Anton Havukainen

Kaakkois-Suomen ammattikorkeakoulun tunkeutumisreittianalyysi

Opinnäytetyö

Tieto- ja viestintätekniikan koulutus

Kyberturvallisuus

2022

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Anton Havukainen
Työn nimi	Kaakkois-Suomen ammattikorkeakoulun tunkeutumisreittianalyysi
Toimeksiantaja	Kaakkois-Suomen ammattikorkeakoulu
Vuosi	2022
Sivut	37 sivua
Työn ohjaaja(t)	Marko Oras

TIIVISTELMÄ

Nykypäivänä tietoturvallisuudesta on tullut huomiota herättävä aihe, varsinkin yrityksiin ja hallituksiin keskittyvien kyberhyökkäyksien takia ja siksi monet niistä ovat alkaneet ottaa huomioon omien tietojensa turvassa pidon internetissä. Siitä huolimatta arkaluonteisen tiedon menetys on mahdollista, jos hyökkääjä voi saada tiedot toisin tavoin ilman internetiä. Tämän takia fyysistä osaa tietoturvasta ei pidä laiminlyödä, vaan sitä pitää kohdella yhtä tärkeänä osana suurta kokonaisuutta.

Opinnäytetyön tavoitteena on tutkia Kaakkois-Suomen ammattikorkeakoulun Kotkan kampuksen Tieto- ja viestintätekniikan alojen oppimisympäristön heikkouksia fyysisen tietoturvallisuuden näkökulmasta. Tutkimus perustuu TUREAN-tunkeutumisreittianalyysimallin käyttöön sekä fyysisen tietoturvan yleiseen teoriaan. Tutkimuksessa on myös käytännön osuus, jossa oppimisympäristöstä etsitään kaikki mahdolliset sisäänkäyntireitit ja tulkitaan, kuinka kauan niiden läpimenossa kuluu aikaa. Lisäksi tutkimuksessa käytetään Exceliin perustuvaa laskentataulukkoa analysoimaan murtoyrityksiin liittyvien hidasteiden aikoja ja niiden aiheuttamat tunkeilijan havainnoinnin todennäköisyydet. Laskentataulukon avulla voidaan tulkita, pystyykö tunkeilija onnistuneesti murtautua kampukseen ja paeta, ennen kun vastevoimat pystyvät pysäyttää hänet.

Opinnäytetyön tutkimuskysymyksiin pystyttiin vastaamaan ja niiden kautta saaduista tuloksista voidaan hyötyä tulevaisuudessa kriittisten järjestelmien ja arkaluonteisten tietojen suojelussa. Niiden avulla voidaan paremmin ymmärtää, miten fyysinen ympäristö voi olla heikko murtautumisyrityksiä kohtaan. Tutkimus hyötyisi kuitenkin jatkotutkimuksesta, jossa pystyttäisiin tutkimaan laajemmin murtoyrityksissä tapahtuvien ovien, ikkunoiden ja seinien läpimurtoihin tarvittavat ajat.

Asiasanat: Fyysinen tietoturva, murtautuminen, tunkeutumisreitti

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author (authors)	Anton Havukainen
Thesis title	Intrusion route analysis for South-Eastern Finland University of Applied Sciences
Commissioned by	South-Eastern Finland University of Applied Sciences
Time	2022
Pages	37 pages
Supervisor	Marko Oras

ABSTRACT

Today, information security has become an eye-catching topic, especially due to cyberattacks focused on businesses and governments. Therefore many of them have begun to take their own data security on the internet into account. Nevertheless, the loss of sensitive information is still possible if the attacker can obtain the information some other ways without the internet. For this reason, the physical part of information security should not be neglected but treated as an equally important part of a larger entity.

The objective of this thesis was to study weaknesses in the learning environment in the ICT fields of Kotka campus of South-Eastern Finland University of Applied Sciences from the point of view of physical information security. The study is based on the use of TUREAN intrusion route analysis model, as well as the general theory of physical security. In the practical part of the study in which all possible entrance routes that are found in the learning environment are interpreted for how long it takes to pass through them. In addition, the study uses an Excel-based spreadsheet to analyze the times of the slowdowns associated with attempted break-ins and the resulting probabilities of intruder detection. The spreadsheet can interpret if an intruder is able to successfully break into the campus and escape before the response forces are able to stop them.

The study managed to find answers to the research questions, and the results obtained (through them) can be used in the future to protect critical systems and sensitive data. They help to better understand weaknesses of the physical environment can be weak towards attempted break-ins. The study would benefit from more extensive further research, on times needed for breakthroughs in doors, windows and walls during break-ins.

Keywords: Physical information security, breaking and entering, Intrusion route

SISÄLLYS

1 JOHDANTO

Kyberturvallisuudessa omien järjestelmien ja tietojen suojaaminen mahdollisilta haitantekijöiltä on noussut yhä tärkeämmäksi vuosien kuluessa. Juuri tällä hetkellä vuonna 2022 Euroopassa oleva kriisi on aiheuttanut sen, että turvallisuus, mukaan lukien tietoturvallisuus, on entistäkin tärkeämpää. Nykypäivän uhkat vaarantavat paitsi valtioiden toimintaa myös ihmisten henkilökohtaisia tietoja, ja mahdollisia haitantekijöitä voi tulla monella eri tavalla, eikä aina pelkästään internetin kautta.

Kyberturvallisuudessa omien laitteiden suojaaminen fyysisiltä uhkilta tulisi olla yhtä tärkeää kuin internetin kautta tulevilta ulkopuolisilta haitantekijöiltä. Oikeilla työkaluilla ja suunnittelulla kuka tahansa pystyy halutessaan aiheuttamaan yhtä paljon vahinkoa tietoverkkoon paikan päällä kuin verkon kautta haittaohjelmalla. Tämän takia laitosten ja yritysten kannattaisikin sijoittaa aikaa omien oppimisympäristöjen tutkimiseen ja suojaamiseen mahdollisilta heikkouksilta. Niiden löytäminen ja korjaaminen oikeilla turvajärjestelmillä ja turvatoimeenpiteillä on paras tapa torjua mahdollisia tulevaisuuden fyysisiä uhkia, kuten murtautumisia.

Fyysisellä tietoturvalla tarkoitetaan esimerkiksi laitteiden, tietojen, aineistojen ja toimitilojen suojaamista erilaisilta fyysisiltä uhkilta. Näitä uhkia voivat aiheuttaa sekä olosuhteet, kuten tulipalot, sähkökatkokset ja tulvat että ihmiset oman toimintansa kautta joko tahallisesti tai tahattomasti. Näitä voi tapahtua esimerkiksi varkauden, ilkivallan takia tahallisesti tai huolimattomuuden takia tahattomasti. Yrityksillä ja yksityisillä henkilöillä pitäisikin olla oikeanlaiset suojauskeinot käytössään turvaamassa molemmilta uhkatyypiltä. Periaatteessa oppimisympäristön fyysisen suojaamisen pitäisi olla ennaltaehkäisevää näille mahdollisille olosuhteista johtuville uhkille ja toimia pelotteena murtautujille. Täten fyysisen tietoturvan konsepti on estää laitteiden ja tiedonmenetys ennen kuin ne tapahtuvat. (Seclion Oy 2021.)

