl dotazník zaměřen spíše na důvod tohoto nedostatku motivace, než na samotnou interakci s platformou.

10.1 Statistiky interakce s platformou

Z celkového počtu 86 studentů předmětu *BI-EHA* zareagovalo na prosbu o vyzkoušení platformy pouze 11 studentů, kteří se do platformy registrovali. Z těchto 11 studentů pouze 2 dokončili úvodní set úloh, které slouží k seznámení uživatelů s platformou a formou řešení úloh. Z této dvojice pouze jeden student dokončil jednu další úlohu, která byla zaměřena na reverzní inženýrství a analýzu malware.

10.2 Dotazník

Zaregistrovaným studentům byl rozeslán dotazník, jehož otázky byly zaměřeny na průběh interakce s platformou. Otázky byly vystaveny jako kombinace otevřených otázek, a hodnocení na stupnici od jedné do pěti. Dotazník je obsažený na přiloženém CD. V dotazníku byly obsaženy otázky na následující témata:

- Uživatelská přívětivost a atraktivnost platformy a zvoleného tématu/příběhu.

- Které úkoly se uživatel pokusil vyřešit, a z jakého důvodu je nedořešil.
- Zpětná vazba o platformě a úkolech.

10.2.1 Výsledek dotazníku

Vzhledem k velmi nízkému počtu odpovědí není možné z dotazníku vyvozovat žádné závěry. Z deseti dotázaných studentů pouze dva reagovali na prosbu o vyplnění dotazníku. Jejich odpovědi byly pozitivní, interakce s platformou je bavila, a celkové průměrné hodnocení v číselných otázkách se pohybovalo okolo hodnoty 4.5/5.

Hlavní nedostatky které mohli zapříčinit nedostatečnou míru interakce studentů s platformou jsou dle názoru autora práce takto:

- Nutnost použití zranitelných virtuálních strojů, které si musí student opatřit. Pro vyřešení všech úkolů které platforma obsahuje je nutné stáhnout objem dat o celkové velikosti okolo 5 GB. Tento bod je také podpořen jednou z odpovědí v dotazníku.
- Krátký časový úsek mezi uveřejněním platformy a sběrem dat, a nevhodně zvolená doba uveřejnění, vzhledem k povinnostem které studentům vysokých škol běžně vznikají s blížícím se koncem semestru.
- Nedostatečná motivace studentů. Samotná existence platformy se sama o sobě nejeví jako dostatečně zajímavá motivace k interakci s ní.

10.3 Možná řešení

Dle nízké míry účasti studentů na platformě lze soudit, že platforma sama o sobě není dostatečně zajímavá, aby většinu studentů motivovala k interakci s ní. Některé z důvodů které by mohli tento fakt zapříčinit jsou napsány výše. Vzhledem k nedostatečné zpětné vazbě není možné odhalit příčinu tohoto nedostatku, a je pouze možné navrhnout obecná řešení, který by mohla míru účasti studentů zvýšit.

Možná řešení, která by mohla v budoucnu zvýšit počet studentů věnujících čas interakci s platformou, a umožnit tím kvalitnější sběr dat a zpětné vazby, jsou například následující:

- Úlohy a platformu studentům představit na začátku semestru. Tím bude vyřešen nedostatek času na řešení úloh.
- Motivovat studenty v rámci předmětu *BI-EHA*, například pozitivním ovlivněním výsledné známky studenta dle počtu vyřešených úloh, nebo vyhlášením věcných odměn pro úspěšné řešitele.
- Zajistit hosting zranitelných virtuálních strojů, nebo studentům umožnit přístup do laboratoře, ve které jsou tyto stroje již k dispozici, aniž by bylo nutné je stahovat za použití internetu.
- Řešení úloh zapojit jako součást laboratorních cvičení při výuce *BI-EHA*.

- Vytvořit jednodušší set úloh, který nevyžaduje zranitelné virtuální stroje. Tento bod je podpořen získanými daty, které ukazují, že 5/10 studentů jenž s platformou interagovali řešili pouze úlohy, pro jejichž řešení nebyl vyžadován virtuální stroj, a o žádné další se nepokusili.

