# Capture the flag -tehtävien käyttö kyberturvan käytännöntaitojen kehittämisessä

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Joulukuu 2025
Jetro Pelttari

TURUN YLIOPISTO
Tietotekniikan laitos

Jetro Pelttari: Capture the flag -tehtävien käyttö kyberturvan käytännöntaitojen kehittämisessä

TkK-tutkielma, 26 s.
Tietotekniikka
Joulukuu 2025

---

Tämä tutkielma käsittelee capture the flag -tehtävien (CTF-tehtävien) käyttöä kyberturvan käytännön oppimisessa. Tutkielman tavoitteena on tutkia CTF-tehtävien käyttöä kyberturvan oppimisessa korkeakouluympäristössä, eritysesti miettien, miten CTF-tehtävämalli vaikuttaa opiskelijoiden motivaatioon, sekä mitä eri toimintatapoja malli mahdollistaa. Tutkimus perustuu kirjallisuuskatsaukseen, johon on kerätty CTF-tehtäväpohjaisista lähteistä tutkimustuloksia.
CTF-tehtävillä pyritään antamaan opiskelijoille käytännön kokemusta teoreettisen osaamisen lisäksi. Tutkimuksessa nähtiin CTF-pohjaisen opetuksen vaikuttavan positiivisesti opiskelijoiden motivaatioon sekä opiskelumieltymykseen. Positiivista vaikutusta vahvisti CTF-tehtävien mahdollistama käytännönkokemus teoreettisen osaamisen lisäksi sekä välitön palaute tehtävistä. Tämän lisäksi kirjallisuudessa oli poikkeamia arvosanakehityksessä, joissakin tutkimuksissa havaitut muutokset olivat negatiivisia, kun taas muissa nähtiin positiivista korrelaatiota arvosanojen ja CTF-tehtävien välillä.
Tutkimus osoitti, että CTF-tehtävät ovat hyödyllinen osa kyberturvan oppimista. Ne eivät kuitenkaan korvaa oppimista kokonaa, vaan toimivat parhaiten yhtenä kokonaisuutena muun kurssin lisäksi. Täten pyritään luomaan yhtenäinen ja vahva yhdistelmä teoriaa ja käytännön läheisyyttä.

Asiasanat: CTF, kyberturvallisuus, oppimismotivaatio, pelillistäminen

# Sisällys

# Kuvat

# Taulukot

# 1 Johdanto

Tässä työssä käsitellään Capture the flag -tehtävien (CTF-tehtävien) hyödyntämistä kyberturvan käytännöntaitojen kehittämisessä. Jatkuva kasvu kyber- ja tietoturva-asiantuntijoiden tarpeesta [1] motivoi löytämään uusia vaihtoehtoja opettamiseen ja tapoihin motivoida uusia opiskelijoita alalle. Vuosittain tapahtuvat kyberhyökkäykset ovat jatkuvassa nousussa [1], [2], tällöin myös kybertietämyksen tulisi nousta. CTF-tehtävät ovat toimineet hyvänä tapana opetellessa uusia aiheita ja parantaneet ongelmanratkaisukykyä. Tätä kautta on myös halu kehittää ja tutkia uusia tapoja opiskella ja opettaa kyber- ja tietoturva-alan aiheita.

Kyber- ja tietoturva aiheet ovat nykyään jokaiselle ihmiselle tärkeitä, sillä lähes kaikki käyttämämme palvelut toimivat digitaalisessa ympäristössä. Näiden kautta myös vahva kyberosaaminen asiantuntijoilla ja alan toimijoilla on tärkeää, sillä mahdollisissa vikatilanteissa tai kriisinaikana pitää varmistaa, että digitaaliset käyttöympäristöt saadaan pidettyä toiminnallisina. Varsinkin kriittisissä infrastruktuureissa korkea osaaminen ja tarve pystyä pitämään kaikki toiminnallisena on erityisen tärkeää, jolloin pitää löytää keinoja varmistaa osaaminen ja parantaa sitä [3].

Tutkielmassa pyritään vastaamaan käytännön kokemuksen tarpeeseen kyber- ja tietoturva-alalla. CTF-tehtäviä voidaan miettiä lipunryöstötehtävinä, joissa osallistujat pyrkivät ratkaisemaan aihepiirin kysymyksiä ja tehtäviä, joiden kautta he löytävät vastauksen eli lipun. Tehtävien ratkaisu vaatii teoreettista osaamista, joka yhdistetään käytännön taitoihin. Pääpiirteinen idea on pelillistää opettamista,

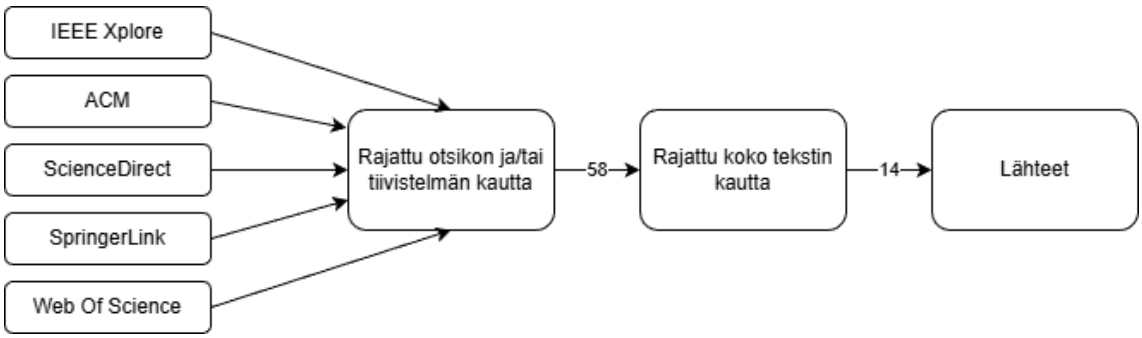
pelillistämisellä kyetään motivoimaan ja innoittamaan opiskelijoita paremmin kuin perinteisillä opetusmenetelmillä. Lisäksi CTF-tehtävät antavat hands-on-kokemusta teoreettisen tietämyksen lisäksi, jolla pyritään luomaan monipuolista osaamista opiskelijoille. Näistä muodostettiin tutkimuskysymykset:

**TK1.** Miten CTF-tehtävät vaikuttavat motivaatioon kyberturvan oppimisessa?

**TK2.** Millaisia toimintatapoja voidaan hyödyntää CTF-pohjaisessa opetuksessa?

**TK3.** Mitä ongelmatilanteita ja vaikeuksia voi ilmetä CTF-pohjaisessa opetuksessa?

Aineistojen haku aloitettiin luomalla hakulausekkeita tärkeimmistä termeistä, joita olivat "CTF" ja "cybersecurity". Näistä luotiin alustava hakulauseke *("CTF" OR "capture-the-flag") AND "cybersecurity" AND "university"*. Tällä hakulausekkeella aloitettiin tekemään hakua IEEE Xploresta, ACM:sta, ScienceDirectistä, Web Of Sciencesta sekä SpringerLinkistä. Tuloksia rajattiin enemmän lisäämällä hakulausekkeisiin "effectiveness" ja/tai "performance". Hakutuloksien rajaus on kuvattu kuvaan 1.1.




Kuva 1.1: Aineiston rajauksen kuvaaminen

Näitä tuloksia rajattiin otsikon ja lyhyen johdannon silmäilyn kautta, jolloin jäljelle jäi 58. Nämä 58 luettiin läpi, jotta löydettiin tutkielmassa lähteiksi haluttuja aineistoja. Rajauksessa katsottiin useasti esille tulevia aihealueita ja teemoja, näiden

kautta saatiin luotua jo perustaa tutkielmaan. Tämä rajasi tutkimuslähteitä 14:sta. Rajaus tehtiin tutkimalla, että teksteissä puhutaan juuri CTF tehtävistä, sekä mahdollisissa kyselyissä oli kohteina korkeakouluopiskelijoita tai työympäristössä olevia. Tärkeänä katsottiin myös, että sisälsikö lähteet teemoiltaan samankaltaisia aiheita, jotta tapaustutkimus onnistuisi. Tämän lisäksi lähteinä toimii yritysten sivuja tai muita ei tieteellisiä tekstejä, jotka toimivat kertomaan CTF aiheesta lisää.

Tutkielman rakenne etenee siten, että luvussa kaksi kerrotaan mikä CTF on ja miten sitä voidaan käyttää opetusmetodina, lisäksi kerrotaan CTF-tehtävien muita käyttökohteita. Tämän jälkeen luvussa kolme käydään eri aihealueita läpi ja luodaan perustaa miten CTF-tehtävät toimivat opetustilanteessa, vastaten samalla tutkimuskysymyksiin. Lopuksi luvussa neljä tehdään pohdintaa, mitä tutkittiin ja mihin lopputulokseen päädyttiin.