Opinnäytetyön inspiraatio tuli Marko Oraksen kurssilta, jossa käytettiin yhdessä tehtävässä Jere Peltosen kehittämää TUREAN-Tunkeutumisreitti-analyysia, joka on matemaattinen malli, jolla voidaan laskea tunkeutumisen epäonnistumisen todennäköisyyttä Excel-laskentakaavioilla. Kurssin

tehtävässä käytettiin esimerkkinä Kaakkois-Suomen ammattikorkeakoulun (Xamk) Tieto- ja viestintätekniikan oppimisympäristöä Kotkassa sijaitsevalla kampuksella. Siinä opiskelijat tutkivat ryhmissä mahdollisia sisäänpääsyreittejä, joihin liittyvät hidasteajat arvioitiin ja murtautumisen onnistuminen ilman havaituksi tulemista laskettiin tämän työkalun avulla. Työni on tapaustutkimus, jonka suunnitelmana on TUREAN-menetelmän käyttö, jotta saadaan konkretisoitunut analyysi oppimisympäristöön kuuluvista sisäänkäyntireiteistä, hidasteajoista ja onnistuneimmista murtautumisyrityksistä. Tämän kautta voidaan suojata nykyinen oppimisympäristö ja samaa menetelmää voidaan käyttää uusissa ympäristöissä ja estää tulevia vaaroja.

Kaakkois-Suomen ammattikorkeakoulu Xamk on toiminut vuodesta 2017 asti korkea-asteen koulutuksen laitoksena ja toimi myös tämän opinnäytetyön toimeksiantajana. Xamk tulee myös olevaan ainoa taho, joka tulee hyötymään tästä työstä suoranaisesti.

1.1 Opinnäytetyön aihe

Tämän opinnäytetyön aiheena on Kaakkois-Suomen ammattikorkeakoulun Kotkan kampuksen ulkopuolisen ja sisäisen fyysisen turvallisuuden analysointi. Tutkimukseen kuuluu siis fyysisen ympäristön tutkiminen sekä paikan päällä että konseptina, testien toteuttaminen ja niiden kautta laskenta ja lopputulosten päättely. Kampus tullaan korvaamaan vuonna 2024, mikä antaa mahdollisuuden tutkia vanhan kampuksen arkkitehtuuria ja tilojen suunnittelun heikkouksia fyysisen turvallisuuden kannalta. Näitä löytöjä voidaan sitten mahdollisesti käyttää uuden kampuksen suunnittelussa samojen virheiden välttämiseksi.

Teoriaosuudessa perehdytään tarkemmin TUREAN-tunkeutumisreittianalyysityökaluun, jonka antamia tuloksia tullaan käyttämään tutkimuksessa käytännön puolelta runkona. Teoriassa myös analysoidaan oppimisympäristöä laajemmin SketchUp-arkkitehtuurisuunnitteluohjelmiston avulla. Kyseisellä ohjelmistolla luodaan malli oppimisympäristöstä ja malli toimii hyödyllisenä työkaluna oppimisympäristön fyysisen kokonaisuuden kuvalliseen muodostamiseen.

1.2 Opinnäytetyön tavoitteet ja kysymys

Tämän opinnäytetyön tavoitteena on tutkia yrityksiin kohdistuvien murtoyrityksien havainnointiin liittyvää todennäköisyyttä. Tutkimuksen tuloksilla on mahdollista saada selville, kuinka hyvä mahdollisuus murtautujalla on päästä kohteeseen ilman, että hän tulee havaituksi. Tämän kautta voidaan saada tietoa siitä, millä tavoin kampuksen fyysinen turvallisuus on puutteellinen ja tarkemmin, mitkä ovat tämän valitun oppimisympäristön suurimmat heikkoudet. Nämä löytyvät tutkimuksen kautta. Testaamisen avulla voidaan arvioida heikoimmat kohdat ja parhaimmat reitit tunkeutumiseen.

Saatujen tulosten perusteella saadaan vastaus tutkimuskysymyksiin, 1. miten Kotkan kampuksen tieto- ja viestintätekniikan oppimisympäristön nykyinen fyysinen turvallisuus vastaa murtautumisuhkaan ja 2. miten oppimisympäristön fyysistä turvallisuutta voidaan parantaa uusilla ratkaisuilla. Näitä ratkaisuja voivat olla esimerkiksi uusien turvakameroiden ja turvalasien ostaminen heikoimpiin sisäänkäyntipisteisiin.

Oppimisympäristössä oleviin heikkouksiin kuuluvat kaikki tunkeilijalle mahdolliset sisäänkäyntipisteet rakennuksen ulkopuolella sekä oppimisympäristön sisällä siihen kuuluvat huoneet. Tunkeutumisprosessissa otetaan huomioon matkan varrella olevat esteet, kuten ovet, ikkunat, seinät, katot ja lattiat. Näiden avulla saadaan selville tunkeutumiseen käytetty aika. Tunkeutumisessa myös simuloidaan hidastajat, eli aika, jonka tunkeilija käyttää tietyn esteen läpimurtoon. Esteet ovat tähän alueeseen kuuluvat ovet, seinät, ikkunat, lattiat, katot, ja kaikki tilat, joiden läpi tunkeilijan pitää kulkea. Nämä kaikki tiedot laitetaan lopulta Jere Peltosen kehittämään TUREAN-laskentataulukkoon. Taulukoinnin jälkeen TUREANista saadaan onnistuneen keskeytyksen todennäköisyyden lopullinen tulos prosentteina. TUREAN on vapaasti ladattavissa Jere Peltosen omalla verkkosivulla: http://www.yhteisturvallisuus.net/.

1.3 Opinnäytetyön menetelmät ja rajaukset

Opinnäytetyö on laajennus lehtori Oraksen kurssilla annetusta tehtävästä, joka oli toiminnallinen menetelmä ja työ jatkui samaa menetelmää noudattaen. Alussa oleva teoriaosuus keskittyy TUREAN-tunkeutumisreittianalyysimallin ja sen Excel-laskentataulukon ymmärtämiseen ja siihen, kuinka sitä voidaan

toteuttaa testiympäristössä. Tämän tavoitteena on parantaa omaa ymmärrystä TUREANiin ja sen kautta edistää seuraavan osuuden toteuttamista. Sisäänkäyntireittien löytäminen ja niiden hidasteaikojen laskeminen TUREANiin avulla kuuluvat tutkimuksen toiminnalliseen osuuteen. Siihen sisältyvät kaikki mahdolliset perussuojien menetelmät eli ovet, ikkunat, seinät, katto ja lattia.

