Capture The Flag (CTF) kao uvod u računarsku bezbednost

Andrija Urošević, prof. dr. Sana Stojanović Đurđević
Računarstvo i društvo
Univerzitet u Beogradu
Matematički fakultet

April, 2022.

Sažetak

Trenutno živimo u dobu koje iziskuje prikupljanje, obradu i deljenje informacija. Informacije se najčešće čuvaju na računarima ili se dele putem Interneta. Svi ti računarski sistemi koji čuvaju informacije moraju biti zaštićeni od potencijalnog curenja informacija. Tada se u računarstvu javlja nova oblast koja se naziva računarska bezbednost. Zbog dinamike u bavljenju računarskom bezbednošću, treniranje stručnih ljudi je veoma teško tradicionalnim edukacionim metodama. Jedan način rešavanja ovog problema pruža CTF kao platforma za gejmifikovani proces učenja.

Ključne reči: *Capture The Flag*, *CTF*, *računarska bezbednost*, *internet bezbednost*, *učenje*, *edukacija*.

1 Uvod

Gejmifikacija je ideja koja koristi mehanike igara radi podsticanja i motivisanja učesnika da se, kroz takmičarsko okruženje u kome je moguće pratiti napredak i relativno rangiranje, angažuju u aktivnosti u kojima je stepen angažovanost nizak [12]. Gejmifikacija ima široke primene najviše u poslovanju i marketingu. Nedavno se pokazalo da gejmifikacija ima primene i u procesu učenja. Da li je moguće iskoristiti CTF igru kao platformu za gejmifikovani proces učenja o računarskoj bezbednosti?

Termin *Capture The Flag* (CTF) se originalno odnosi na igru između dva tima. Svaki tim ima zadatak da sačuva svoju fizičku zastavicu (*flag*), dok u isto vreme pokušava da osvoji zastavicu (*flag*) drugog tima. Od 90-tih, format CTF-a se premešta na računare i Internet.

Capture The Flag (CTF) je takmičenje u oblasti računarske bezbednosti. Cilj takmičenja je pronaći *flag*-ove u nekom okruženju. Okruženje može biti različitog opsega i formata, ali generalno pronađen *flag* je dokaz rešenog zadatka (npr. pristupljeno je skrivenim podacima ili bazi). Okruženje može biti jedan veb domen ili može biti mreža računara na većoj skali.

Flag je tipično neki string karaktera, čiju specifikaciju daju organizatori takmičenja. Specifikacija mora biti jasna svim učesnicima kako bi znali da su uspešno pronašli *flag* i rešili zadatak. *Flag* obično ima neki prefiks koji učesnicima ukazuje da su zapravo pronašli *flag*. Na primer, *flag* može imati prefiks oblika `FLAG`, a sam *flag* može izgledati kao `FLAG{K73BSSxY3nFc1oAs9WwG}`. Prostor *flag*-ova mora biti dovoljno velik, kako će ta činjenica sprečiti takmičare da koriste metod grube sile za pronalaženje *flag*-a.

Od takmičara se očekuje da pronađu *flag* u datom okruženju.

Kada takmičar pronađe *flag*, on ga šalje sistemu za verifikaciju, i ukoliko je *flag* ispravan takmičar dobija poene za odgovarajući zadatak koji je rešio. Ovaj sistem je obično realizovan preko veb aplikacije, gde se takmičari mogu prijaviti, poslati pronađene *flag*-ove, i uživo pratiti trenutne rezultate.

Nakon uspešno završenog takmičenja, javlja se potreba kod takmičara da podele svoja genijalna rešenja sa ostalim učesnicima. Za osvojene *flag*-ove takmičari pišu iscrpe korake kako doći do tog *flag*-a. Dokumenti koji nastaju nazivaju se *write-up*-ovi. Preko *writeup*-ova učesnici mogu da uporede svoja rešenja ili pronađu određeno rešenje za *flag* koji nisu uspešno pronašli. U ovom procesu učesnici pospešuju svoja znanja, i stiču nove tehnike.