# 2 Capture the Flag

Capture the Flag -tehtävät ovat kyberturvan oppimisessa toimivia käytännön harjoituksia. Tehtäviä on nykyään pääsääntöisesti kahden tyylisiä. Ensimmäinen on "Jeopardy-style" eli vaaratyyppinen CTF. Näissä tehtävissä osallistujille annetaan erilaisia haasteita eri vaikeustasoilla ja kategorioilla. Yleisiä kategoria ovat verkkopalvelujen hakkerointi, takaisinmallinnus (engl. reverse engineering), avoimen lähteiden tiedustelu (engl. Open-source intelligence, OSINT), kryptografia (engl. cryptography) tai forensiikka (engl. forensics). Tehtävissä osallistujan on määrä löytää lippu joko ratkaisemalla haasteessa olevat kysymykset tai löytämällä lippu haasteessa olevalta laitteelta. Lippu palautetaan tehtävän vastaukseen ja tällöin siitä saa pisteet. Lippu löytyy jostain tehtävän sisällä olevasta tiedostosta ja lippu on yleisesti tyyliä "flag{tekstiä tai numeroita}". Toinen CTF-tehtävätyyli on tilanne, jossa kaksi tiimiä asetetaan vastakkain hyökkääjät (engl. Red team) vs puolustajat (engl. Blue team) tilanteeseen. Nämä tehtävät vaativat yleisesti osallistujilta enemmän kokemusta kuin ensimmäinen tehtävätyyli. [4], [5]

Ideana on, että CTF-tehtävät koittavat mimikoida oikean elämän tilanteita siten, että niissä on jokin haavoittuvuus, jota tulee hyödyntää tehtävät ratkaisemiseksi. Tehtävistä saa käytännön esimerkkejä siitä, miten palveluhyökkäyksiä voidaan toteuttaa ja miten käytännössä teoreettiset tilanteet voisivat toimia. Yritysmaailmassa on myös CTF-tehtävä tyylisiä ohjelmia, näitä ovat Bug Bounty -ohjelmat[1].

[1]Bug Bounty -ohjelman avaus www.hackerone.com/bug-bounty-programs

Ohjelmien ideana on luoda yrityksen omista palveluista maailmanlaajuisesti testattavia, jossa halukkaat tietoturvaosaajat voivat etsiä haavoittuvuuksia palveluista. Näin yritys saa tietoonsa tietoturvaongelmia ja ongelmien löytäjät palkitaan. [3], [6]

CTF-tehtävät voivat olla esimerkiksi kilpailutyylisesti järjestettyjä tapahtumia, joissa annetaan aikaraja ja jokin määrä tehtäviä, joista pitää löytää lippu ennen aikarajan umpeutumista. Tehtävät voivat olla myös nettisivuilla pyöritettäviä haaste- tai oppimistehtäviä, joita pystyy ratkaisemaan koska vaan, tälläisestä esimerkki on tryhackme [7]. Palveluilla, kuten tryhackme on yleensä luotu myös pisteytysjärjestelmä ja tulostaulukko, joilla tehdään CTF-ratkaisusta kilpailullisempaa ja mahdollisuus henkilöille haastaa itseään enemmän.

Perinteisesti CTF etenee yrityksen tai oppilaitoksen valitessa alusta, jossa kilpailu pidetään. Alusta voi olla omilla palvelimilla pyörivä ns. "offline" kilpailu tai valmista pohjaa käyttävä palvelu kuten CTFd, Facebook CTF tai TryHackme [5], [8]. Tämän jälkeen kutsutaan pelaajat mukaan ja annetaan ohjeet miten ja missä kilpailu järjestetään. Kilpailussa haavoittuvaiset palvelut pyörivät virtuaaliverkossa ja kilpailivat tarvitsevat pääsyn tähän virtuaaliverkkoon ennen aloittamista. Päästyään virtuaaliverkkoon kilpailijoille aukeaa näkyviin kohteita, joihin hyökkäykset voi tehdä. Riippuen järjestäjästä näihin kohteisiin merkataan vaikeustaso, kategoria eli millaisesta haavoittuvuudesta on kyse ja mahdolliset pisteet mitä lipun löytämisestä saa.

Kun kilpailija valitsee kohteen, jota haluaa alkaa selvittämään niin hänelle annetaan valitun kohteen IP-osoite. IP-osoitteen avulla kohteesta selvitetään mikä mahdollinen palvelu siellä pyörii, onko kyseessä esimerkiksi nettisivu tai jokin muu. Kilpailija lähtee tutkimaan kohdetta itselle tutulla tai opitulla tavalla ja jotain kautta pääsee kohteeseen sisälle, joka tarkoittaa pääsyä kohteen tiedostoihin. Tiedostoihin pääsy on yleensä haastavin osuus ja tämän jälkeen lipun löytäminen on melko help-

poa. Kohteessa voi myös olla useampia lippuja, joista ensimmäisen saa pääsemällä tiedostoihin ja toinen voi vaatia esimerkiksi järjestelmänvalvojaoikeuksia. [7], [9]

## 2.1 CTF-opetusmenetelmänä

CTF-tehtävät toimivat opetusmenetelmänä teorian apuna. Tehtävät perustuvat käytännön oppimiseen (engl. practical learning), jolloin opittu ei jää pelkästään teoriaksi vaan pääsee soveltamaan taitoja oikeissa tilanteissa. Lisäksi tehtävät toimivat hyvänä tapana parantaa tiimityötaitoja ja ongelmanratkaisukykyä. Tehtävillä tai haasteilla on usein monta eri ratkaisutapaa, jolloin opiskelijat yhdessä pääsevät käyttämään oppimaansa teoriaa ja pohtimaan mahdollisia ratkaisuja. Haasteiden ideana on esittää oikeanelämän ratkaisuja, jolloin lisäämällä haasteita opetukseen valmistetaan opiskelijoita paremmin työelämään. [3], [10], [11]

Tehtävät ovat hyvin muokattavissa kurssin tarpeiden mukaan, jolloin niitä voidaan rajata aiheiden mukaisesti. Tutkimuksessa Ellis et al. [4] CTF-tehtävät jaettiin kolmeen kategoriaan, joista ensimmäinen oli johdatus CTF-tehtäviin, toinen oli johdatus kryptografiaan ja kolmas oli johdatus tietokoneverkkoihin. Lisäksi aiheiden rajauksen lisäksi tehtävät mahdollistavat laajan vaikeustaso ohjauksen, jolloin kurssitehtävien vaikeustasoa saadaan säädettyä tarpeen mukaan. Alustat mahdollistavat opettajille myös hyvät mahdollisuuden valvoa opiskelijoiden tehtävien tekoa ja tuloksia [12].

Pelillistäminen (engl. gamification) tarkoittaa pelimekaniikkojen ja toiminnallisuuksien tuomista ei-pelillisiin käyttökohteisiin. Pelillistämisellä kyetään muokkaamaan oppimista muokkaamalla nykyistä oppimisprosessia ja muutoksia tuomalla pyritään parantamaan opiskelijoiden osallistumista ja motivaatiota opiskeluun [13]. Pelillistämiseen liittyvää tutkimusta on tehty paljon ja tutkimuksissa on todettu olevan positiivisia vaikutuksia kognitiivisiin, motivaatio- ja käyttäytymiseen liitty-

viin opetustuloksiin [14]. CTF-tehtävät ovat suoraan pelillistämistä, ne sisältävät pelillistämisen mekaniikkoja, kuten pisteytys, tavoitteet ja kilpailullisuus.

## 2.2 CTF-käyttötarkoitukset

CTF-tehtävät eivät ole rajattu vain kyberturvan opetukseen vaan näille on monia käyttökohteita. Yksi näistä on turvallinen ohjelmointi (engl. secure programming). Turvallisella ohjelmoinnilla pyritään välttämään haavoittuvuudet ohjelmoijien koodissa. Haavoittuvuudet antavat mahdollisuuden esimerkiksi jollekin osapuolelle pääsyn salattuun tietoon tai vaikuttaa muuten ohjelmiston toimintaan.

Turvallisen ohjelmoinnin opetuksen tarve on nousussa sekä ohjelmistoturvallisuuden ammattilaisilla, kuin opiskelijoilla [15]. Tällöin pitää löytää tapoja parantaa ohjelmistojen turvallisuutta uusilla tavoilla. Ryan et al. [16] tutkimuksessa kysyttiin ohjelmoijilta mikäli heille on tarjottu koulutusta ohjelmistoturvallisuuteen tai -yksityisyyteen liittyviin asioihin. Tutkimuksessa vain 381 ohjelmoijaa (39.6 %) vastasivat "kyllä", 495 (51.5 %) vastasivat "ei" ja loput 86 (8.9 %) vastasivat "Ei sovellu", kyselyn tulokset on kuvattu taulukkoon 2.1.