Závěr

Hlavním cílem této práce bylo vytvořit počítačovou hru, platformu anebo soutěž, která interaktivní formou, a za využití prostředků gamifikace, představí a umožní uživatelům prakticky si vyzkoušet a procvičit základní témata z osnov kurzu Etického Hackování na FIT ČVUT. Po důkladné literární rešerši a analýze se ukázalo jako nejvhodnější řešení vytvořit gamifikovanou platformu, jejíž funkce se soustředí převážně na vyřešení problémů s komunikací a zpětnou vazbou, které byly pozorovány jako nejslabší stránky existujících řešení.

Tato platforma byla implementována jako zásuvný modul do existujícího frameworku pro soutěže s názvem *CTFd*. Mezi hlavní implementované funkce patří systém zpětné vazby, který umožňuje studentům odevzdávat postupy řešení, které jsou po ohodnocení vyučujícím zveřejněny, a systém vzájemné pomoci, který umožňuje studentům kontaktovat své spolupracovníky v případě, že si s úlohou neví rady.

Dále bylo vytvořena pětice úloh, inspirovaných reálnými událostmi v kybernetickém trestním právu, jejichž řešení využívá znalosti ze všech témat probraných v osnovách kurzu Etického Hackování.

Vypracované řešení bylo vyzkoušeno na studentech kurzu *BI-EHA*. Zájem bohužel nebyl vysoký, a naprostá většina studentů nevěnovala řešení úloh potřebný čas.

Vzhledem k rozsahu práce, a nutnosti vytvořit během realizace nápad, návrh, implementaci a také obsah, práce nezahrnuje dostatečné testování řešení. V budoucnosti by bylo možné provést na platformě penetrační testování, a důkladně otestovat její bezpečnost. Také je možné aplikaci rozšířit o další gamifikační prvky, jako je například větší personalizace profilu, dynamičtější systém nápovědy, jednodušší přístup k návodům a řešení, nebo automatický hosting zranitelných virtuálních strojů za použití cloudových služeb.

Literatura

[1] *Capture The Flag Competitions · isislab/Project-Ideas Wiki · GitHub* [online] [cit. 2018-02-26]. Dostupné z: `https://github.com/isislab/Project-Ideas/wiki/Capture-The-Flag-Competitions`

[2] *CTFtime.org / DEF CON CTF Qualifier 2017* [online] [cit. 2018-02-17]. Dostupné z: `https://ctftime.org/event/459`

[3] *picoCTF - CMU Cybersecurity Competition* [online] [cit. 2018-02-16]. Dostupné z: `https://picoctf.com/`

[4] *[The Circle Of HOPE] - Hackers On Planet Earth Conference* [online] [cit. 2018-02-10]. Dostupné z: `https://hope.net/`

[5] *Tools and Resources to Prepare for a Hacker CTF Competition or Challenge* [online] [cit. 2018-02-26]. Dostupné z: `http://resources.infosecinstitute.com/tools-of-trade-and-resources-to-prepare-in-a-hacker-ctf-competition-or-challenge/`

[6] ISO/IEC/IEEE International Standard - Systems and software engineering – Life cycle processes –Requirements engineering. *ISO/IEC/IEEE 29148:2011(E)*, Dec 2011: s. 1–94, doi:10.1109/IEEESTD.2011.6146379.

[7] Aharoni, M.; Kearns, D.; Hertzog, R.: *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution* [online] [cit. 2018-05-10]. Dostupné z: `https://www.kali.org/`

[8] Amazon Web Services, Inc: *Amazon EC2* [online] [cit. 2018-05-11]. Dostupné z: `https://aws.amazon.com/ec2/`

[9] Amazon Web Services, Inc: *Managed Cloud DNS - Domain Name System - Amazon Route 53 | AWS* [online] [cit. 2018-05-11]. Dostupné z: `https://aws.amazon.com/route53/`

[10] Amazon.com, Inc.: *Amazon Best Sellers: Best Computer & Video Game Design* [online] [cit. 2018-04-02]. Dostupné z: https://www.amazon.com/Best-Sellers-Books-Computer-Video-Game-Design/zgbs/books/10806593011

[11] Apple Inc.: *Foursquare City Guide on the App Store* [online] [cit. 2018-04-03]. Dostupné z: https://itunes.apple.com/cz/app/foursquare-city-guide/id306934924?mt=8

[12] Bayer, M.: *SQLAlchemy - The Database Toolkit for Python* [online] [cit. 2018-05-09]. Dostupné z: https://www.sqlalchemy.org/

[13] Blizzard Entertainment: *Blizzard Entertainment: About Blizzard Entertainment* [online] [cit. 2018-02-15]. Dostupné z: http://eu.blizzard.com/en-gb/company/about/

[14] Bogost, I.: Gamification is bullshit. *The gameful world: Approaches, issues, applications*, ročník 65, 2015.