Opinnäytetyöni on tapaustutkimus, koska toimeksiantaja Kaakkois-Suomen ammattikorkeakoulu Xamk toivoi sitä toteutettavaksi tietyllä alueella eli tieto- ja viestintätekniikan alojen opetusympäristössä. Tapaustutkimus eli case-study on yksittäisen ja ainutkertaisen tapauksen tutkimista sen omaperäisessä ympäristössä. Tätä tutkimusmuotoa käytetään monella tieteenalalla esimerkiksi psykologiassa, lääketieteessä, arkeologiassa ja kauppatieteessä. Tapaustutkimuksen tavoitteena on tutkia, kuvata ja raportoida tapahtumaa huolellisesti, jotta tutkimuksesta saataisiin vastaukset tutkimuksen esittämiin kysymyksiin. Nämä kysymykset ovat yleisesti, miten-ja-miksi muodossa. (Saarenen-Kauppianinen, & Puusniekka 2006.)

Tapaustutkimusta ei kuitenkaan pidä kohdella aineiston keräämisen menetelmänä, vaan tutkimusstrategiana, jonka kautta työ toteutetaan. (K, Cherry. 2021)
Tapaustutkimus muodostuu eri tyypeistä ja ne ovat luokiteltu niiden lähestymistapojen mukaan (Eriksson & Koistinen 2014):

- Kuvaileva tapaustutkimus
- Selittävä tapaustutkimus
- Eksploratiivinen ja uutta teoriaa kehittävä tapaustutkimus
- Itsessään arvokas, välineellinen ja kollektiivinen tapaustutkimus
- Intensiivinen ja ekstensiivinen tapaustutkimus

Tapaustutkimuksissa sovelletaan kvalitatiivista eli laadullista tutkimusta etenkin, jos tutkimuksen kohteena on yhtiö tai yksilö. Kvalitatiivisissa tutkimuksissa kerätään aineistoa tekstien, kuvien ja omien havaintojen kautta.

Tietojen keräämisen kautta voidaan kehittää mahdollisimman laaja ja syvällinen ymmärrys tapahtumasta ja sen ympäristöstä, joilla selvitetään tutkimuksen kokonaisuus. Tapaustutkimuksessa toimitaan samoin ja näiden avulla voidaan kehittää uusia parannuskeinoja. (Aaltio-Marjosola 1999.)

Tapaustutkimusta voi myös liittää kvantitatiiviseen eli määrälliseen tutkimukseen, sillä molemmissa voidaan käyttää ihmisten haastattelua tiedonkeräämisessä ja tutkimuskysymyksen vastaamisessa. (Vilpas 2013.)

Olen hyödyntänyt taustatutkimusta kvalitatiivisen menetelmän kautta perehtymällä TUREAN-työkalun aineistoon ja tarkastelemalla oppimisympäristöä. Oppimisympäristön läpikäymiseen kuului omien havaintojen tekeminen sen nykyisistä suojausmenetelmistä ja ottamalla kuvia ympäristön ulkopuolisesta ja sisäisestä alueesta.

Tutkimukseni testialue rajoittuu kampuksen tieto- ja viestintätekniikan koulutuksen tiloihin, koko loppukampus mahdollisina heikkouksineen jäi tutkimuksen ulkopuolelle. Koko kampuksen sisällyttäminen tutkimukseen olisi tehnyt tutkimuksesta liian monimutkaisen, etenkin kun testauksessa käytettiin aina samaa kohdetta. Testaamista rajattiin myös poistamalla hidasteaikojen itsenäinen laskeminen ja sen sijaan käytettiin Schneiderin ja Pesosen opinnäytetyössä, “Benchmark-aikoja hidaste-elementeille Tunkeutumisreittianalyysityökaluun”(2009), olevia käytännön kokeiden tuloksia kampuksen tiloja varten. Lähtökohtaisesti näiden testaaminen ei ollut mahdollista, sillä ikkunoiden tai seinien rikkominen taikka kampuksen ovien läpi murtautuminen ei ole hyväksyttävää eikä edes korvaushintojen arvoista tutkimusta varten.

2 TUREAN-TUNKEUTUMISREITTIANALYYSI

Jere Peltosen luoma työkalu on Microsoftin taulukkolaskentaohjelma Exceliin pohjautuva ohjelma, jonka avulla pystytään saamaan selville, kuinka todennäköistä on, että rikollinen epäonnistuu tunkeutumisessa. Se perustuu The Estimate of Adversary Sequence Interruption (EASI) -menetelmään ja yrittää samalla korjata menetelmässä puutteellisia osia. TUREAN-tunkeutumisreittianalyysin avulla testataan rikollisen tunkeutumisen epäonnistumisen todennäköisyyttä toimitilaturvallisuuden ratkaisuihin liittyen.

TUREAN laskee vaihtoehtoiset tunkeutumisreitit käyttäjän syöttämien tietojen pohjalta ja laatii eri tapahtumaketjut sisältävän tulosluettelon. Analyysin avulla tunnistetaan tehokkaat ja vähemmän tehokkaat tilojen suojaukseen liittyvät ratkaisut. (Peltonen 2003.)