Postoje 3 glavne vrste CTF takmičenja: *Jeopardy*, *Attack-Defence*, i *Mixed* [4]. U *Jeopardy* CTF-u, takmičari dobiju unapred zadatke, koji su zadati u statičkom okruženju, tj. drugi takmičari ne mogu uticati na okruženje i pri tome otežavati pronalaženje *flag*-ova. *Attack-Defence* stil podrazumeva borbu između više timova. Svaki tim ima sopstveno dinamičko okruženje u kome se nalaze *flag*-ovi. Tim može menjati svoje dinamičko okruženje, i time osigurava svoj *flag*. Ovaj postupak predstavlja odbranu (*defence*) iz naziva. Napad (*attack*) podrazumeva pronalaženje *flag*-ova u protivničkom okruženju. Za svaku uspešnu odbranu od napada, ili uspešan napad timovi dobijaju *flag* sa određenim brojem poena. *Mixed* CTF može biti različitog formata, ali kao što ime sugeriše predstavlja mešavinu prethodna dva stila.

Popularnost CTF takmičenja raste iz godinu u godinu. `CTFTime` u svojoj arhivi ima preko 300 javno dostupnih CTF takmičenja za 2021. godinu, dok za 2016. godinu ima preko 100 javno dostupnih CTF takmičenja [4]. Jedno od prvih i najpoznatijih CTF takmičenja je DEFCON CTF koji se svake godine održava na DEFCON konferenciji o računarskoj bezbednosti [3]. Pored DEFCON CTF-a postoje i mnoga druga CTF takmičenja kao što su UCSB iCTF, Mozilla CTF, Facebook CTF, Google CTF, PHD CTF, RuCTFe, Hack.lu CTF, SECUINSIDE CTF, rwth CTF, CSAW CTF, PICO CTF [15]. Jedan interesantan CTF, koji se održava u Srbiji svake godine, u okviru DESCON hakatona je DESCON CTF [6]. DESCON CTF je namenjen za početnike. Takođe, dobar resurs za vežbanje pre takmičenja predstavlja `OverTheWire` [14].

2 Znanja i veštine koje se stiču kroz CTF

Treniranje profesionalaca u oblasti računarske bezbednosti zahteva puno vremena i novca, ali pruža jedno veoma održivo globalno rešenje. Mnoge obrazovne institucije, društva informatičara, državne organizacije, i privatne kompanije su svesne toga te konstantno uvode nove studijske programe, i kurseve. Jedan od tih studijskih programa je CSEC2017 [5].

Pored formalnog obrazovanja, povećava se popularnost neformalnih metoda. CTF predstavlja jednu takvu metodu gde učesnici poboljšavaju svoje znanje u oblasti računarske bezbednosti kroz razne zadatke. Kako CTF zadaci često poseduju takmičarske elemente i elemente igre, oni su neformalnog karaktera i teško je odrediti njihovu vezu sa formalnim metodama.

Postavlja se pitanje o tome kako i koliko su povezani formalni metodi, u vidu studijskih programa, sa neformalnim metodama poput CTF-a. U daljem tekstu su opisane oblasti znanja koje definiše CSEC2017, nakon čega sledi studija o distribuciji tih oblasti znanja u CTF zadacima.

2.1 CSEC2017 oblasti znanja

CSEC2017 definiše osam oblasti znanja u računarskoj bezbednosti.

1. *Bezbednost podataka* sadrži kriptografiju, forenziku, integritet podataka, i autentifikaciju.

2. *Bezbednost softvera* se fokusira na bezbednost u programiranju, testiranju, i druge aspekte razvoja softvera.

3. *Bezbednost komponenti* se odnosi na bezbednosti komponenti koje se integrišu u veće sisteme, što uključuje njihov dizajn i obrnuto inženjerstvo.

4. *Bezbednost konekcije* podrazumeva mrežne servise, odbrane, i napade.

5. *Bezbednost sistema* sadrži kontrolu pristupa, i etičko hakovanje (eng. *pen testing*).

6. *Bezbednost ljudi* se odnosi na čuvanje identiteta, podataka, i privatnost. Sadrži socijalno inženjerstvo i svesnost o računarskoj bezbednosti.

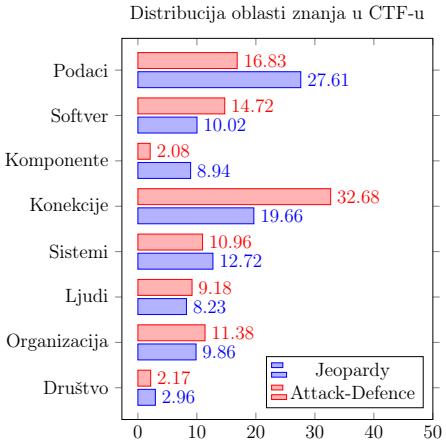
7. *Organizaciona bezbednost* se fokusira na menadžment rizika, bezbednosne polise, i upravljanje incidentima na nivou organizacije.