[15] Boopathi, K.; Sreejith, S.; Bithin, A.: Learning cyber security through gamification. *Indian Journal of Science and Technology*, ročník 8, č. 7, 2015: s. 642–649.

[16] Bratrstvo Luny feat. Petr Štěpán: *Bratrstvo Luny feat. Petr Štěpán (XIII. století) - Třináctý úplněk* [online]. 12 2017 [cit. 04/04/2018]. Dostupné z: https://sanctuarycz.bandcamp.com/track/t-in-ct-pln-k

[17] Brumley, D.; Stephanie; Carlisle, M.: *picoCTF 2017* [online] [cit. 2018-02-12]. Dostupné z: https://picoctf.com/

[18] Cheung, R. S.; Cohen, J. P.; Lo, H. Z.; aj.: Challenge based learning in cybersecurity education. In *Proceedings of the 2011 International Conference on Security & Management*, ročník 1, 2011.

[19] kai Chou, Y.: *The 14-day Gamification Course* [online] [cit. 2018-04-08]. Dostupné z: http://join.yukaichou.com/14-day-gamification-course/

[20] kai Chou, Y.: *Octalysis: Complete Gamification Framework - Yu-kai Chou* [online] [cit. 2018-04-03]. Dostupné z: http://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/

[21] kai Chou, Y.: *Gamification to improve our world: Yu-kai Chou at TEDxLausanne - YouTube* [online]. 2 2014 [cit. 2018-04-03]. Dostupné z: https://www.youtube.com/watch?v=v5Qjuegtiyc

[22] Chung, K.: *CTFd GitHub* [online] [cit. 2018-02-12]. Dostupné z: https://github.com/CTFd

[23] Concise AC Ltd: *Infosec Conferences* [online]. 2017 [cit. 2018-01-30]. Dostupné z: https://infosec-conferences.com/

[24] Conklin, A.: The use of a collegiate cyber defense competition in information security education. In *Proceedings of the 2nd annual conference on Information security curriculum development*, ACM, 2005, s. 16–18.

[25] Conklin, A.: The Use of a Collegiate Cyber Defense Competition in Information Security Education. In *Proceedings of the 2Nd Annual Conference on Information Security Curriculum Development*, InfoSecCD '05, New York, NY, USA: ACM, 2005, ISBN 1-59593-261-5, s. 16–18, doi: 10.1145/1107622.1107627. Dostupné z: http://doi.acm.org/10.1145/1107622.1107627

[26] Conti, G.; Babbitt, T.; Nelson, J.: Hacking competitions and their untapped potential for security education. *IEEE Security & Privacy*, ročník 9, č. 3, 2011: s. 56–59.

[27] Cowan, C.; Arnold, S.; Beattie, S.; aj.: Defcon capture the flag: Defending vulnerable code from intense attack. In *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, ročník 1, IEEE, 2003, s. 120–129.

[28] CTFd LLC: *Advanced Deployment - CTFd/CTFd Wiki - GitHub* [online] [cit. 2018-05-11]. Dostupné z: https://github.com/CTFd/CTFd/wiki/Advanced-Deployment

[29] CTFtime team: *CTFtime.org / Archive 2017* [online] [cit. 2018-02-16]. Dostupné z: https://ctftime.org/event/list/?year=2017&online=-1&archive=true&restrictions=-1

[30] CTFtime team: *CTFTime.org* [online]. 2012 [cit. 2018-01-31]. Dostupné z: https://ctftime.org/ctfs

[31] CTFtime team: *DEF CON CTF Qualifier 2017* [online]. 2017 [cit. 2018-01-31]. Dostupné z: https://ctftime.org/event/459

[32] Czech News Agency: *Czech, Moldovan police bust up large drug-trafficking gang | Prague Monitor* [online] [cit. 2018-05-10]. Dostupné z: http://praguemonitor.com/2018/03/22/czech-moldovan-police-bust-large-drug-trafficking-gang

[33] datagram: *DC24 Tamper-Evident Contest: King of the Hill* [online]. 2016 [cit. 2018-01-31]. Dostupné z: https://forum.defcon.org/forum/defcon/dc24-official-unofficial-parties-social-gatherings-

events-contests/dc24-villages/tamper-evident-village-ac/223347-dc24-tamper-evident-contest-king-of-the-hill