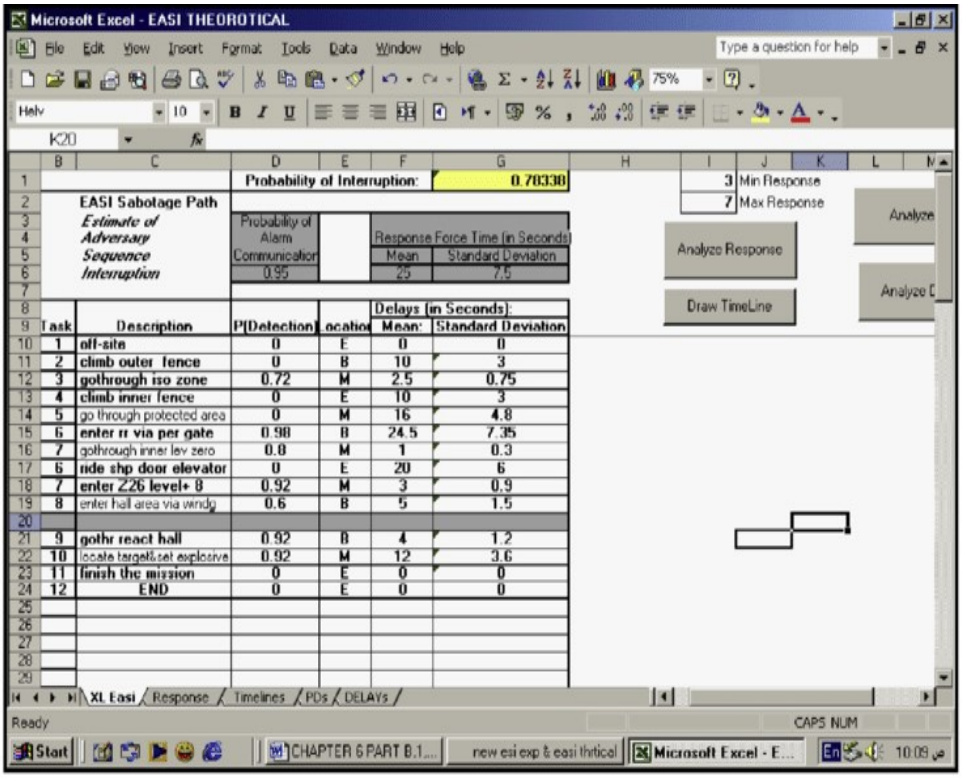
TUREAN soveltaa vyöhykeperiaatetta, jossa toteutettujen rakenteellisten suojauksien ja turvallisuusvalvonnan tehokkuus analysoidaan. Tätä varten tutkimuksessa pitää havainnoita ja kirjata kaikki vyöhykkeeseen kuuluvat oleelliset fyysiseen turvallisuuteen liittyvät asiat ja tutkia, miten tunkeilija voi murtautua vyöhykkeen eri alueisiin ja mitä eri reittejä hän voi käyttää päästäkseen hänen kohdepisteeseensä. Nämä tiedot lisätään Excel-laskentataulukkoon, joka sisältää myös muita murtautumisyrityksiin liittyviä asioita, kuten läpikulkuun tarvittavat ajat ja niiden aiheuttamat hidasteajat. Kaikissa murtautumisyrityksissä on kuitenkin omat variaationsa riippuen tunkeilijan tekemistä valinnoista. Nämä valinnat muuttavat tunkeutumisen yksityiskohtia ja voivat aiheuttaa äärimmäisen erilaisia tuloksia. Näitä yksityiskohtia ovat esimerkiksi eri sisäänkäyntireitin käyttäminen, erilaisen työkalun käyttö tai niiden puuttuminen. Tutkimukseen tulee myös sisältymään vasteaika, eli aika, johon on huomioitu tunkeilijan havaitseminen ja jossa hälytys on lähetetty eteenpäin vastetoimeenpiteiden suorittajille, jotka sitten saapuvat paikalle tietyssä ajassa. Tätä aikaa verrataan lasketettuun hidasaikaan taulukkolaskentaohjelmassa. Laskentaosassa saadaan jokaisen mahdollisen tunkeutumisreitinvaihtoehdon ja niihin kuuluvien aikojen pohjalta luettelo kaikista eri tuloksista, joihin kuuluvat läpikulku, hidasteet ja vasteajat.

Näiden tietojen perusteella Excel laskee kaikki murtautumisyritykset ja antaa tuloksena jokaiselle reitille niiden tunkeutumisen keskeyttämisen todennäköisyyden kohteen ympärille.

2.1 Estimate of Adversary Sequence Interruption

Estimate of Adversary Sequence Interruption (EASI), joka tarkoittaa vapaasti suomennettuna ”vastustajan tunkeutumisen sekvenssin arvio”, on tietokonepohjainen sovellus, jota käytetään onnistuneen varkauden tai sabotaasin todennäköisyyden laskemiseksi ydinlaitoksessa. Siinä tunkeilija asetetaan määritellylle polulle ja laitoksen vastausvoima on saada ilmoitus tunkeilijasta ja sitten joko pysäyttää tai viivyttää tunkeilija tietyssä ajassa. Tällä menetelmällä voidaan tutkia, voiko laitoksen fyysinen suojausjärjestelmä vastata ajoissa keskeyttää tunkeilijan polun varrella. (Levine 1978.)

Analyysin suorittamista varten tarvitaan neljä tietoa: 1. tunkeilijan havaitsemisen todennäköisyys riippuen jokaisesta havaintojärjestelmästä, kuten sensorit ja kamerat, 2. kuinka todennäköisesti ja kuinka nopeasti on mahdollista saada yhteys laitoksen vastausvoimiin, 3. vastausajan keskiarvo ja keskihajonta ja 4. keskiarvo ja keskihajonta jokaisen tehtävän vastustajan suorittamisessa toimintasekvenssissä. (Bennett 1977.) Kuvassa 1 näkyy käytännöllinen esimerkki EASI-mallista Excel-laskentataulukossa.

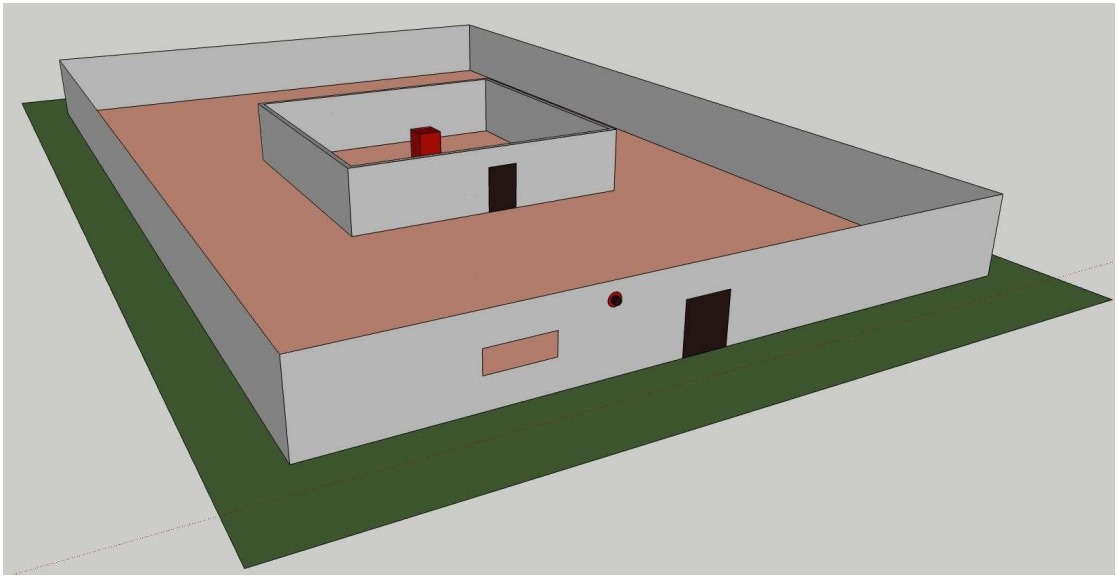


Kuva 1. Esimerkki EASI ohjelman menusta (Wadoud, Adail, Saleh, 2017)

The Estimate Time of Adversary Sequence on kuitenkin Peltosen mukaan puutteellinen verrattuna TUREANiin, koska sillä pystytään laskemaan vain yhden tunkeutumisreitin onnistumisen todennäköisyys kerrallaan. TUREAN taas pystyy laskemaan mahdollisesti tuhansia, mikä tekee siitä helpomman käyttöä varten ja samalla hyödyllisemmän sovelluksen tutkimuksia varten. (Peltonen, 2003).