Taulukko 2.1: Kysely ohjelmiston tietoturvaan liittyvästä koulutuksesta, perustuen lähteeseen [16]

| Vastaus | Vastaajamäärä | Prosentti |
|---|---|---|
| Kyllä | 381 | 39.6 |
| Ei | 495 | 51.5 |
| Ei sovellu | 86 | 8.9 |

Tutkimuksen tulokset vahventavat väitettä turvallisen ohjelmoinnin koulutuksen tarpeelle. Lisäksi on havaittu ohjelmoijien jättävän soveltamatta tietoturva opetustaan tehtäviin, jotka ovat vaatineet turvallista ohjelmointia, ellei sitä ole erikseen vaadittu [16].

Turvallisessa ohjelmoinnissa ohjelmoijat ja ohjelmistokehittäjät pyrkivät tunnistamaan haavoittuvuuksia suunnitteluvaiheessa tai ohjelmoinnin aikana. CTF-

tehtävät tarjoaisivat kehittäjille mahdollisuuden nähdä, miten pienetkin haavoittuvuudet vaikuttavat oikeissa tilanteissa, ja täten tarjoaisivat käytännön oppimiskokemusta. Tällä tavoin mahdollisesti parannettaisiin kehittäjien kiinnostusta turvalliseen ohjelmointiin. Kehittäjille olisi hyvä pakottaa tietoturva-ajattelua, jolloin siitä tulee normi eikä erikseen mietitty asia, jota ajatellaan vain kysyttäessä tai vaadittaessa.

## 2.3 Luvun yhteenveto

Luvussa 2 kerrottiin mitä CTF tarkoittaa ja miten CTF-tehtäviä voidaan käyttää sekä opetus- että harjoitusmenetelmänä. Luvussa käytiin läpi yleisimmät CTF-tehtävätyypit sekä normaali tehtävien eteneminen. Tehtävätyypeillä pyrittiin kuvaamaan, miten CTF-tehtävät toimivat teorian apuna luodessaan käytännön kokemusta sekä kyberturva-aiheisiin että muihin soveltuviin aiheisiin. Tietoturva-ajattelun tarvetta pyrittiin luomaan esittämällä käytännön esimerkki turvallisen ohjelmoinnin ajattelun vähyydestä. Tämän lisäksi esitettiin kuinka pelillisyyttä saadaan tuotuta CTF-tehtäviä käyttämällä. Luku pyrkii antamaan lukijalle kuvan siitä, mitä CTF-tehtävät ovat ja miten niitä voidaan hyödyntää opetuksessa. Tämän luvun tarkoitus on toimia taustana luvulle 3, jossa käsitellään tarkemmin CTF-tehtävien käyttöä opetusmuotona aineistopohjaisella pohdinnalla.

# 3 CTF:n käyttö opetusmuotona

Tässä luvussa käsitellään aineistoista esille nousevia aihealueita liittyen kyberturvan käytännön oppimiseen. Tunnistetut aihealueet on esitetty Taulukossa 3.1. Aihealueiden kautta vastataan tutkimuskysymyksiin ja tehdään pohdintaa niiden kautta. Luvussa käytännön esimerkkien ja tutkimuksen kautta luodaan pohjaa käsitteille.

Taulukko 3.1: Aineistojen aihealueet

| | Motivaatio | Arvosanakehitys | Työympäristö | Ongelmanratkaisu | CTF-myönteisyys | Vaikeustaso | Toimintatavat | Ongelmatilanteet | Kehitysehdotuksia |
|---|---|---|---|---|---|---|---|---|---|
| Abaimov et al. [11] | | | x | | | | x | x | |
| Chhetri [17] | x | | | | x | | x | | |
| Cole [18] | x | x | | | | | | | |
| Deaconescu et al. [19] | | | | | | | x | x | x |
| Egamberganova et al. [3] | x | | | x | | | x | | |
| Ellis et al. [4] | x | x | | | | | x | | |
| Ford et al. [9] | | | x | | | | x | | |
| Gleeson [20] | | | | | x | x | | x | |
| Hamad et al. [21] | x | | | | x | | x | x | |
| Leune ja Petrilli [5] | x | x | | x | | | | | |
| Schafeitel-Tähtinen ja Lazarov [12] | x | x | | | x | | x | | |
| Tobarra et al. [22] | | | | | | | x | | x |
| Vigl ja Abramova [23] | x | | | | x | x | x | | x |
| Vykopal et al. [24] | | x | | | x | | x | x | x |

## 3.1 Motivaatio ja myönteisyys

Kyberturvatehtävien ja -opettamisen pelillistäminen on todettu parantavan opiskelijoiden suorituskykyä sekä kiinnostusta aiheisiin liittyen [12]. Tutkimusta on tehty myös CTF-tehtävien samanlaisesta toiminnallisuudesta, näissä on tutkittu esimerkiksi CTF-tehtävien käyttöä kurssien aikana työkaluna, jolla tuodaan hands-on kokemusta opiskelijoille. Kiinnostusta ja motivaatiota on mitattu pääsääntöisesti kyselyillä, joita tehty esimerkiksi ennen ja jälkeen kurssien. Kyselyt on suoritettu joko avoimina vastauslomakkeina, johon voi kirjoittaa mikä opetustyylissä oli hyvää ja mikä ei, tai numeerisina tai valmiina vastausvaihtoehto tyylisinä, joissa vastataan esimerkiksi tyylillä täysin samaa mieltä tai täysin eri mieltä. Tässä alaluvussa kerrotaan näiden tutkimuksien tuloksista.

Opiskelijoiden motivaatiota parannetaan luomalla enemmän käytännön harjoitusta ja toiminnallista vaativaa opetusta, jotka näkyvät kurssipalautteissa positiivisena [21]. Lisäksi pelillistäminen opettaminen parantaa opiskelijoiden itseluottamusta ja innostaa siten oppimaan lisää aiheesta myös kurssien ulkopuolella. CTF-tehtävät mahdollistavat myös opiskelijoiden saavan palautetta tehtävästä heti tehtyään sen, sillä he näkevät oliko tulos oikein. Tämän lisäksi voidaan antaa palautetta opettajan toimesta, jossa kerrotaan tarkemmin, miten tehtävän ratkaisu onnistui. Tällä pyritään parantamaan opiskelijamotivaatiota yhä paremmaksi.

Schafeitel-Tähtinen ja Lazarov [12] tutkimuksessa oli mukana Tampereen yliopisto sekä Brnon teknillinen yliopisto. Opiskelijat osallistuivat tutkimuksessa samaan CTF-kilpailuun molemmissa yliopistoissa. CTF-kilpailun toimivuutta mitattiin esi- ja loppukyselyllä. Loppukysely oli jaettu kahteen osaan, joista toinen osa kysyttiin heti ja toinen kaksi viikkoa myöhemmin. Brnon teknillisen yliopiston tuloksia on kuvattu Taulukkoon 3.2.

Taulukko 3.2: Esi- ja loppuarvot N = 40, vihreällä merkityt arvot tilastollisesti merkitsevät muutokset, perustuen lähteeseen [12]

| | z | p | Efektikoko |
|---|---|---|---|
| CTF-aiheiden tietoisuus | -3,78 | <0,001 | 0,60 |
| CTF-tehtävätaidot | -1,64 | 0,102 | 0,26 |
| Yleinen itsevarmuus | -0,22 | 0,826 | 0,03 |
| Kyberturva itsevarmuus | -3,37 | <0,001 | 0,53 |
| CTF-tehtävä itsevarmuus | -3,41 | <0,001 | 0,54 |
| CTF-aiheiden kiinnostus | -2,51 | 0,012 | 0,4 |
| Jatko-opinto kiinnostus | -1,21 | 0,195 | 0,19 |
| Alakiinnostus | -2,24 | 0,025 | 0,35 |
| Tutkimuskiinnostus | -2,22 | 0,027 | 0,35 |

Kyselyihin osallistui yhteensä 40 opiskelijaa. Z-arvo kuvaa havaittujen erojen suuntaa ja suuruutta, jossa negatiivinen arvo tarkoittaa, että tulokset parantuivat. P-arvo kertoo eron merkitsevyyden, vihreällä merkityt arvot ovat tilastollisesti merkitseviä muutoksia. Tulokset osoittavat, että CTF-kilpailun jälkeen opiskelijoiden aiheen tuntemus, kyberturvallisuusitsevarmuus sekä CTF-tehtäväitsevarmuus paranivat merkittävästi. Tämän lisäksi alakiinnostus ja tutkimuskiinnostus paranivat tilastollisesti merkittävästi. Toisaalta CTF-tehtävätaidot, yleinen itsevarmuus ja jatko-opinto kiinnostus eivät muuttuneet tilastollisesti merkittävästi.