[34] Dautry, P.; Delval, H.: *GitHub - pdautry/py_chall_factory: Small framework to create/manage/package jeopardy CTF challenges* [online] [cit. 2018-02-12]. Dostupné z: https://github.com/pdautry/py_chall_factory

[35] David Kotz, C. M., Tristan Henderson: *A Community Resource for Archiving Wireless Data At Dartmouth* [online] [cit. 2018-02-10]. Dostupné z: https://crawdad.org/

[36] Davis, A.; Leek, T.; Zhivich, M.; aj.: The Fun and Future of CTF. In *3GSE*, 2014.

[37] DEF CON Communications, Inc.: *DEF CON® Hacking Conference* [online] [cit. 2018-02-17]. Dostupné z: https://www.defcon.org/

[38] Deterding, S.: Gamification: Designing for Motivation. *interactions*, ročník 19, č. 4, Červenec 2012: s. 14–17, ISSN 1072-5520, doi: 10.1145/2212877.2212883. Dostupné z: http://doi.acm.org/10.1145/2212877.2212883

[39] Deterding, S.; Dixon, D.; Khaled, R.; aj.: From Game Design Elements to Gamefulness: Defining „Gamification“. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, MindTrek '11, New York, NY, USA: ACM, 2011, ISBN 978-1-4503-0816-8, s. 9–15, doi:10.1145/2181037.2181040. Dostupné z: http://doi.acm.org/10.1145/2181037.2181040

[40] Eagle, C.: Computer security competitions: Expanding educational outcomes. *IEEE Security & Privacy*, ročník 11, č. 4, 2013: s. 69–71.

[41] Eagle, C.; Clark, L., John; (U.S.), N. P. S.: Capture-the-Flag: Learning Computer Security Under Fire. 2004. Dostupné z: https://calhoun.nps.edu/handle/10945/7203

[42] Fink, G.; Best, D.; Manz, D.; aj.: Gamification for Measuring Cyber Security Situational Awareness. In *Foundations of Augmented Cognition*, editace D. D. Schmorrow; C. M. Fidopiastis, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, ISBN 978-3-642-39454-6, s. 656–665.

[43] Foursquare Labs, Inc.: *About* [online] [cit. 2018-04-02]. Dostupné z: https://foursquare.com/about

[44] Gamification.co: *Gamification Summit 2011 San Francisco* [online] [cit. 2018-04-02]. Dostupné z: https://en.xing-events.com/gamificationsummit.html

[45] Ganas, C.; Becker, T.; Burket, J.: *GitHub - picoCTF/picoCTF-Platform-2: A genericized version of picoCTF 2014 that can be easily adapted to host CTF or programming competitions.* [online] [cit. 2018-02-12]. Dostupné z: `https://github.com/picoCTF/picoCTF-Platform-2`

[46] Genovese, V.: *GitHub - legitbs/scorebot* [online] [cit. 2018-02-12]. Dostupné z: `https://github.com/legitbs/scorebot`

[47] Goodreads Inc: *Popular Game Design Books* [online] [cit. 2018-04-02]. Dostupné z: `https://www.goodreads.com/shelf/show/game-design`

[48] Google: *Google CTF 2017 - Rules* [online] [cit. 2018-02-16]. Dostupné z: `https://capturetheflag.withgoogle.com/rules`

[49] Google LLC: *Our company | Google* [online] [cit. 2018-02-15]. Dostupné z: `https://www.google.cz/intl/en_cz/about/our-company/`

[50] Hipp, Wyrick & Company, Inc.: *SQLite* [online] [cit. 2018-05-09]. Dostupné z: `https://www.sqlite.org/index.html`

[51] Internet Security Research Group: *Let's Encrypt - Free SSL/TLS Certificates* [online] [cit. 2018-05-11]. Dostupné z: `https://letsencrypt.org/`

[52] iOUCH Research Team: *Pain Squad App* [online] [cit. 2018-04-06]. Dostupné z: `http://www.sickkids.ca/Research/I-OUCH/Pain-Squad-App/index.html`

[53] Johnson, L. F.; Smith, R. S.; Smythe, J. T.; aj.: Challenge-Based Learning: An Approach for Our Time. *New Media Consortium*, 2009.