2.2 TUREAN-tunkeutumisreittianalyysi käytännössä

Käytännön esimerkkinä voidaan käyttää kuvassa 2 olevaa yksinkertaista aluetta, joka on jaettu kahteen osaan: ulkopuoliseen alueeseen ja sisäiseen alueeseen, joka kattaa kaikki rakennuksen sisäiset huoneet.



Kuva 2. Malli käytännön esimerkin alueesta

Tässä testissä löytyy alueiden keskipisteessä punaisella suorakulmiolla merkitty palvelin, jota käytetään murtautumisyrityksen kohteena, eli asiana, johon tunkeilija yrittää päästä käsiksi. Tämä palvelin on sijoitettu tiiliseinien sisälle rakennettuun yhdellä sisäänkäyntireitillä (ruskea ovi) varustettuun huoneeseen, joka on yksi osa testin sisäisen alueen kokonaisuutta.

Tähän sisäisen alueen kokonaisuuteen kuuluvat myös rakennuksen sisässä oleva huone, joka ympyröi kohdetta ja kaikki siihen kuuluvat seinät. Tätä sisäistä aluetta ympäröi taas laajempi ympäristö, joka muodostuu rakennuksen ulkopuolisista seinistä, joissa on yksi avaimella lukittu ruskea ovi ja läpinäkyvä ikkuna mahdollisina sisäänkäyntireitteinä. Näistä koostuu ulkopuolinen alue. Testissä ei esiinny fyysisiä valvojia, mutta ulkopuolisen alueen ovea ja ikkunaa valvoo punainen turvakamera ja sisäisen alueen ovessa on sähköinen lukko, joka hälyttää, mikäli ovi aukeaa ilman tietyn koodin syöttämistä.

Tunkeilija aloittaa tunkeutumisyrityksensä ulkopuolisen huoneen laitamalla, valitsee reittinsä ja tästä analyysi alkaa. Tässä esimerkissä esiintyvät hidasteajat ja vasteajat ovat keksittyjä eivätkä siis ole todenmukaisia. Sisäänkäyntireittien käytössä tulee myös olemaan havainnoinnin todennäköisyys, minkä takia niille pitää arvioida omat tyypit. TUREAN-mallissa on kolme tyyppiä: H, K, J ja ne kertovat, kuinka paljon hidastetta on jäljellä havainnoinnin syntyessä.

H-tyypissä tunkeilija havaitaan ennen murtautumisen alkua, jolloin hidaste lasketaan koko murtautumisyrityksen ajalta. K-tyypissä tunkeilija havaitaan, kun hänen murtoyrityksensä on kesken, jolloin hidasteajasta lasketaan loppuaika, jonka hän tarvitsee läpipääsyyn. J-tyypissä tunkeilija havaitaan vasta, kun hän on onnistuneesti läpipäässyt esteensä, jolloin hidasteaikaa ei lasketa. Tilanteissa, joissa tyypin muoto ei ole selvä, Excel-laskentataulukko olettaa sen olevan H-tyyppinen.

Ulkopuolisessa alueessa tunkeilijan pitää päästä rakennuksen sisälle, jossa hänellä on kolme mahdollista sisäänkäyntireittiä.

1. Ulko-oven kautta murtautuminen, jota valvoo turvakamera ja tunkeilijan tarvitsee käyttää työkaluja esim. sorkkarautaa tai ruuvimeisseliä ja vasaraa päästäkseen sisälle. (Hidaste 60 s, havainnoinnin todennäköisyys 95 %, havaitaan ennen murtautumista, joten H-tyyppi.).
2. Ikkunan rikkominen ja aukosta sisään meneminen (Hidaste 30 s, havainnoinnin todennäköisyys 95 %, havaitaan ennen murtautumista, joten H-tyyppi.).
3. Kiviseinän rikkominen sähkötyökalulla, esim. puukkosahalla ja sisään meneminen aukosta (Hidaste 600 s, havainnoinnin todennäköisyys 5 %, havainnointi epäselvä, sillä kamera ei voi huomata häntä, mutta ihminen voi huomata hänet jokaisen vaiheen aikana. Tämä tekee siitä H-tyypiksi.).

Seuraavaksi riippumatta valitusta sisäänkäyntireitistä tunkeilija kulkee kohti sisäistä huonetta.

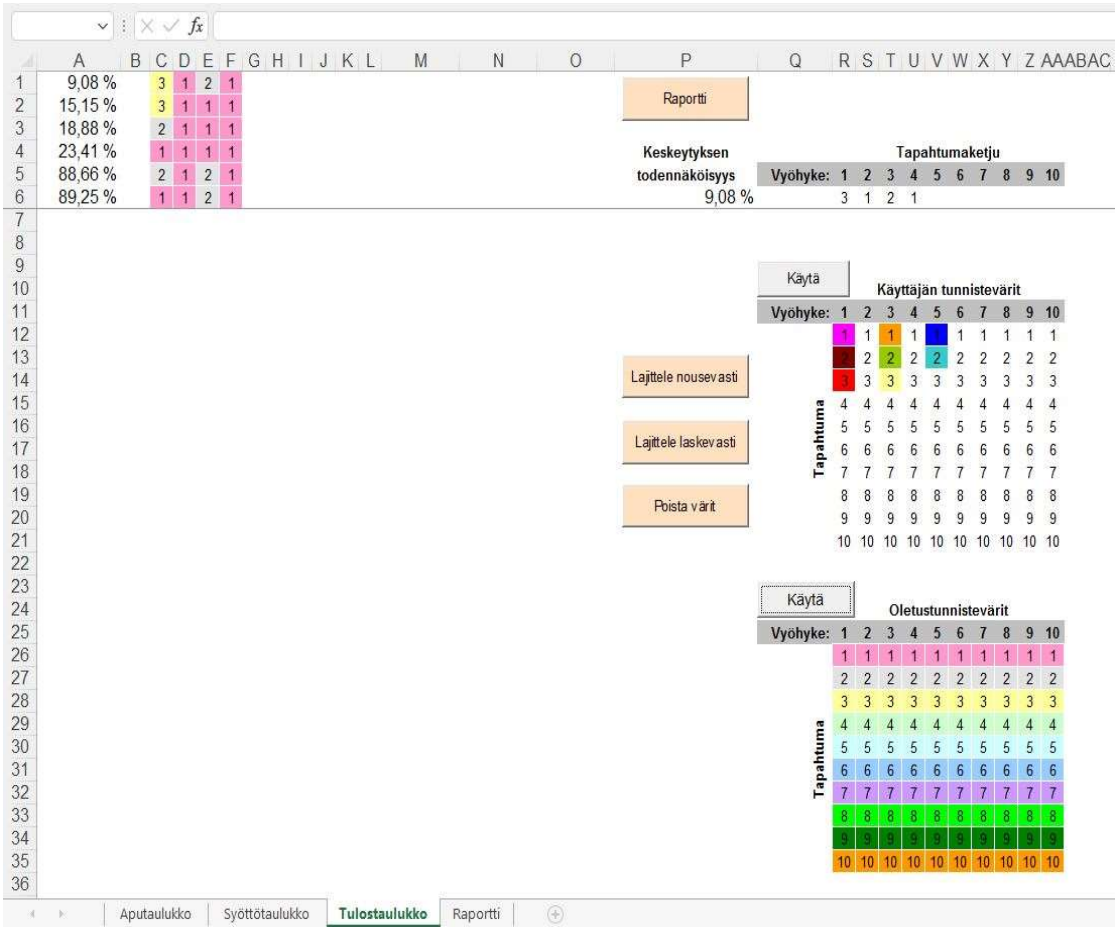
1. Siirtyminen (Hidaste 30 s, havainnoinnin todennäköisyys 0 %, pystytään huomata missä tahansa vaiheessa, eli H-tyyppi).