8. *Društvena bezbednost* se bavi računarskom bezbednošću na nacionalnom ili globalnom nivou.

2.2 Distribucija oblasti znanja u CTF zadacima

Švábenský i dr.[17] ispitivali su distribuciju oblasti znanja u CTF zadacima. Ispitivanje je vršeno nad podacima, koji čine 5963 *writeup*-ova. Ovi podaci su preuzeti sa `CTFTime.org` koji u svojoj bazi, između ostalog, čuva i *writeup*-ove raznih zadataka sa CTF takmičenja [4].

Metod podrazumeva pet faza. Prva faza je izdvajanje ključnih reči iz CSEC2017 [5], koje određuju svako od znanja. Druga faza je preuzimanje i parsiranje *writeup*-ova sa `CTFTime.org` [4]. Treća faza predstavlja analizu *writeup*-ova, tj. prebrojavanje



Slika 1: Distribucija oblasti znanja u 15879 *jeopardy* i 86 *attack-defense writeup*-ova [17].

instanci ključnih reči u svakom *writeup*-u. Sledeća, četvrta faza predstavlja normalizaciju broja instanci ključnih reči. Poslednja, peta faza se sastoji u dodeljivanju *writeup*-ova odgovarajućoj oblasti znanja [17].

Najzastupljenija oblast znanja za *Jeopardy* stil CTF-a je *bezbednost podataka*, dok *bezbednost konekcije* i *bezbednost sistema* zauzimaju drugo i treće mesto, respektivno. *Bezbednost podataka* uključuje kriptografiju, i autentifikaciju, što opravdava prvo mesto zbog same prirode zadataka iz tih oblasti. Naime, takvi zadaci su laki za dizajn i proveru. Za *Attack-Defence* stil CTF-a dobija se da je *bezbednost konekcija* na prvom mestu. Ovaj rezultat ima smisla kako timovi konstantno vrše napade na druge timove. Ostali rezultati se nalaze na slici 1 [17]. Interesantno je to da dobijeni rezultati odgovaraju rezultatima o distribuciji oblasti znanja na master studijskim programima iz kurseva o računarskoj bezbednosti [1, 17].

Glavno ograničenje ove analize je mali skup podataka nad kojima je analiza vršena, zajedno sa odbacivanjem polovine skupa podataka zbog neuspešnog parsiranja [17]. Postavlja se, takođe, pitanje o pouzdanosti samih *writeup*-ova, tj. o njihovoj povezanosti sa samim CTF zadatkom. Pod pretpostavkom da *writeup*-ove pišu entuzijasti i

sami dizajneri CTF zadataka, možemo pretpostaviti njihovu pouzdanost.

3 Problemi u CTF modelu

Cilj CTF takmičenja je okupiti ljude koji se bave računarskom bezbednošću različitog nivoa znanja i veština, kako bi oni mogli međusobno da dele informacije, pored samog takmičarskog elementa. Čitava zajednica poštuje CTF kao platformu za učenje novih veština, ali nekolicina članova direktno priča o problemima sa kojima se susreću organizatori i takmičari, gde je svaki problem detaljno opisan u narednim podsekcijama.

CTF se vrti oko računarske bezbednosti, ali je u suštini slobodan za bilo koje druge oblasti. Zbog toga CTF zadatak može testirati dosta nepoznate oblasti znanja, koje se samo delimično mogu naći u literaturi, dokumentaciji, ili čuti na nekom kursu ili radionici. Dobra strana slobode koju CTF-ovi pružaju je u tome što otvara nove teme i uzdiže bezbednost na viši nivo.

Sama struktura CTF zadataka se svodi na "sve ili ništa", tj. nije moguće parcijalno rešiti neki zadatak. To otvara mogućnosti za dalje istraživanje, i zajedno sa ograničenim vremenom forsira takmičare da budu efikasniji. Čak i kada takmičar nije na pravom putu on može naučiti o nekoj oblasti. Ovo stvara okruženje u kome najuporniji pobeđuju, bez obzira na njihov tehnički nivo. Veruje se da ce uspešni takmičari biti oni koji se prepuste učenju i kulturi CTF-ova.