Vigl ja Abramova [23] tutkimuksessa käsitellään yliopistokurssia liittyen tietosuojaan ja tietoturvaan. Kyseessä oli peruskurssi maisteriopiskelijoille. Kurssin päätteeksi opiskelijoille annettiin kysely, jossa piti vastata kysymyksiin "Ehdottomasti eri mieltä" ja "Ehdottomasti samaa mieltä" välillä. Kyselyn tuloksia on koottu Taulukkoon 3.3, vastausvaihtoehdot etenevät siten, että 1a on "Ehdottomasti eri mieltä" ja 5a "Ehdottomasti samaa mieltä". Tämän lisäksi taulukkoon on merkitty keskiarvo

ja keskihajonta. Palautteista nähdään, että varsinkin motivaatioon ja tyytyväisyyteen liittyvissä asioissa CTF-tehtävät ovat toimineet opiskelijoiden mielestä.

Taulukko 3.3: CTF-haaste kurssi liittyen yksityisyyteen, perustuen lähteeseen [23]

| | 1a | 2a | 3a | 4a | 5a | Keskiarvo | SD |
|---|---|---|---|---|---|---|---|
| **Oppimisympäristö** | | | | | | | |
| Minulla oli hauskaa ratkaistaessa CTF-tehtäviä | 0 | 1 | 5 | 9 | 12 | 4,19 | 0,88 |
| CTF-tehtävät olivat nautittavia | 0 | 3 | 2 | 11 | 11 | 4,11 | 0,97 |
| CTF-tehtävät olivat nautittavia mukaansatempaava tapa oppia | 0 | 2 | 4 | 10 | 11 | 4,11 | 0,93 |
| **Oppimisen joustavuus** | | | | | | | |
| CTF antoi joustavuutta kurssin aiheiden oppimisessa | 0 | 3 | 6 | 13 | 5 | 3,74 | 0,9 |
| Pystyin oppimaan ja suorittamaan tehtävät omaan tahtiin | 0 | 2 | 3 | 6 | 16 | 4,33 | 0,96 |
| CTF:n avulla pystyin järjestämään opintoni kurssia varten paremmin | 2 | 3 | 7 | 6 | 9 | 3,63 | 1,28 |
| **Motivaatio** | | | | | | | |
| CTF-haasteet motivoi minua oppimaan kurssin aiheita | 0 | 1 | 7 | 8 | 11 | 4,07 | 0,92 |
| Motivaationi kurssin aiheisiin kasvoi, tehdessä tietosuoja haasteita | 0 | 3 | 2 | 10 | 12 | 4,15 | 0,99 |
| Motivaationi aiheiden oppimiseen kasvoi CTF-tehtävien ansiosta | 1 | 2 | 3 | 12 | 9 | 3,96 | 1,06 |
| **Tyytyväisyys** | | | | | | | |
| Kaiken kaikkiaan olen mielissäni CTF-haasteisiin | 0 | 2 | 1 | 14 | 10 | 4,19 | 0,83 |
| Kaiken kaikkiaan CTF-haasteet olivat miellyttäviä minulle | 0 | 1 | 5 | 13 | 8 | 4,04 | 0,92 |
| Kaiken kaikkiaan olen tyytyväinen CTF-tehtäviin | 0 | 1 | 5 | 14 | 7 | 4,00 | 0,78 |
| Kaiken kaikkiaan CTF-tehtävät vastaavat oppimistarpeitani | 1 | 3 | 6 | 12 | 5 | 3,63 | 1,04 |
| **Tehtävä-Teknologia-sopivuus** | | | | | | | |
| CTF-haasteissa käsiteltävät käsitteet | | | | | | | |
| ... vastaavat oppimistarpeitani | 0 | 2 | 4 | 15 | 6 | 3,93 | 0,83 |
| ... ovat yhteensopivia oppimistarpeideni kanssa | 0 | 0 | 5 | 17 | 5 | 4,00 | 0,62 |
| ... vastaavat kattavasti oppimistarpeitani | 0 | 2 | 11 | 10 | 4 | 3,59 | 0,84 |
| Oppimistavoitteeni ja -tarpeeni täyttyvät ratkaisemalla CTF-haasteita | 1 | 1 | 12 | 8 | 5 | 3,56 | 0,97 |

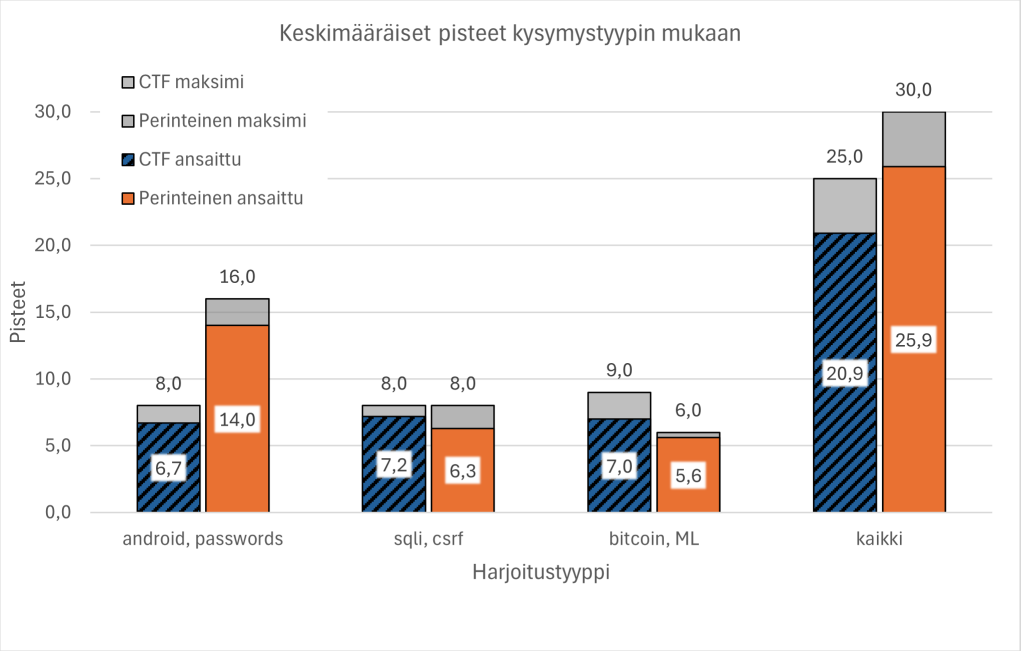
Keskimäärin tutkimuksissa havaittiin opiskelijoiden nauttivat CTF tehtävien teosta ja nämä nähtiin positiivisena muutoksena kurssien aikana. Opiskelijat kommentoivat tehtäviä sanomalla niiden mahdollistavat taitojen käyttämisen hauskoissa ja laatikon ulkopuolella olevissa tilanteissa [20]. Tutkimuksissa otettiin kantaa myös opettajien mielenkiintoon CTF tehtävien käytössä ja näissä keskimäärin opettajat

olivat hyvin tehtävien kannalla ja näkivät näiden olevat hyvä apuväline [12], [17], [21], [24].

## 3.2 Arvosanakehitys

Aiemmin todettuna CTF tehtävät antavat käytännön kokemusta opiskeluun ja tämän vaikutusta on tutkittu arvosanankehityksen kannalta. Tutkimusta on tehty vertaamalla samanlaisten kurssien opetusta ilman CTF pohjaista opetusta ja sitten CTF pohjaisella opetuksella, tai käyttäen tehtäviä opetuksen apuna.

Tutkimuksien pohjalta CTF tehtävien käyttäminen opetuksen apuna ei ainakaan heikentänyt opiskelijoiden koetuloksia ja osaamista. Tutkimuksessa Cole [18] havaittiin lähes samanlaisia koetuloksia riippumatta oliko kyseessä tavanomainen opetustapa tai CTF pohjainen. Pistekaavioon 3.1 on kuvattu tutkimuksesta [18] löytyvien harjoitusten pisteet.




Kuva 3.1: Keskimääräiset pisteet kurssin koetuloksista, jossa perinteiset tehtävät verrattuna CTF-tehtävä pisteisiin, perustuen lähteeseen [18]

Tutkimustietona toimi kokeen kysymysten pisteet, jotka on jaoteltu CTF-tyylisiin ja perinteistyylisiin tehtäviin. Kaavioon on kuvattu 3 eri tehtävää sekä kaikkien tehtävien yhteispisteet. Kaavion pohjalta nähdään, että kokonaispisteissä ei ole havaittavissa suurta eroa, CTF-tyylisissä pisteitä saatiin 84 % ja perinteistyylisissä saatiin 86 % kokonaispisteistä.