Huoneen luona, tunkeilijan pitää vielä valita sisäänkäyntireitti, jotta hän pääsee kohteeseensa.

1. Oven murtaminen (Hidaste 60 s, havainnoinnin todennäköisyys 95 %, oven hälytin laukeaa avatessa, eli J-tyyppi).
2. Sisäisen huoneen seinien rikkominen (Hidaste 600 s, havainnoinnin todennäköisyys 5 %, voi tapahtua jokaisessa vaiheessa, eli H-tyyppi).

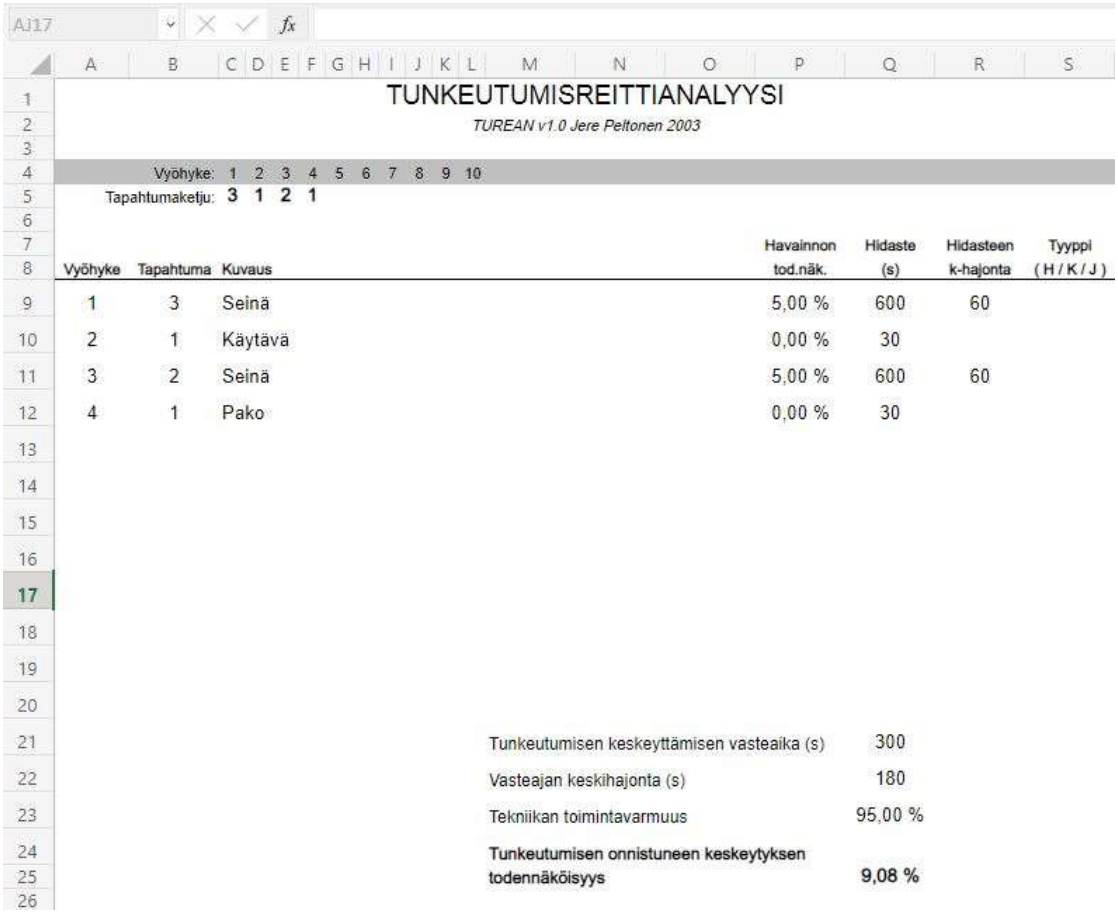
Lopulta tunkeilijan pitää paeta alueelta, jossa hän käyttää sisäänkäyntireittiään (Hidaste 60 s, havainnoinnin todennäköisyys 0 %, voi tapahtua jokaisessa vaiheessa, eli H-tyyppi).

Tunkeutumisreittejä on kokonaisuudessaan (3 x 1 x 2 x 1), eli 6 mahdollista vaihtoehtoa, joiden onnisteen keskeytyksen todennäköisyydet näkyvät kuvassa 3.



Kuva 3. TUREAN antama tulostaulukko esimerkistä

Kuvassa 4 näkyy näistä tuloksista onnistuvin murtautumisyritys, jossa tunkeilija kulki molempien seinien läpi ja jonka havaitsemisen todennäköisyys on 9,08 %.



TUNKEUTUMISREITTIANALYYSI

TUREAN v1.0 Jere Peltonen 2003

Vyöhyke: 1 2 3 4 5 6 7 8 9 10

Tapahtumaketju: 3 1 2 1

Vyöhyke	Tapahtuma	Kuvaus	Havainnon tod.näk.	Hidaste (s)	Hidasteen k-hajonta	Tyyppi (H / K / J)
1	3	Seinä	5,00 %	600	60	
2	1	Käytävä	0,00 %	30		
3	2	Seinä	5,00 %	600	60	
4	1	Pako	0,00 %	30		

Tunkeutumisen keskeyttämisen vasteaika (s)	300
Vasteajan keskihajonta (s)	180
Tekniikan toimintavarmuus	95,00 %
Tunkeutumisen onnistuneen keskeytyksen todennäköisyys	**9,08 %**

Kuva 4. Raportti onnistuneimmasta murtautumisesta

3 FYYSINEN TIETOTURVA

Fyysinen tietoturva ja tekninen tietoturva eli kyberturvallisuus muodostavat tietoturvallisuuden kokonaisuuden, jossa fyysinen puoli yrittää suojata laitteita ja informaatiota fyysisiltä uhkilta. Näihin uhkiin kuuluvat kaikenlaiset tapahtumat tai toimet, jotka voivat vahingoittaa laitteistoa ja ohjelmistoa tai aiheuttaa tiedon menetystä yritykselle tai henkilölle. Nämä uhat voivat johtua ihmisistä varkauden tai ilkivallan kautta, mutta myös luonnonilmiöistä, kuten tulipaloista, tulvista maanjäristyksistä tai sähkökatkoista. Fyysinen tietoturva yrittää suojata näiltä uhkilta eri turvallisuusmenetelmillä, joihin kuuluu esimerkiksi kulunvalvonta, hälytysjärjestelmät, vartiointi, tilojen lukitseminen, paloturvallisuus ja varmuuskopiointi. (Tirronen 2003.)