Pored svih uspešnih stvari koje donosi CTF kao platforma za učenje i proveru znanja, postoje problemi koji narušavaju ovaj model. Jedan od najvećih problema je uvođenje novih ljudi u takmičenja [2]. Novi takmičari počinju sa takmičenjem po preporuci. Oni veoma retko nastavljaju sa igranjem CTF-a ukoliko ne uspevaju da reše ni jedan zadatak. Ovo može izazvati frustracije, te mnogi odustaju od takmičenja.

Sledeće podsekcije sadrže neke probleme koje su uočili Čang i Koen [2] u višegodišnjoj organizaciji CTF takmičenja.

3.1 Težina igre

CTF igre nisu jednostavne za igranje, tj. teško je ući u sam zadatak, čak i za veterane, a pogotovu za nove takmičare. CTF zadatak objašnjava veoma malo o tome kako ga rešiti, već prepušta igraču da sam smisli optimalan put do rešenja, kao što je to u igrama poput šaha ili igre go. Baš na ovom aspektu se dobija na mogućnosti izučavanja raznih oblasti. CTF podrazumeva da će njegovi takmičari biti eksperti u svojoj oblasti, te iz godine u godinu zajednica raste, a sami zadaci postaju sve teži. Ovo stvara veoma veliki pritisak na novog takmičara. Zbog toga je veoma teško početi sa takmičenjem, čak i za one sa dobrim tehničkim predznanjem.

3.2 Relacija između dizajna zadataka i njegove uspešnosti pri rešavanju

Uspešan CTF događaj je onaj koji ima balans između učenja i provere znanja. Zbog toga, organizatori imaju veoma težak posao da osmisle dovoljno teške zadatke iz kojih će takmičari steći znanje. Sa druge strane zadaci ne smeju biti previše teški, jer se takmičari mogu zaglaviti na tom zadatku, i pri tome se stvara rizik o izgubljenom vremenu učesnika i organizatora. Naime, takmičari neće pogledati ostale zadatke, i samim tim neće rešiti neki lakši zadatak i steći priliku za učenje nove oblasti. Pored toga, organizatori će izgubiti vreme pri kreiranju zadataka koje niko neće pokušavati da reši. Iz tog razloga dobri zadaci predstavljaju one zadatke koji navode do sopstvenog rešenja. Jedna metrika koja meri težinu zadatka može biti broj uspešnih rešenja. Lak zadatak će imati veliki broj uspešnih rešenja, dok će težak zadatak imati

mali broj uspešnih rešenja.

Svakom zadatku organizatori dodeljuju poene, koje će takmičar dobiti pri uspešnom rešavanju tog zadatka. Poeni su u direktnom odnosu sa težinom zadatka, pa će tako teški zadaci nositi puno poena, dok će laki zadaci nositi malo poena. Kako postoje mnogi CTF događaji, koji ciljaju na određene nivoe znanja, poeni predstavljaju lokalnu skalu težine zadataka tog CTF događaja.

Često organizatori pokušavaju da modifikuju zadatke, tako da oni postanu teži, dodavanjem veštačkih konstrukcija. Ovakve konstrukcije su dizajnirane da namerno izazovu frustracije takmičara, i veruje se da će mali broj takmičara uspeti da ih reši. Ove tehnike otežavanja dovode do toga da zadatak ostane nerešen ili pak rešen od strane malog broja takmičara, jer zapravo uključuje faktor sreće.

Još jedan način otežavanja zadatka je integrisanje grube sile u rešenje zadatka. Gruba sila ne predstavlja dobar način savladavanja novih veština, već samo dovodi do gubitka vremena pri rešavanju na CTF događaju gde je vreme veoma bitan faktor.

CTF takmičenja pored uobičajenih zadataka uključuju i veoma lake zadatke. Laki zadaci podužu entuzijazam takmičara, i vagaju između igre i takmičenja. Oni su tu radi uživanja, jer će ih svaki takmičar rešiti bezmalo truda.

3.3 Dokaz o kvalitetu

Veterani su vešti u razumevanju postavke zadatka, ali problem nastaje kod novajlija. Naime, novajlije treba uvesti u novu oblast, kroz uvod u zadatak. Ne treba takmičare u potpunosti navoditi do rešenja, jer tu onda dolazi do slepog ispunjavanja uslova i gubi se na istraživanju i učenju. Kako bi ovaj problem bio smanjen, pri organizaciji i kreiranju zadataka najbolje je imati tim ljudi koji su na istom nivou kao i takmičari. Ovo želimo jer tada oni razmišljaju isto kao i takmičari, te mogu davati direktne povratne informacije o navođenju koje treba implementirati u zadatke.