CTF-tehtävien korrelaatiota muihin kurssitehtäviin/aiheisiin on myös tutkittu. Vykopal et al. [24] Tutkimuksessa oli käytössä kaksi CTF-tehtävää kotitehtävinä eri aiheista. Näiden tehtävien pohjalta tehtiin mittausta, miten CTF-tehtävissä pärjääminen korreloitui muihin kurssin osa-alueisiin. Taulukkoon 3.4 on koottu korrelaatiokertoimia, joista vahvimmat ei-ilmeiset positiiviset korrelaatiot ovat merkitty vihreällä, sekä vahvin ei-ilmeinen negatiivinen korrelaatio on merkitty sinisellä. Taulukkoon on merkitty vain tilastollisesti merkittäviä ($p \leq 0,05$). Taulukossa käytetyt korrelaatiokertoimet ovat Spearmanin järjestyskorrelaatiokertoimia, joissa luku kertoo, kuinka vahvasti kaksi asiaa liittyvät toisiinsa ja mihin suuntaan. CTF tarkoittaa Taulukossa kahden CTF-tehtävän kokonaispisteitä, bonus kohta ottaa huomioon sekä kahdet CTF-tehtävät että näiden lisätehtävistä saatavat pisteet. Taulukon pohjalta nähdään vahva korrelaatio opiskelijoilla, jotka saivat paljon pisteitä CTF- ja bonustehtävistä, niin he pärjäsivät hyvin myös väliarvioinnissa ja tentissä. Tämän lisäksi Taulukosta näkee, kuinka opiskelijat, jotka tekivät paljon virheitä, eivät myöskään pärjänneet hyvin väliarvioinnissa.

Taulukko 3.4: CTF-tehtävissä mitatut korrelaatiot, perustuen lähteeseen [24]

| | CTF | Bonustehtävät | Väliarviointi | Tentti | Kaikki | Väärät liput |
|---|---|---|---|---|---|---|
| CTF | 1,00 | 0,63 | 0,35 | 0,31 | 0,31 | 0,11 |
| Bonus | | 1,00 | 0,50 | 0,49 | 0,50 | -0,15 |
| Väliarviointi | | | 1,00 | 0,89 | 0,92 | -0,47 |
| Tentti | | | | 1,00 | 0,99 | - |
| Kaikki | | | | | 1,00 | - |
| Väärät liput | | | | | | 1,00 |

Tutkimuksissa nähdyistä tuloksista voidaan todeta, että CTF-tehtävät eivät ainakaan heikentänyt arvosanoja opiskelijoilla. Tarkemmin Ellis et al. [4], Leune ja Petrilli [5], Schafeitel-Tähtinen ja Lazarov [12] ja Vykopal et al. [24] tutkimuksissa päädyttiin tulokseen, että arvosanoilla ja CTF-tehtävien tekemisellä nähtiin korrelaatiota. Vain Cole [18] tutkimuksessa nähtiin tilanne, että pisteet pysyivät samana CTF-tehtävän jälkeenkin. Vaikka kaikissa tilanteissa CTF-tehtävät eivät paranna arvosanoja, niin voidaan pohtia tämän jälkeen CTF-tehtävien tärkeyttä muista aihealueista. Kuten Alaluvussa 3.1 todettiin CTF-tehtävien parantavat opiskelijoiden motivaatiota. Opettamisessa ja oppimisessa ei kuitenkaan ole kyse pelkästään arvosanoista, vaan myös opiskelijoiden innostamisesta oppimiseen.

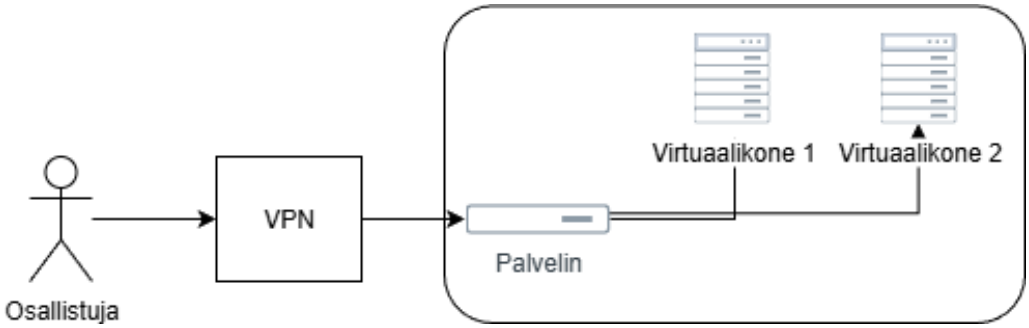
## 3.3 Toimintatavat

CTF-tehtäviä on mahdollista toteuttaa todella monella tavalla, sillä CTF toimii tehtäväpohjana, jota tehtävien suunnittelijat hyödyntävät haluamallaan keinolla. Monipuoliset toteutustavat tekevät CTF-tehtävistä jo valmiiksi modulaarisen ja toimivan keinon opiskeluun, sillä sitä saa muovattua tarkasti tarpeiden mukaan. Tehtävien tarkkailemiseen voidaan käyttää apuna joko kaupallisesti tuotettuja tai avoimen lähdekoodin palveluita, kuten TryHackMe[1], CTFd[2] tai FBCTF[3]. Kuvassa 3.2 on näytetty yksinkertainen esimerkki mahdollisesta CTF-infrastruktuurista, jossa osallistuja yhdistää VPN-yhteyden kautta palvelimeen, josta hänellä on pääsy virtuaalikoneisiin. Virtuaalikoneilla pyörii ohjelma/ohjelmisto, johon on jätetty tietty haavoittuvuus. Virtuaalikoneisiin yhteys muodostetaan yleensä verkkosivun kautta.

[1]Kaupallinen CTF-palvelu tryhackme.com

[2]Kaupallinen CTF-alusta ctfd.io

[3]Avoimen lähdekoodin CTF-alusta github.com/facebookarchive/fbctf




Kuva 3.2: CTF-infrastruktuuri, perustuen lähteeseen [19]

Kaupallisesti tuotetut tai avoimen lähdekoodin CTF-palvelut voidaan liittää osaksi Kuvan 3.2 mukaista infrastruktuuria, jolloin tehtävien edistystä voidaan nähdä paremmin. CTF-palvelut, kuten FBCTF tuovat mahdollisuuden lisätä pelillisyyttä tehtäviin, kuten tulostaulukon pisteille [5]. Näin erilaiset toimintavat ja pelillisyyden lisäys, pyrkii parantamaan myös CTF-osallistujien innostusta ja motivaatiota.

CTF-tehtävät voivat toimia hyvin monella tavalla apuna opetuksessa. Ne voivat olla oma aktiiviteetti, jota voidaan toteuttaa opiskelijoille esimerkiksi koulun kautta tai työelämässä. Ensimmäisenä toimintatapana on erillinen CTF-kilpailu suunniteltu opiskelijoille, jossa toteuttetaan kilpailun opiskelijoille. Ideana on yleensä olla lyhytaikainen kilpailu, jossa pääsee kurssien ulkopuolella testaamaan taitojaan käytännön harjoituksissa, kuten aineistossa [11]. Nämä kilpailut etenenevät aiemmin Luvussa 2 kerrotulla tavalla.

Toinen aineistoissa esille tullut toimintatapa oli liittää CTF-tehtävät jollain tyylillä osaksi kurssia. Tällä tavoin korvataan normaalit kurssitehtävät CTF-tyylisillä tehtävillä, jolla pyritään aiemmin mainittuun motivaation lisäämiseen ja pelillisyyden tuomiseen tehtävissä. Näin voidaan myös jakaa kurssin aikana olevia asioita viikottaisiin tehtäväpaketteihin kuten aineistossa [4]. Pitkät CTF-tehtävät voivat kuitenkin aiheuttaa omanlaisia ongelmatilanteita [24], näistä kerrotaan lisää seuraavassa aliluvussa.

CTF-tehtäviin ei voida suoraan määrittää oikeaa toimintatapaa, sillä samanlainen opetustapa ei toimi kaikissa tilanteissa. Kuitenkin yleinen laitteistoinfrastruktuuri ja päällimmäinen järjestelmän toimivuudet ovat samanlaiset, joita on kuvattu tässä luvussa.

## 3.4 Ongelmatilanteet ja kehitysehdotukset

CTF-tehtävät ja pelillistäminen tarjoavat monia hyötyjä, kuten tutkielmassa aiemmin todetut hyödyt opiskelijoiden motivaatiossa, käytännön oppimisessa ja arvosanojen mahdollisessa paranemisessa, toteutukseen liittyy myös haasteita. Tutkimuksissa on havaittu sekä teknisiä että mahdollisesti pedagogisia ongelmatilanteita. Tässä luvussa käsitellään näitä ongelmatilanteita ja näihin esitettyjä kehitysehdotuksia, joita aineistoista on tullut esiin.