[54] Jordan, P.: *GitHub - mcpa-stlouis/hack-the-arch: Welcome to HackTheArch! A free open source scoring server for cyber Capture the Flag competitions!* [online] [cit. 2018-02-12]. Dostupné z: `https://github.com/mcpa-stlouis/hack-the-arch`

[55] Kamasheva, A.; Valeev, E.; Yagudin, R.; aj.: Usage of Gamification Theory for Increase Motivation of Employees. *Mediterranean Journal of Social Sciences*, feb 2015, doi:10.5901/mjss.2015.v6n1s3p77. Dostupné z: `https://doi.org/10.5901/mjss.2015.v6n1s3p77`

[56] Kapp, K. M.: *The gamification of learning and instruction: game-based methods and strategies for training and education.* John Wiley & Sons, 2012.

[57] Kickstarter, PBC: *Kickstarter* [online] [cit. 2018-04-08]. Dostupné z: `https://www.kickstarter.com/`

[58] Kittle, M.: *GDC Vault - Your Users Just Want to Play: Learning the Basics of Gamification* [online]. 2011 [cit. 2018-04-01]. Dostupné z: http://www.gdcvault.com/play/1015065/Your-Users-Just-Want-to

[59] ladymerlin: *Rance wining black bag at defcon 21* [online]. 2013 [cit. 2018-01-31]. Dostupné z: https://www.youtube.com/watch?v=92STsM0hU2k

[60] Lee, J.; Hammer, J.: Gamification in Education: What, How, Why Bother? ročník 15, 01 2011: s. 1–5.

[61] Legitimate Business Syndicate: *DEF CON CTF 2017* [online] [cit. 2018-02-15]. Dostupné z: https://legitbs.net/

[62] Locasto, M. E.: Helping Students 0wn Their Own Code. *IEEE Security Privacy*, ročník 7, č. 3, May 2009: s. 53–56, ISSN 1540-7993, doi:10.1109/MSP.2009.66.

[63] Marcos, J.; Singh, G.; Wray, J. M.: *GitHub - facebook/fbctf: Platform to host Capture the Flag competitions* [online] [cit. 2018-02-12]. Dostupné z: https://github.com/facebook/fbctf

[64] Marczewski, A. C.: *Even Ninja Monkeys Like to Play: Gamification, Game Thinking and Motivational Design.* CreateSpace Independent Publishing Platform, 2015, ISBN 1514745666. Dostupné z: https://www.amazon.com/Even-Ninja-Monkeys-Like-Play/dp/1514745666?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1514745666

[65] MCEACHERN, A.: *A History of Loyalty Programs, and How They Have Changed* [online]. 10 2017 [cit. 2018-04-01]. Dostupné z: https://blog.smile.io/a-history-of-loyalty-programs

[66] McGonigal, J.: *Gaming can make a better world | TED Talk* [online]. 2 2010 [cit. 2018-04-06]. Dostupné z: https://www.ted.com/talks/jane_mcgonigal_gaming_can_make_a_better_world

[67] McGonigal, J.: *GDC Vault - We Don't Need No Stinkin' Badges: How to Re-invent Reality Without Gamification [SGS Gamification]* [online]. 2011 [cit. 2018-04-02]. Dostupné z: http://www.gdcvault.com/play/1014576/We-

[68] McGonigal, J.: *Reality Is Broken: Why Games Make Us Better and How They Can Change the World.* Penguin Books, 2011, ISBN 9780143120612. Dostupné z: https://www.amazon.com/Reality-Broken-Games-Better-Change/dp/0143120611?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0143120611

[69] Microsoft: *Python Development Tools | Visual Studio* [online] [cit. 2018-05-11]. Dostupné z: https://www.visualstudio.com/vs/features/python/

[70] Microsoft: *Visual Studio Team Services* [online] [cit. 2018-05-11]. Dostupné z: https://www.visualstudio.com/team-services/

[71] Miller, C.: The gamification of education. *Developments in Business Simulation and Experiential Learning*, ročník 40, 2013.