Nakon što je zadatak napravljen ulazi se u fazu dokaza o kvalitetu. Za svaki CTF događaj ova faza je drugačija. Jedan primer može biti u tome da organizatori između sebe dele zadatke i pokušavaju da reše tuđi zadatak. Organizatori koji rešavaju zadatke direktno mogu da revidiraju zadatak, i da daju povratne informacije o tome kako ga popraviti. Onda započinje novi krug razvoja zadataka, koji se sastoji u poboljšanju trenutnih zadataka.

Mnogi CTF događaji zanemaruju ovu fazu, ili joj ne pridaju veliki značaj. To dovodi do nerešivih zadataka, neadekvatno konfigurisane infrastrukture, i zadataka čiji poeni ne reflektuju njihovu težinu.

3.4 Poeni i njihov obrnuti efekat na takmičare i organizatore

Dolazimo do interesantnog zapažanja nakon što takmičari dobiju zadatke. Naime, takmičari će veštački odrediti težinu zadatka, pre čitanja uvoda u zadatak, samo na osnovu njegovog broja poena. Neiskusni takmičari će pomisliti da nemaju dovoljno znanja za neki zadatak koji ima veliki broj poena, pa će se fokusirati na one sa manjim brojem poena. Ova strategija odabira zadataka može dovesti do zaglavljanju na zadacima određene oblasti sa kojim takmičar ima veoma malo iskustva. Sa druge strane, takmičar može imati znanja o nekom zadatku sa više poena, te ga u potpunosti zanemariti, jer nije uspeo rešiti onaj sa manjim brojem poena. Izbegavanje CTF zadataka je trenutno nerešivi problem.

3.5 Infrastruktura zadataka

Interakcija sa takmičarima se obično odvija putom veb platforme. Na platformi se nalaze timovi, zadaci, sistem za bodovanje i proveru *flag*-ova. U nekim situacijama dešava se korišćenje nefunkcionalnih veb

platformi. Neki primeri: (1) nemogućnost učitavanja, (2) *flag*-ove je moguće pronaći grubom silom, (3) takmičari ostvaruju proizvoljan broj poena. Ovo najčešće nastaje kada organizatori nemaju dovoljno vremena da osiguraju infrastrukturu.

Pre samog CTF događaja organizatori treba da testiraju sve moguće propuste infrastrukture. Serveri treba da podnesu veliki saobraćaj. Za svaki zadatak treba imati posebnu formu koja će proveravati *flag*, zajedno sa vremenskim ograničenjem provere kako bi se sprečilo korišćenje metoda grube sile. Treba očekivati pokušaje varanja, kao što se to i očekuje na svim ostalim takmičenjima, te zbog toga treba osmisliti sisteme za detekciju varanja. Sve to doprinosi sigurnom i fer CTF događaju.

3.6 Dvosmisleni zadaci

Postoje primeri zadataka koji imaju više od jednog puta do rešenja. Isto tako postoje zadaci kod kojih rešenja nisu jasno određena u opisu, i sam tok rešavanja ne navodi do pravog rešenja. Ako spojimo ove dve činjenice dobijamo dvosmislene zadatke koji se jedino mogu rešiti uz faktor sreće. Ovakvi zadaci nastaju jer im se pridaje malo pažnje na kreativnoj formulaciji. Zbog toga svaki zadatak mora imati svoj opis koji pruža korisne informacije, zajedno sa navođenjem i uveravanjem takmičara da je na pravom putu.

4 CTF na univerzitetskim kursevima

Jedan od glavnih aspekata CTF takmičenja je u nadmudrivanju protivnika. Ali na žalost ovaj aspekt nedostaje na mnogim univerzitetskim kursevima računarske bezbednosti. Jedno rešenje predlažu Mirković i Piterson [11] sa svojom verzijom CTF-a: *Class Capture The Flag* (CCTF). Naime, CCTF zahteva minimalno dodatnog vremena od studenata, minimalno rada na osmišljanju zadataka od strane profesora i saradnika u nastavi, dok u isto vreme uključuju studente u timski rad simulacijom realnog scenarija. Svaki CCTF zadatak se fokusira na jednu oblast koja se obrađuje na datom kursu. Ovo doprinosi primeni znanja koje je student stekao tokom predavanja. Nakon svakog CCTF događaja, vrši se analiza sa studentima o tome šta su uradili ispravno, a šta pogrešno, sa ciljem unapređenja sledećeg CCTF događaja.