Aineistoissa esille tullut aihealue oli opiskelijoiden osaamisen varmistaminen. Sillä toisissa tutkimuksissa CTF-tehtävät toteutettiin ryhmätyönä, jolloin piti löytää tapa varmistaa kaikkien osaaminen, tämä tehtiin tentin avulla [21]. Tämän lisäksi esille tullut aihe oli CTF-tehtävien lippujen jakaminen. Tätä tutkittiin vertaamalla lippujen palautusaikoja ja katsomalla kuinka usein opiskelijat palauttivat lähes samaanaikaan liput. Otettiin huomioon myös mahdottomassa ajassa ratkaistut tehtävät, jossa oli laskettu minimiratkaisuaika tehtäville ja lippuja oli palautettu tämän ajan alapuolelle. [24]

Pelillisyys aiheuttaa myös mahdollisia ongelmatilanteita CTF-tehtäväpohjaisessa ratkaisussa, sillä tehtävillä on tarkoitus luoda motivoivia ja hyviä opetustilanteita. Pelillisyyden myötä opiskelijoille tuodaan mukaan kilpailullisuusnäkökulma tehtävien ratkaisuun, jolloin opiskelijoiden keskittyminen ei ole enää pelkästään oppimisessa vaan myös toisten opiskelijoiden voittamisessa [20]. Pelillisyyttä ei kuitenkaan haluta kokonaan pois, koska kuten tutkielmassa on aiemmin todettu pelillisyydellä pyritään parantamaan motivaatiota. Tärkeää on siis pelillisyyden ja opiskelijoiden

oppimisen tasapainotus, jolloin pelillisyys ei saa yliajaa opiskelijoiden keskittymistä aiheen syvälliseen oppimiseen.

Gleeson [20] tutkimuksessa puhutaan myös vähän yllättävästä ongelmasta, joka johtuu CTF-tehtävien teknisyydestä. Vaikka aihealueiden teorian osaisi hyvin, niin CTF-tyylinen käytännön tehtävien ratkaisumalli voi olla vaikea oppia. Tällöin henkilöt, joilla ei ole tietämystä aiemmista käytännön taidoista, saattavat haluta pärjätä hyvin kilpailullisen näkökulman kautta, jolloin aiheen oppiminen voi jäädä vähemmälle. Toisaalta henkilöt joilla on jo alkujaan CTF-tehtävistä kokemusta, voivat nähdä tehtävät tylsinä.

## 3.5 Luvun yhteenveto

Luvun 3 tarkoitus oli tarkastella teemoja aineistoista olevista aiheista, jotka liittyivät CTF-tehtävien hyödyntämiseen kyberturvan opettamisessa ja oppimisessa. Käsitellyt aihealueet olivat motivaatio, CTF-myönteisyys, arvosanakehitys, toimintavat sekä ongelmatilanteet ja kehitysehdotukset. Näitä aihealueita käsiteltiin aineistoissa tehdyillä tutkimuksilla.

Aineistojen perusteella nähtiin CTF-tehtävien lisäävän opiskelijoiden motivaatiota, tämä näkyi kurssipalautteissa, joita opiskelijoilta kysyttiin. Tämän lisäksi palautteissa nähtiin positiivisia palautteita CTF-järjestelystä. Arvosanakehityksen tuloksissa ei nähty CTF-tehtävien heikentävän tuloksia ja tietyissä tapauksissa nähtiin niiden korreloivan positiivisesti kurssin muiden tehtävien ja suoritusten kanssa.

Luvulla pyrittiin näyttämään CTF-tehtävien potentiaali opetusvälineenä kyberturvassa. CTF-tehtävillä pystytään parantamaan opiskelijoiden motivaatiota ja opetuskokemusta sekä mahdollistetaan teorian yhdistäminen käytännön esimerkkeihin oikeasta elämästä, jolla syvennetään oppimista. Kuitenkin CTF-tehtävämalli vaatii suunnittelua ja oikeanlaista toteutusta, jotta sen potentiaalista saadaan kaikki irti. Seuraavassa luvussa käydään läpi pohdintaa, millä tavoin CTF-tehtävämalli voisi

hyödyntää osana kyberturvaopettamista jatkossa. Sekä pohditaan tuloksia ja niiden merkityksiä, mitä tässä luvussa tuli esille.

# 4 Pohdinta

Luvun tarkoituksena on pohtia tarkemmin tutkimuksessa esille tulleita tuloksia ka esitää tulkintoja mitä merkitystä tuloksilla on. Luvussa pohditaan näitä asioita kirjallisuuskatsauksen pohjalta. Tutkimuksen pohjalta keskeisin tulos oli CTF-tehtävien positiivinen vaikutus opiskelijoiden motivaatioon ja oppimismieltymykseen. Oppimisen kannalta voidaan todeta, että motivaatio on juuri tärkeä osa, sillä se innostaa oppimaan lisää ja pysymään aiheen parissa.

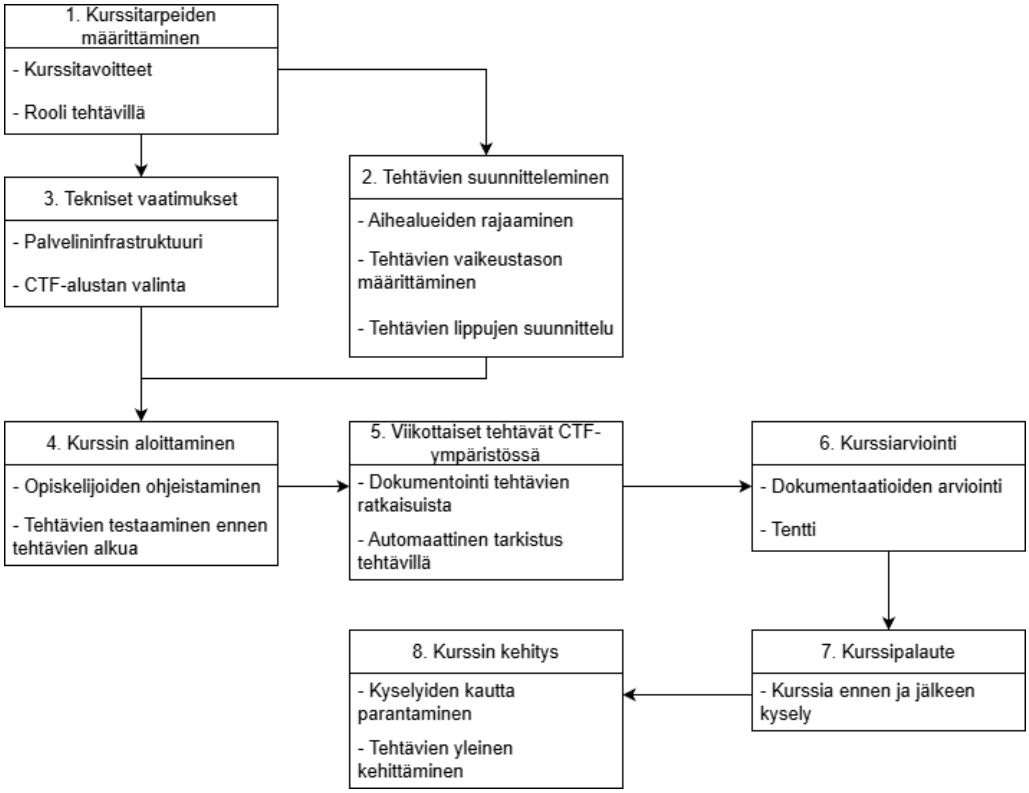
Tutkimuksen tulos on yhdenmukainen muiden tutkimusten kanssa, kuten Schafeitel-Tähtinen ja Lazarov [12], Cole [18] ja Vigl ja Abramova [23]. CTF-tehtävien nähtiin olevan opiskelijoille motivoivia ja mielenkiintoisia. Kuitenkin on todettava eroavaisuuksia kirjallisuudessa, jotka liittyivät varsinkin arvosanakehitykseen. Cole [18] tutkimuksessa todettiin, että CTF-pohjainen opetustapa ei parantanut opiskelijoiden arvosanoja, mutta Vykopal et al. [24] nähtiin positiivista korrelaatiota CTF-tehtävillä ja arvosanakehityksellä. Tämän perusteella voidaan arvioida, että CTF-tehtävien vaikutus opiskelijoihin ei ole aina samanlainen, tähän vaikuttaa opetuksen yleinen rakenne, arviointi- ja toimintatavat.

Kirjallisuuden pohjalta voidaan perusteellisesti sanoa, että CTF-tehtävät antavat mahdollisuuden käytännön kokemukseen teorian lisäksi, joka selittää motivaation ja oppimisinnon kasvua. Tehtävät antavat mahdollisuuden opiskelijoiden soveltaa oppimistaan käytännön tehtävissä, joista he voivat saada välitöntä palautetta. Tällöin opiskelija syventää oppimistaan aiheeseen, eikä osaaminen jää vain teorian

puolelle. Tulkintaa tukee esimerkiksi Egamberganova et al. [3], Schafeitel-Tähtinen ja Lazarov [12], Hamad et al. [21] ja Vigl ja Abramova [23], joissa nähtiin opiskelijoiden kasvava into ja motivaatio kyberturvaan liittyen, koska CTF-pohjainen opetus tarjosi teoreettisista aiheista käytännön tehtäviä.