[72] MIT Cambridge: *MIT Lincoln Laboratory CSAIL Capture the Flag Competition on April 2-3* [online]. 2011 [cit. 2018-02-10]. Dostupné z: http://mitctf2011.wikispaces.com/

[73] Moloch, J.: *GitHub - moloch–/RootTheBox: A Game of Hackers (CTF Scoreboard & Game Manager)* [online] [cit. 2018-02-12]. Dostupné z: https://github.com/moloch--/RootTheBox

[74] MultiMedia LLC: *Hackfortress* [online]. 2009 [cit. 2018-01-31]. Dostupné z: http://hackfortress.net/

[75] Nakiami; Nelson, J.: *GitHub - Nakiami/mellivora: Mellivora is a CTF engine written in PHP* [online] [cit. 2018-02-12]. Dostupné z: https://github.com/Nakiami/mellivora

[76] Namecheap.com: *About Namecheap - Our Story and Mission | Namecheap.Com* [online] [cit. 2018-05-11]. Dostupné z: https://www.namecheap.com/about.aspx

[77] National Security Agency: *Cyber Defense Exercise (CDX)* [online]. 2017 [cit. 2018-01-31]. Dostupné z: https://www.iad.gov/iad/programs/cyber-defense-exercise/index.cfm

[78] NCCDC: *National Collegiate Cyber Defense Competition* [online]. 2017 [cit. 2018-01-31]. Dostupné z: http://www.nationalccdc.org/

[79] Nike, Inc.: *Nike+* [online] [cit. 2018-04-06]. Dostupné z: https://secure-nikeplus.nike.com/plus/what_is_fuel/

[80] Oracle: *Oracle VM VirtualBox* [online] [cit. 2018-05-11]. Dostupné z: https://www.virtualbox.org/wiki/Downloads

[81] Pallets Team: *Deployment Options — Flask 1.0.2 documentation* [online] [cit. 2018-05-12]. Dostupné z: http://flask.pocoo.org/docs/1.0/deploying/

[82] Palmer, C. C.: Ethical hacking. *IBM Systems Journal*, ročník 40, č. 3, 2001: s. 769–780, ISSN 0018-8670, doi:10.1147/sj.403.0769.

[83] Parliment of Pwning: *PlaidCTF 2017 - Rules* [online] [cit. 2018-02-16]. Dostupné z: http://play.plaidctf.com/rules

[84] POMO Media Group s.r.o.: *Československá Filmová Databáze - Jeopardy! (TV Pořad)* [online]. 2001 [cit. 2018-01-31]. Dostupné z: https://www.csfd.cz/film/319403-jeopardy/komentare/

[85] Raymond, E. S.: *Amateria Wargame, Level 2 Scoreboard* [online]. 2004 [cit. 2018-01-31]. Dostupné z: http://amateria.smashthestack.org:89/tags/level2.html

[86] Raymond, E. S.: *SmashTheStack Wargames* [online]. 2004 [cit. 2018-01-31]. Dostupné z: http://smashthestack.org/wargames.html

[87] Richardson, K.: *The Speed Camera Lottery - The Fun Theory - YouTube* [online]. 2010 [cit. 2018-04-06]. Dostupné z: https://www.youtube.com/watch?v=iynzHWwJXaA

[88] Rigby, S.: *GDC Vault - Gamification: That Word Doesn't Mean What You Think...* [online]. 2012 [cit. 2018-04-02]. Dostupné z: http://www.gdcvault.com/play/1016599/Gamification-That-Word-Doesn-t

[89] Ringwood, A.: *GitHub - UnrealAkama/NightShade: A simple capture the flag framework.* [online] [cit. 2018-02-12]. Dostupné z: https://github.com/UnrealAkama/NightShade

[90] Robertson, M.: *Can't Play, Won't Play* [online]. 10 2010 [cit. 04/04/2018]. Dostupné z: https://kotaku.com/5686393/cant-play-wont-play

[91] Ronacher, A.: *Flask (A Python Microframework)* [online] [cit. 2018-05-09]. Dostupné z: http://flask.pocoo.org/

[92] Ronacher, A.: *Jinja2 Templating Rngine for Python* [online] [cit. 2018-05-09]. Dostupné z: http://jinja.pocoo.org/docs/2.10/

[93] Savin, N.: *CVE-2012-0805* [online] . Dostupné z: https://www.cvedetails.com/cve/CVE-2012-0805/

[94] Schell, J.: *The Art of Game Design: A Book of Lenses.* San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2008, ISBN 0-12-369496-5.