4.1 CCTF vs CTF

CCTF se za razliku od tradicionalnog CTF-a održava na manjoj skali. Razlog toga je okruženje u kome se on izvršava. Naime, CCTF ima neke jedinstvene osobine koje ga čine pogodnim za univerzitetske kurseve. Razlike između CTF-a i CCTF-a su date na tabeli 1. U nastavku su opisane neke osobine koje CCTF poseduje:

Osobina	CTF	CCTF
Pripremanje	nekoliko meseci	nekoliko nedelja
Trajanje	1-2 dana	2 časa
Uloge timova	crveni[a] ili plavi[b]	crveni i plavi
Uparivanje timova	svi na sve	parovi
Učestalost	jednom godišnje	2-3 puta po semestru
Analiza	retko	uvek
Težina	stručni	početni do srednji

[a]Oni koji napadaju u *Attack-Defense* CTF-u
[b]Oni koji se brane u *Attack-Defense* CTF-u

Tabela 1: Upoređivanje CTF-a i CCTF-a.

1. **Laka realizacija.** CTF događaji zahtevaju najmanje 24 časa za izvršavanje i mnogo nedelja za samu pripremu. Dok je za CCTF potrebno oko dve nedelje priprema, i izvršava se u roku od 2 časa. Time studenti i predavači ne gube vreme za ostale aktivnosti.
2. **Učestaliji i sa analizom.** Mnogi CTF događaju se održavaju jednom godišnje i sa sobom nose malo pobednika i mnogo gubitnika. Ovo može da demotiviše one koji su izgubili i odvrati ih od oblasti računarske bezbednosti. Mnogi učesnici nemaju visok nivo edukacije, i iskustva. Oni zbog toga vrlo lako

odustaju od samog takmičenja. Sa druge strane, CCTF se dešava više puta u toku jednog semestra. To omogućava studentima da se takmiče više puta godišnje sa minimalno dodatnog ulaganja i truda. Nakon svakog CCTF vrši se analiza, gde učesnici mogu diskutovati o strategijama koje su koristili, i tako unaprediti svoje veštine.

3. **Dvostran.** CTF takmičenja su obično jednostrana, u smislu da timovi napadaju neki unapred određen sistem, ili da se brane od napada profesionalaca iz struke. CCTF su dvostrana, te će timovi biti u prilici da napadaju i da budu napadnuti.

4. **Doigravanje.** Za razliku od CTF takmičenja gde svaki tim igra protiv svih ostalih timova, CCTF uparuje timove u više iteracija. Ovo omogućava postojanje više pobedničkih timova tokom semestra i ima kao posledicu povećanje entuzijazma.

5. **Svestran.** CCTF pruža mogućnost fokusiranja na određene oblasti, pa studenti mogu primeniti znanje koje su stekli tokom semestra. Sa druge strane, CCTF omogućava kombinaciju različitih oblasti, što će studente naterati da posmatraju računarsku bezbednost u celosti. Takođe, studenti će morati da donose brze odluke, i da snose posledice za one loše odabrane odluke.

4.2 Poboljšanje edukacije kroz CTF

Gejmifikacija poboljšava pored ostalog i proces učenja [7, 16]. Odatle dolazimo do prirodnog pitanja: Da li CTF (kao igra) može da poboljša samo učenje o računarskoj bezbednosti. Postoji nekoliko radova koji se bave ovom problematikom.