Kirjallisuuskatsauksessa ilmi tulleita tuloksia on mitattu itsearvioinneilla, jolloin tuloksia pitää arvioida kriittisesti. Itsearvioinneissa henkilöt voivat merkitä taitonsa tai osaamisensa paremmalle tasolle, kuin ne todellisuudessa ovat. Tämän lisäksi pitää ottaa huomioon tutkimuksissa käytetyt otantakoot, kuten Schafeitel-Tähtinen ja Lazarov [12] N=40 ja Vykopal et al. [24] N=25. Kuitenkin tutkimuksen tulokset ovat kirjallisuuden valossa samanlaisia ja johdonmukaisia, joka vahvistaa sitä, että tulokset ja muutokset oppimisessa ja motivaatiossa eivät ole satunnaisia.

Käytännön tilannetta ja viakutuksia kuvaamaan on luotu prosessikaavio. Seuraavalla sivulla Kuvassa 4.1 on esitettynä CTF-mallin prosessikaavio, jolla havainnollistetaan miten kurssi, jossa hyödynnetään CTF-mallia etenisi. Kurssin suunnittelu alkaa tarpeiden määrittämisellä, jolla luodaan pohjaa mitä kurssilla pitää saada aikaan. Tästä lähdetään luomaan sekä teknisiä vaatimuksia että suunnittelemaan tarkemmin tehtäviä CTF-malliin liittyen. Kurssin alkaessa käydään läpi opiskelijoille miten CTF-tehtävätyyli toimii ja mahdollisesti voi olla introtehtävä. Tämä toimii samalla testinä, että järjestelmä toimii. Mallissa CTF-tehtävät toimivat kurssin aihealueiden oppimisen tukena viikottaisina haasteina, joista luodaan dokumentaatiota lisäksi miten tehtävä ratkaistiin. Tällä dokumentaatiolla pyritään estämään lippujen kopiointi kaverilta. Tämän lisäksi automaattinen tarkistus antaa heti palautteen oliko lippu oikea. Kurssiarviointiin otetaan huomioon sekä CTF-tehtävät mukaanlukien niiden dokumentointi ja tentti. Tentillä varmistetaan opiskelijoiden aiheen oppiminen. Kurssia voidaan kehittää kurssipalautteella ja myös mitata CTF-tehtävien toimimista samalla kyselyllä ennen ja jälkeen kurssin.




Kuva 4.1: Prosessikaavio CTF-pohjaisesta kurssista

Prosessikaaviolla pyritään osoittamaan, että CTF-malli ei ole pelkästään CTF-tehtäväosuus vaan kokonaisuus kurssin osana. Kaaviolla pyritään havainnollistamaan tutkimuksen tuloksia, osoittamalla kuinka kurssin suunnittelu ja kehitys tarjoavat hyvät mahdollisuudet kehittää CTF-pohjaista opetusta ja luoda motivoivaa ja kehittävää ympäristöä opiskelijoille. Kurssipalaute toimii mahdollisuutena muuttaa toimintatapaa mikäli kurssin alussa mietitty toimintamalli ei sovellukkaan parhaiten opiskelijoille. Toiseksi prosessikaaviolla pyritään osoittamaan, että CTF-mallin sisällytyksen kurssirakenteeseen ei tarvitse korvata perinteisiä arviointitapoja. Muutenkaan kurssirakenne ei muutu vaan CTF otetaan osaksi normaalia kurssirakennetta.

Voidaan todeta pohdinnan tulokseksi, että CTF-tehtävämallilla on positiivinen vaikutus opiskelijoiden motivaation sekä oppimisinnossa. Kirjallisuudessa esiintyy eroavaisuuksia arvosanavaikutuksessa, mutta motivaation kasvuun liittyvät tulok-

set ovat yhdenmukaisia kirjallisuudessa. Näiden asioiden valossa voidaan kokonaisuutena päätellä, että yhdistämällä prosessikaavion pohdinnan ja muun pohdinnan voidaan luoda kokonaisuus, jossa mahdollistetaan opiskelijoiden motivaation kasvu luomalla käytännönläheistä opetusta CTF-pohjaisella mallilla. Malli antaa mahdollisuuden syventävälle oppimiselle, jolloin saadaan tärkeä teorian sekä käytännönoppimisen yhdistelmä.

# 5 Yhteenveto

Tämä tutkielma käsitteli CTF-tehtävien käyttöä kyberturvan käytännöntaitojen kehittämisessä, erityisesti millainen vaikutus niillä on opiskelijoiden motivaatioon, oppimiseen sekä arvosanoihin, lisäksi tutkittiin mahdollisia ongelmatilanteita ja haasteita opetusmetodiin liittyen. Tutkielmassa vastattiin tutkimuskysymyksiin käyttämällä aineistoissa löytyviä tutkimuksia sekä oman pohdinnan myötä.

TK 1. *Miten CTF-tehtävät vaikuttavat motivaatioon kyberturvan oppimisessa?* Aineistojen perusteella nähtiin CTF-tehtävien positiivisesti vaikuttavan opiskelijoiden motivaatioon. Tutkimustuloksista korostui CTF-tehtävien käytännön kokemuksen antama hyöty ja tämän nähtiin motivoivan opiskelijoita yhä paremmin. Tämän lisäksi nähtiin tutkimuksissa positiivisia korrelaatioita arvosanakehityksen ja CTF-tehtävämallin kanssa. Työssä mainittiin myös pelillistämisen mahdollinen hyöty opiskelijoiden motivaation lisäämisessä.

TK 2. *Millaisia toimintatapoja voidaan hyödyntää CTF-pohjaisessa opetuksessa?* Tutkimuksessa esitettiin useita erilaisia toimintatapoja, joilla CTF-pohjaista opetusta voidaan luoda. CTF-tehtävät voivat toimia erillisinä kilpailuina, joissa lyhyessä ajassa opiskelijat ratkaisevat ongelmia. CTF-tehtävät voivat toimia myös osana kurssia lisäämällä käytännön kokemuksen teorian oppimisen lisäksi, tässä tavassa CTF-tehtävät voivat toimia viikkotehtävinä tai muuten laajempina kokonaisuuksina. Tutkimuksessa otettiin kantaa myös CTF-tehtäviin vaadittavaan infrastuktuuriin ja esitettiin mahdollisia vaihtoehtoja. Vaihtoehtoina toimivat järjestäjän oma palve-

lin toiminnallisuus tai erikseen kaupallisesti tai avoimen lähdekoodin kautta pyörivä CTF-palvelu. Pohdinnassa esitettiin mahdollinen prosessimalli, jossa CTF-tehtävät toimisivat osana kurssia ja esitettiin mitä vaiheita tälläisen kurssin suunnitteluun ja toteutukseen voisi liittyä.

TK 3. *Mitä ongelmatilanteita ja vaikeuksia voi ilmetä CTF-pohjaisessa opetuksessa?* CTF-pohjainen opetusmalli antaa suurimmaksi osaksi positiivisia viitteitä opetukseen liittyen, mutta työssä otettiin kantaa myös tämän ongelmakohtiin. Suurimmiksi ongelmakohdiksi ilmeni tehtävien tekninen puoli, joka saattaa aiheuttaa ongelmatilanteita, sekä pelillistämisen mahdolliset huonot puolet. Työssä todettiin, että CTF-pohjaiset tehtävät voivat olla haastavia henkilöille, joilla ei ole CTF-taustaa ja tämä aiheuttaisi epätasaisuutta kurssin suorituksen kannalta niillä joilla kokemusta löytyy. Pelillisyyden tuominen taas voisi aiheuttaa oppimisen painottamisen vähentämistä ja korvaisi tämän kilpailulla, jossa on tärkeämpää pärjätä paremmin kuin toinen, kun oppia aihetta syvällisesti. Lisäksi CTF-ympäristö vaatii paljon valmistelua ja on heikko esimerkiksi lippujen jakamiseen liittyvissä ongelmissa.

Tutkimukselle on mahdollista luoda jatkotutkimusta. Tässä tutkimuksessa käytetyt kirjallisuudet käyttivät CTF-tehtävien toiminnan arvioimiseen suurimmaksi osaksi itsearviointeja, sekä mittaus tapahtui lyhyen aikavälin aikana eli yhden kurssin aikana. Lisätutkimuksissa voitaisiin arviointiin luoda objektiivisempia tapoja sekä mittausta voitaisiin tehdä monen kurssin tai opintojakson aikana. Nämä antaisivat paremmat mahdollisuudet arvioida CTF-mallin vaikutuksia opiskelijoihin. Tämän lisäksi tutkimusta voisi tehdä tarkemmin pelillisyyden vaikutuksiin CTF-mallissa. Pelillisyyden positiivisia vaikutuksia on tutkittu paljon, mutta aineistotutkimuksessa näkyi vähemmän tutkimuksia, joissa yhdistyi pelillisyys sekä CTF-malli. Näin voitaisiin nähdä miten kilpailullisuus ja pelimekaanikat vaikuttavat opiskelijoihin.