Suomessa on nykypäivänä tarjolla erilaisia ohjeita, asetuksia ja standardeja, joilla yritys tai yksilö voi käyttää oman tietosuojan parantamiseen. Näihin kuluvat mm. EU:n yleinen tietosuoja-asetus General Data Protection Regulation (GRPR), Tietoturvallisuuden auditointityökalu Katakri, kansainvälinen standardi ISO 27001 ja VAHTI, jonka toiminnasta vastaa Digi- ja väestötietovarasto.

ISO 27001 jakaa fyysisen turvallisuuden rakenteessa kuuteen eri kohtaan:

- Alue
- Ulkopinta
- Sisäseinät
- Ala- ja yläpohjat
- Ovirakenteet
- Ikkunat

4 MURTAUTUMISEN UHKAT

Kyberturvallisuudessa laitteiden ja tietojen suojaamista fyysisiltä hyökkäyksiltä ei ole yleisesti katsottu yhtä tärkeänä toimenpiteenä kuin verkon kautta tulevilta ulkopuolisilta vahingontekijöiltä, vaikka välinpitämättömyys näiden fyysisten hyökkäysten suhteen voi aiheuttaa enemmän vahinkoa yritykselle tai henkilölle kuin alun perin luullaan. Nykypäivänä ei voida myöskään olettaa, että tunkeilijan syy murtautumiseen olisi pelkästään rahallinen, sillä varkaus, sabotointi tai laitteiden käyttö paikan päällä voivat olla tapoja vahingoittaa valittua kohdetta. Yleisesti kyberturvallisuudessa yritykset, yksilöt ja yhteisöt yrittävät suojella tietojaan manipuloinnilta hyökkääjiltä, joiden ei tule päästä käsiksi heidän laitteisiinsa.

Tämän takia infrastruktuuri pitäisikin rakentaa turvallisuuden kannalta, siten että ymmärretään minkälaisia mahdollisia uhkia molemmat hyökkäysmuodot tarjoavat. Tällöin pystyttäisiin suunnitelmaan oikeankaltaisia turvajärjestelmiä ja toimenpiteitä, jotka pystyvät toimimaan esteenä molempien hyökkäystapojen näkökulmasta. Riskitekijöiksi hyökkäystilanteissa muodostuu se, jos turvajärjestelmät ja toimenpiteet epäonnistuvat, tai jos niitä ei ole alun perin käytössä.

Esimerkiksi, jos yrityksen rakennuksessa tapahtuu sähkökatkos joko vahingossa tai tahallisesti aiheutettuna, eikä käytössä ole olemassa kunnollista varavoimasysteemiä, yrityksen sähköiset turvajärjestelmät kaatuvat. Tällöin eivät sähköiset lukot ja turvakamerat pysty estämään tai hidastamaan ulkopuolelta tulevaa tunkeilijaa.

Fyysisessä hyökkäyksessä tunkeilija pystyy aiheuttamaan vahinkoa kyberturvallisuuden näkökulmasta monella eri tavalla. Tämä opinnäytetyö antaa hyvän esimerkin tilanteesta, jossa tunkeilija yrittää päästä käsiksi Xamkin kampuksen tieto- ja viestintätekniikan alueen datakeskukseen. Siellä hän pystyy helposti, joko varastamaan tai tuhoamaan laitteistoja ja lisäksi hän pystyy myös infektoimaan ne esimerkiksi tietoa varastavalla haittaohjelmalla. On olemassa muitakin esimerkkejä aivan tavallisissa oppimisympäristöissä ilmenevistä vastaavaan tilanteeseen johtavista tapahtumista. Esimerkiksi tietokone on jätetty auki ja lukitsematta, jolloin tunkeilija pystyy helposti pääsemään käsiksi koneessa oleviin tiedostoihin, ovat ne sitten kovalevyllä tai pilvipalveluissa. Tunkeilija pystyy myös asentamaan viruksen sisältävän USB-tikun koneeseen, jolloin tämä virus pystyy toimimaan vakoilu- tai haittaohjelmana. (Resolver 2022.)

5 TYÖN ETENEMINEN

Käytännön tutkimus toteutettiin testiympäristössä, kun tilat eivät olleet muussa käytössä, kuitenkin aukioloaikoina ja niin, että testaaminen ei häiritsisi muita ihmisiä ja että sitä olisi helpompi toteuttaa ilman oikean murtautumisyrityksen syytettä. Testaamisessa ajan mittaaminen alkoi aina ympäristön ulkopuolella olevasta parkkitiloista, josta edetään valittuun sisäänkäyntikohtaan. Testaamisessa otettiin huomioon se, että tunkeilija pystyy tuomaan mukanansa apuvälineitä tai työkaluja ja käyttämään murtautumisessa apunaan myös kaikkia esineitä, joita hän löytää testausympäristöstä. Tunkeilija voi käyttää näitä esineitä, jotka ovat esitetty kuvassa 5 hidasteiden läpäisemisessä, apuvälineenä kiipeämisessä tai työkaluna lasien ja ovien rikkomisessa.

Kuva 5 Kampuksen pihalla löytyviä esineitä

Testiympäristössä on myös monia ikkunoita, joita ei voinut täysin avata sisältäpäin ja jotka tunkeilijan on pakko rikkoa pystyäkseen kulkemaan niiden kautta. Näiden ikkunoiden ja ovien rikkomisen välttämisen takia ajanmittaukset keskeytettiin aina kun tunkeilija pääsi niiden luokse ja pystyi todenmukaisesti kulkemaan niiden läpi. Mittaukset käynnistettiin uudestaan rakennuksen sisällä vastapäätä sisäänkäyntikohdetta. Tällöin tunkeilija kulkisi nopeinta reittiä loppupisteensä suuntaan. Testaamisessa rakennuksen sisäiset ovet ovat myös suljettuja, mutta suurin osa niistä ei aiheuttanut suurta estettä. Tunkeilija saattoi joko avata ne ilman minkäänlaista avainta tai muutamassa esimerkissä ovissa on lasiset ikkunat, jotka tunkeilija pystyi rikkomaan ja näin tehdä tarpeeksi ison reiän päästäkseen niistä läpi. Mahdollista oli myös tehdä reikä tarpeeksi alas ikkunalasiin ja sen kautta ylettää avaamaan ovi sen toiselta puolelta.

Kaikkien ovien, ikkunoiden ja seinien läpäisy, joka tunkeilijan tarvitsee suorittaa päästäkseen kohteeseen, on arvoitu käyttäen apuna aiempaa opinnäytetyötä, josta saadaan hidasteiden läpipääsyn ajat. (Schneider & Pesonen 2009). Nämä läpäisyajat on esitetty kuvassa 6.