Leune i Petrilli [8] u svom radu postavljaju sledeće pitanje: Da li se uključivanjem u realne simulacije odbrana i napada — u obliku CTF zadataka — povećava efektivnost pri učenju o računarskoj bezbednosti? Kao meru uspešnosti definišu sledeće hipoteze:

1. Samopouzdanje studenata će se povećati učestvovanjem u CTF-u.

2. Studenti će uživati u CTF-u.

3. Studenti će steći praktične veštine učestvovanjem u CTF-u.

4. Učestvovanje u CTF potkrepljuje teorijske koncepte.

Prva hipoteza se pokazuje kao tačna. Mogućnost izvođenja raznih tehnika u kontrolisanom okruženju povećava samopouzdanje kod studenta da sam izvrši, prepozna i odbrani se od napada. Druga hipoteza je, takođe, tačna. Mnogi studenti su prijavili kako su veoma uživali u samom rešavanju zadataka, i da su provodili mnogo više vremena na samim zadacima nego što su planirali. I treća hipoteza je tačna, jer postoji jasna razlika između rezultata onih koji su učestvovali u CTF-u i onih koji nisu. Četvrta hipoteza nije jasno pokazana, ali se spekuliše da treba podeliti CTF zadatke na teorijske i praktične, i da će ta podela doprineti poboljšanju samih rezultata kod studenata.

4.3 Prednosti i mane CTF zadataka na univerzitetskim kursevima

CTF igre nisu idealno rešenje koje donosi samo dobre stvari sa sobom. Kao i sve ostalo ima svoje mane. Neka zapažanja o dobrim i lošim stranama CTF zadataka na univerzitetskim kursevima nam daju Vikopal i dr. [18]:

1. **Performanse studenata.** Postoji značajna statistička korelacija između promenljivih koje su izvučene iz CTF zadataka i rezultata kolokvijum/ispita.

Korišćen je Spirmenov keoficijent korelacije i dobijeni rezultati su u intervalu od -0.5 do 0.63, ali se veruje da su mnogo bolji zbog nedostatka vođenja evidencije o važnim događajima tokom CTF-a (vreme prikaza zadatka, vreme podnošenja tačnog *flag*-a, itd.).

2. **Korisna navođenja.** Medijalna razlika između vremena pružanja smernica i podnošenja tačnog *flag*-a pokazuje da su neke smernice korisnije od drugih. Treba izbegavati navođenja koja su očigledna i ne pružaju nikakvu dodatnu informaciju kako bi se problem rešio. Zbog toga ona moraju biti dovoljno informativna i adaptivna, ali ne smeju biti u obliku uputstva.

3. **Plagiranje CTF *flag*-ova.** Primećeno je četiri vrste plagijata: (1) slanje istih *flag*-ova u bliskim vremenskim opsezima; (2) korektan *flag* je poslat kao nekorektan *flag* na drugom zadatku: (3) zadaci su rešeni bez preuzimanja potrebnih fajlova; (4) brzo rešavanje uzastopnih zadataka.

4. **CTF igre sa studentske strane.** Anketa koja je sprovedena nakon uspešno završenog kursa pokazuje da većina studenata (13 od 16) preferira CTF igre u odnosu na uobičajene zadatke koje imaju tokom regularnih kurseva. Studenti koji preferiraju CTF igre, vole to što su igre zabavne, interaktivne, koriste razne alate, i uče kroz pokušavanjem. Dva studenta su tvrdila da su CTF zadaci teži od uobičajenih zadataka i da je potrebno puno vremena za njihovo rešavanje. Jedan student je izjavio da je lakše prepisati CTF zadatak od uobičajenih zadataka (dovoljno je prepisati *flag*).

5 Zaključak

Videli smo da se formalni metodi učenja (kursevi, seminari, master studijski programi, itd.) i neformalni metodi učenja (CTF takmičenja) u velikoj meri poklapaju po oblastima znanja koje definiše CSEC2017. Naime, i jedan i drugi metod pridaju veći značaj određenim oblastima znanja. Ovo ima smisla kako su baš te oblasti znanja primarne.

Dalje, uvideli smo da CTF takmičenja donose jako puno problema takmičarima kao i organizatorima takmičenja. Novi takmičari retko nastavljaju sa takmičenjima, jer su zadaci veoma teški. Organizatori veoma često u procesu otežavanja zadataka dodaju neke oblasti znanja koje su veoma šturo opisane u literaturi, ili dokumentaciji. Takođe, organizatori vrlo često zamrse problem tako da on postane nerešiv. Pored toga postoje i problemi sa infrastrukturom zadataka i platforme.

Na kraju smo razmatrali i pokušaje implementiranja CTF-a na univerzitetskim kursevima. Pored otklonljivih problema koje donosi ovakav poduhvat, ukupan rezultat je pozitivan i sa profesorske i sa studentske strane.