Yhteenvetona voidaan todeta, että CTF-tehtävillä on hyöty ja merkitys kyberturvan käytännöntaitojen kehittämisessä. Aineistot osoittivat, että CTF-pohjainen

toteutus kasvatti opiskelijoiden motivaatiota, koska se antoi mahdollisuuden käytännönläheiseen tekemiseen. Erilaiset toimintatavat mahdollistivat toimintamallin mukautuvuuden erilaisiin käyttötarkoituksiin, kuten prosessikaavion esittämä tapa liittää CTF-malli osaksi kurssikokonaisuutta. CTF-tehtävien tarkoitus ei ole korvata kyberturva opetusta, vaan ne muodostavat kokonaisuuden yhdessä perinteisen opetuksen kanssa.

# Lähdeluettelo


[1] Microsoft, *Microsoft Digital Defense Report 2024*. viitattu 12. lokakuuta 2025. url: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024.

[2] ENISA, *ENISA Threat Landscape 2024 | ENISA*, lokakuu 2025. viitattu 12. lokakuuta 2025. url: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[3] A. Egamberganova, U. Abdalov, S. Latipova, S. Ataev, D. Ismatova ja N. Ubaydullayeva, "Teaching Cybersecurity with CTF: New Pedagogical Methods and Strategies", teoksessa *2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM)*, ISSN: 2325-419X, kesäkuu 2025, s. 2170–2175. DOI: 10.1109/EDM65517.2025.11096633.

[4] M. Ellis, L. Baum, K. Filer ja S. H. Edwards, "Experience Report: Exploring the Use of CTF-based Co-Curricular Instruction to Increase Student Comfort and Success in Computing", teoksessa *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*, sarja ITiCSE '21, New York, NY, USA: Association for Computing Machinery, 2021, s. 303–309, ISBN: 978-1-4503-8214-4. DOI: 10.1145/3430665.3456376.

[5] K. Leune ja S. J. Petrilli, "Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education", teoksessa *Proceedings of the 18th Annual Conference on Information Technology Education*, sarja SIGITE '17, New

York, NY, USA: Association for Computing Machinery, 2017, s. 47–52, ISBN: 978-1-4503-5100-3. DOI: 10.1145/3125659.3125686.

[6] F-Secure, *Vulnerability Reward Program | F-Secure*. viitattu 12. lokakuuta 2025. url: https://www.f-secure.com/en/vulnerability-reward-program.

[7] TryHackMe, *Learn Cyber Security | TryHackMe Cyber Training*. viitattu 12. lokakuuta 2025. url: https://tryhackme.com/.

[8] A. Erola, L. Axon, A. Janse van Rensburg, I. Agrafiotis, M. Goldsmith ja S. Creese, "Control Effectiveness: a Capture-the-Flag Study", teoksessa *Proceedings of the 16th International Conference on Availability, Reliability and Security*, sarja ARES '21, New York, NY, USA: Association for Computing Machinery, 2021, s. 1–10, ISBN: 978-1-4503-9051-4. DOI: 10.1145/3465481.3470095.

[9] V. Ford, A. Siraj, A. Haynes ja E. Brown, "Capture the Flag Unplugged: an Offline Cyber Competition", teoksessa *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, sarja SIGCSE '17, New York, NY, USA: Association for Computing Machinery, 2017, s. 225–230, ISBN: 978-1-4503-4698-6. DOI: 10.1145/3017680.3017783.

[10] W. Noonpakdee, "Developing a Cybersecurity Curriculum Using Best Practices and Student Awareness Insights", teoksessa *2025 16th International Conference on E-Education, E-Business, E-Management and E-Learning (IC4e)*, huhtikuu 2025, s. 578–582. DOI: 10.1109/IC4e65071.2025.11075416.

[11] S. Abaimov et al., "Capture The Industrial Flag: Lessons from hosting an ICS cybersecurity exercise", teoksessa *Proceedings of the 10th ACM Cyber-Physical System Security Workshop*, sarja CPSS '24, New York, NY, USA:

Association for Computing Machinery, 2024, s. 98–106, ISBN: 979-8-4007-0420-8. DOI: 10.1145/3626205.3659148.

[12] T. Schafeitel-Tähtinen ja W. Lazarov, "Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia", *Computer Applications in Engineering Education*, vol. 33, nro 5, e70082, 2025, ISSN: 1099-0542. DOI: 10.1002/cae.70082.

[13] M. Malone, Y. Wang, K. James, M. Anderegg, J. Werner ja F. Monrose, "To Gamify or Not? On Leaderboard Effects, Student Engagement and Learning Outcomes in a Cybersecurity Intervention", teoksessa *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, sarja SIGCSE '21, New York, NY, USA: Association for Computing Machinery, 2021, s. 1135–1141, ISBN: 978-1-4503-8062-1. DOI: 10.1145/3408877.3432544.

[14] M. Sailer ja L. Homner, "The Gamification of Learning: a Meta-analysis", *Educational Psychology Review*, vol. 32, nro 1, s. 77–112, maaliskuu 2020, ISSN: 1573-336X. DOI: 10.1007/s10648-019-09498-w.

[15] R. Singh, "Software Security (Capture the Flag)", teoksessa *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, heinäkuu 2021, s. 165–168. DOI: 10.1109/CCICT53244.2021.00041.

[16] I. Ryan, U. Roedig ja K.-J. Stol, "Training Developers to Code Securely: Theory and Practice", teoksessa *Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability*, sarja EnCyCriS/SVM '24, New York, NY, USA: Association for Computing Machinery, 2024, s. 37–44, ISBN: 979-8-4007-0565-6. DOI: 10.1145/3643662.3643956.

[17] C. Chhetri, ""It was a one of a kind experience:"Student Experiences and Pedagogical Design of a Project-based Hands-on Cybersecurity Pen-testing Course", teoksessa *Proceedings of the 24th Annual Conference on Information Technology Education*, sarja SIGITE '23, New York, NY, USA: Association for Computing Machinery, 2023, s. 22–27, ISBN: 979-8-4007-0130-6. DOI: 10.1145/3585059.3611402.

[18] S. V. Cole, "Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class", teoksessa *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*, sarja ITiCSE '22, New York, NY, USA: Association for Computing Machinery, 2022, s. 470–476, ISBN: 978-1-4503-9201-3. DOI: 10.1145/3502718.3524806.

[19] R. Deaconescu, A. Baltoiu, T. Georgescu ja A. Puncioiu, "Using Cybersecurity Exercises as Essential Learning Tools in Universities", teoksessa *International Conference on Computer Supported Education, CSEDU - Proceedings*, Journal Abbreviation: International Conference on Computer Supported Education, CSEDU - Proceedings, vol. 2, Science ja Technology Publications, Lda, 2022, s. 434–441, ISBN: 978-989-758-562-3. DOI: 10.5220/0010994700003182.

[20] M. Gleeson, "Cybersecurity Students Experiences of Capture the Flag (CtF) in an Irish Technological University", teoksessa *2024 Cyber Research Conference - Ireland (Cyber-RCI)*, marraskuu 2024, s. 1–9. DOI: 10.1109/Cyber-RCI60769.2024.10939974.

[21] M. Hamad, A. Finkenzeller, M. Hasan, M.-O. Pahl ja S. Steinhorst, "A Gamified Learning Approach for IoT Security Education Using Capture-the-Flag Competitions: Architecture and Insights", teoksessa *Secure IT Systems*, L. Horn Iwaya, L. Kamm, L. Martucci ja T. Pulls, toim., Cham: Springer Nature

Switzerland, 2025, s. 161–175, ISBN: 978-3-031-79007-2. DOI: 10.1007/978-3-031-79007-2_9.

[22] L. Tobarra et al., "Game-based Learning Approach to Cybersecurity", teoksessa *2020 IEEE Global Engineering Education Conference (EDUCON)*, ISSN: 2165-9567, huhtikuu 2020, s. 1125–1132. DOI: 10.1109/EDUCON45650.2020.9125202.

[23] W. Vigl ja S. Abramova, "Design and Use of Privacy Capture-the-Flag Challenges in an Introductory Class on Information Privacy and Security", teoksessa *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1*, sarja ITiCSE 2024, New York, NY, USA: Association for Computing Machinery, 2024, s. 618–624, ISBN: 979-8-4007-0600-4. DOI: 10.1145/3649217.3653572.

[24] J. Vykopal, V. Švábenský ja E.-C. Chang, "Benefits and Pitfalls of Using Capture the Flag Games in University Courses", teoksessa *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, sarja SIGCSE '20, New York, NY, USA: Association for Computing Machinery, 2020, s. 752–758, ISBN: 978-1-4503-6793-6. DOI: 10.1145/3328778.3366893.