[95] Schell, J.: *The Pleasure Revolution: Why Games Will Lead the Way (GSummit SF 2013) - YouTube* [online]. 10 2013 [cit. 2018-04-06]. Dostupné z: https://www.youtube.com/watch?v=-55Nz73_zm4

[96] Sciglimpaglia Jr, R. J.: Computer Hacking: A Global Offense. *Pace International Law Review*, ročník 3, č. 1, 1991: str. 199.

[97] See, C.: *Gamification in Higher Education | TEDxCUHK - YouTube* [online] [cit. 2018-03-30]. Dostupné z: `https://www.youtube.com/watch?v=d8s3kZz1yQ4`

[98] Sheldon, L.: *The multiplayer classroom: Designing coursework as a game*. Cengage Learning, 2011.

[99] Steven "Steven" Van Acker, m.: *OverTheWire* [online]. 2011 [cit. 2018-01-31]. Dostupné z: `http://overthewire.org/wargames/`

[100] Thomashaw, T.: *GitHub - cliffe/SecGen: Create randomly insecure VMs* [online] [cit. 2018-02-12]. Dostupné z: `https://github.com/cliffe/SecGen`

[101] Todor, V.; Pitică, D.: The gamification of the study of electronics in dedicated e-learning platforms. In *Proceedings of the 36th International Spring Seminar on Electronics Technology*, May 2013, ISSN 2161-2528, s. 428–431, doi:10.1109/ISSE.2013.6648287.

[102] UBM: *Game Developers Conference | GDC | Conference Overview* [online] [cit. 2018-04-06]. Dostupné z: `http://www.gdconf.com/conference/index.html`

[103] UW Center for Game Science: *Solve Puzzles for Science | Foldit* [online] [cit. 2018-04-06]. Dostupné z: `http://fold.it/portal/`

[104] Vigna, G.: *Teaching Network Security through Live Exercises*. Boston, MA: Springer US, 2003, ISBN 978-0-387-35694-5, s. 3–18, doi:10.1007/978-0-387-35694-5_2. Dostupné z: `https://doi.org/10.1007/978-0-387-35694-5_2`

[105] Vinet, J.; Griffin, A.: *Arch Linux* [online] [cit. 2018-05-10]. Dostupné z: `https://www.archlinux.org/`

[106] Wang, J.; Zhang, M.: *GitHub - EasyCTF/openctf: CTF in a box. Minimal setup required.* [online] [cit. 2018-02-12]. Dostupné z: `https://github.com/easyctf/openctf`

[107] Weight Watchers International, Inc.: *WeightWatchers.com: History of Helping People Lose Weight* [online] [cit. 2018-04-01]. Dostupné z: `https://www.weightwatchers.com/about/his/history.aspx`

[108] Weiser, B.: Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison. *New York Times*, 2015.

[109] Wikimedia Foundation: *Wikipedia* [online] [cit. 2018-04-08]. Dostupné z: https://www.wikipedia.org/

[110] Zichermann, G.: *GDC Vault - Gamification: Why Every Brand Wants to Be Zynga, and How You Can Help* [online] [cit. 2018-04-02]. Dostupné z: http://www.gdcvault.com/play/1013785/Gamification-Why-Every-Brand-Wants

[111] Zynga Inc.: *Build a farm online with FarmVille | Zynga Farm Games* [online] [cit. 2018-04-08]. Dostupné z: https://www.zynga.com/games/farmville

[112] České vysoké učení technické v Praze: *Fakulta informačních technologií ČVUT |* [online] [cit. 2018-05-07]. Dostupné z: https://fit.cvut.cz/

Příloha **A**

Seznam použitých zkratek

BI-EHA Kurz Etického Hackování na FIT ČVUT

CBL Challenge-Based Learning

CCDC National Collegiate Cyberdefence Competition

CDX Cyber Defence Exercise

CD Compact Disk

CTF Capture The Flag soutěž

ČVUT České vysoké učení technické

DEP Data Execution Prevention

EHA Viz. BI-EHA

FIT ČVUT Fakulta Informačních Technologií ČVUT

FLAG ForensicLink Access Gateway

HOPE Hackers on Planet Earth

HTML Hypertext Markup Language

NSA National Security Agency

SMTP Simple Mail Transfer Protocol

SQL Structured Query Language

SSL Secure Sockets Layer

SegFault Segmentation Fault

VM Virtual Machine

VTST Visual Studio Team Services

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `install.txt` ..... ilustrační popis nasazení práce
- `zdroj`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
- `attach` ..... přílohy práce, tabulky, dotazníky a zadání úloh