Dalja diskusija. CTF donosi jako puno dobih osobina: razmišljanje van okvira poznatog, istraživanje, poboljšava efikasnost, timski rad, široko znanje iz mnogih oblasti, i mnoge druge intelektualne osobine. Pored toga donosi i nekakvo interno i društveno zadovoljstvo. Problem nastaje u tome što je CTF zajednica veoma zatvorena za početnike. Pored povećanja popularnosti potrebno je omogućiti novim članovima da se glatko upuste u CTF vode. CTF je igra čija pravila mogu biti definisana i adaptirana na mnoge oblasti van računarske bezbednosti. Te se postavlja pitanje: Da li je moguće jednako uspešno ili čak uspešnije primeniti CTF koncept na druge oblasti?

Literatura

[1] Krzysztof Cabaj i dr. “Cybersecurity education: Evolution of the discipline and analysis of master pro-

grams". U: *Computers & Security* 75 (2018.), str. 24–35. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.01.015.

[2] Kevin Chung i Julian Cohen. "Learning Obstacles in the Capture The Flag Model". U: *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. San Diego, CA: USENIX Association, avg. 2014.

[3] Crispin Cowan i dr. "Defcon Capture the Flag: defending vulnerable code from intense attack". U: maj 2003., 120–129 vol.1. ISBN: 0-7695-1897-4. DOI: 10.1109/DISCEX.2003.1194878.

[4] *CTFTime.org / All about CTF (Capture The Flag)*. 2022. URL: https://ctftime.org.

[5] Joint Task Force on Cybersecurity Education. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. 2018. URL: https://cybered.acm.org/.

[6] *DESCON, DESCON IoT Hackathon*. 2022. URL: https://descon.me.

[7] Benjamin Geelan i dr. "Improving Learning Experiences Through Gamification: A Case Study". U: *Australian Educational Computing* 30.1 (jul 2015.).

[8] Kees Leune i Salvatore J. Petrilli. "Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education". U: *Proceedings of the 18th Annual Conference on Information Technology Education*. SIGITE '17. Rochester, New York, USA: Association for Computing Machinery, 2017., str. 47–52. ISBN: 9781450351003. DOI: 10.1145/3125659.3125686.

[9] William Marchand Niño, Edwin Vega Ventocilla i Jose Santillan. "Capture the Flag for Computer Security Learning". U: nov. 2017.

[10] L. McDaniel, E. Talvi i B. Hay. "Capture the Flag as Cyber Security Introduction". U: *2016 49th Hawaii International Conference on System Sciences (HICSS)*. Los Alamitos, CA, USA: IEEE Computer Society, jan. 2016., str. 5479–5486. DOI: 10.1109/HICSS.2016.677.

[11] Jelena Mirkovic i Peter A. H. Peterson. "Class Capture-the-Flag Exercises". U: *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. San Diego, CA: USENIX Association, avg. 2014.

[12] Cristina Ioana Muntean. "Raising engagement in e-learning through gamification". U: *Proc. 6th international conference on virtual learning ICVL*. Sv. 1. 2011., str. 323–329.

[13] Eric Nunes i dr. "Cyber-Deception and Attribution in Capture-the-Flag Exercises." U: (2015.).

[14] *OverTheWire.org / We're hackers, and we are good-looking. We are the 1%.* 2022. URL: https://overthewire.org.

[15] Raghu Raman i dr. "Framework for evaluating Capture the Flag (CTF) security competitions". U: *2014 International Conference for Convergence of Technology, I2CT 2014* (apr. 2015.). DOI: 10.1109/I2CT.2014.7092098.

[16] Ganit Richter, Daphne R. Raban i Sheizaf Rafaeli. "Studying Gamification: The Effect of Rewards and Incentives on Motivation". U: *Gamification in Education and Business*. Urednik Torsten Reiners i Lincoln C. Wood. Cham: Springer International Publishing, 2015., str. 21–46. ISBN:

978-3-319-10208-5. DOI: 10 . 1007 / 978-3-319-10208-5_2.

[17] Valdemar Švábenský i dr. "Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges". U: (jan. 2021.).

[18] Jan Vykopal, Valdemar Švábenský i Ee-Chien Chang. "Benefits and Pitfalls of Using Capture the Flag Games in University Courses". U: (apr. 2020.).

[19] Fabio Massimo Zennaro i Laszlo Erdodi. "Modeling Penetration Testing with Reinforcement Learning Using Capture-the-Flag Challenges: Trade-offs between Model-free Learning and A Priori Knowledge." U: (2020.).