Este	Hidasteaika
Kevyt väliseinä	195
Puinen ulkoseinä	330
Tiiliseinä	205
Teräsbetoniseinä	240
Kevytrakenteinen väliovi, rikkomalla	40
Kevytrakenteinen väliovi, vääntämällä	15
Metallirakenteinen ovi	103
Yksinkertainen ikkuna	75
Kalterilla suojattu ikkuna	205
Verkkoaita, kiipeämällä	11
Verkkoaita, leikkaamalla	192
Verkkoaita, tikkailla ylittämällä	9
Säleverkkoaita, kiipeämällä	16
Säleverkkoaita, leikkaamalla	180
Säleverkkoaita, tikkailla ylittämällä	6

Kuva 6 Schneider & Pesonen hidasteaikojen yhteenveto

Testissä ei yhdenkään tunkeutumisen ajanmittaus lopu ennen kuin tunkeilija on paennut oppimisympäristöstä, eli palannut lähtöpisteeseen käyttäen omaa pakoreittiään. Pakoreittinä voidaan käyttää samaa reittiä, jonka tunkeilija avasi sisäänpääsyssä tai se voi olla reitti jonkin toisen oven tai ikkunan kautta.

5.1 Vyöhykeperiaate

Aiemmassa luvussa mainitsin, että TUREAN-työkalulla analysoidaan alueen rakenteellisia suojauksia vyöhykeperiaatteella. Tämä tarkoittaa alueen jakamista osiin perustuen näiden läheisyyteen tunkeilijan kohteesta. Päätin käyttää tätä periaatetta tutkimuksessani. Vyöhykeperiaatteen avulla saadaan parempi ymmärrys siitä, miten jokainen oppimisympäristön huone toimii, mukaan lukien murtausmisyrityksessä oleva kohdehuone. Minun mallini oppimisympäristöstä on rakennettu samalla tavalla kuin käytännön esimerkissä.

Ennen kun pystyin aloittamaan kolmiulotteisen mallin luomisen oppimisympäristöstä, minun piti laatia sille perusteet. Tähän käytin sekä itsenäistä

tutkimusta paikan päällä että kiinteistöpäällikkö Tuomo Kotolan antamia arkkitehdin pohjapiirustuksia. Itsenäiseen tutkimukseen kuului tilojen kuvaaminen ja mittaaminen. Näiden avulla pystyin rakentamaan mallin mahdollisimman tarkasti sen muodon ja koon kannalta.

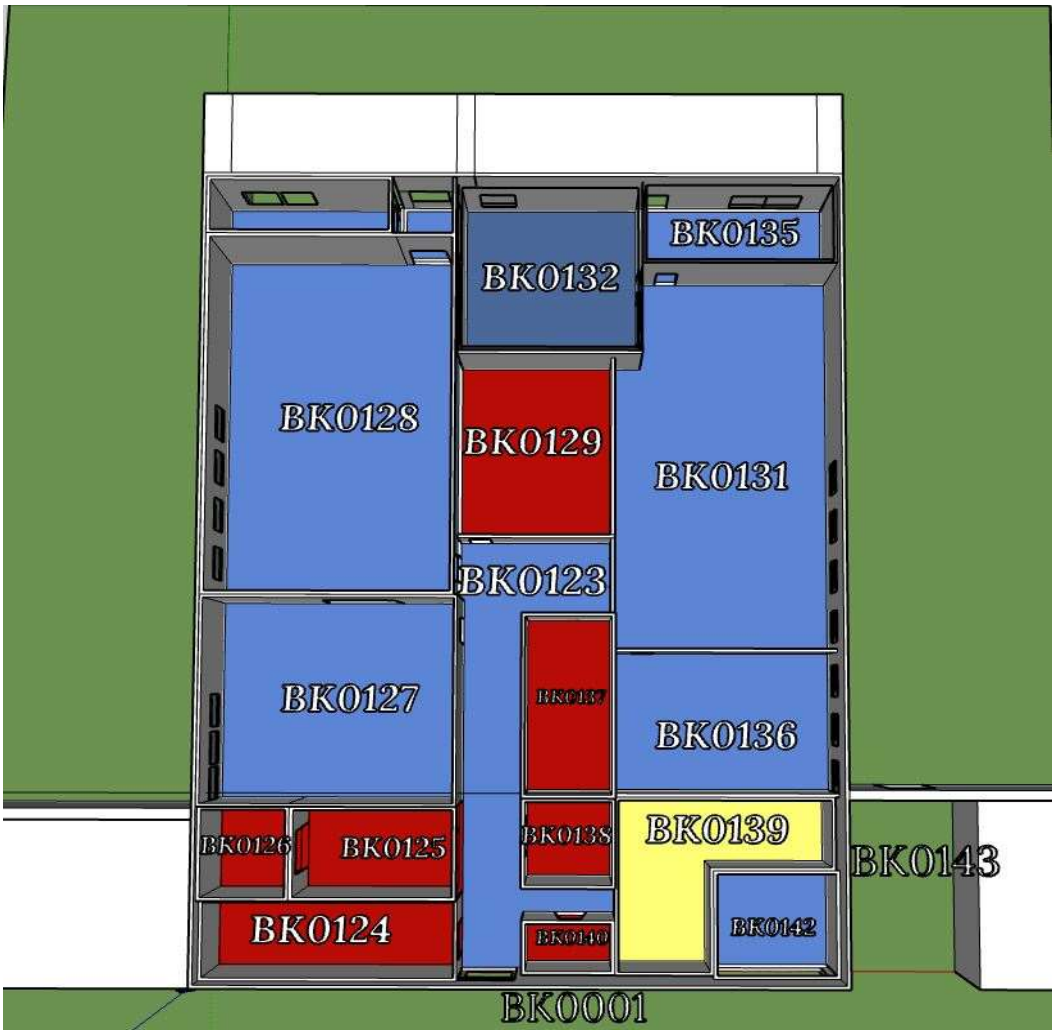
Paikan päällä tapahtuneessa tutkimuksessa etsin ja taltioin kaikki oppimisympäristön huoneiden sisäänkäyntireitit, eli ovet ja ikkunat, jotta pystyisin muistamaan niiden sijainnit ja ulkonäön mallin rakentamisessa. Otin niistä kuvia käyttämällä puhelimeni kameraa sekä mittasin niiden leveydet ja pituudet käyttäen mittanauhasovellusta. Halusin myös saada mahdollisimman tarkan kuvan huoneiden koosta, joten päätin myös mitata ne samalla tavalla kuin sisäänkäyntireitit. Tähän kuului jokaisen huoneen pituuden mittaaminen päästä päähän ja lattiasta kattoon. Oppimisympäristön pinta-ala on mittaamisen tulosten mukaan 574,5 neliömetriä (m²).

3D-mallia rakentaessa päätin jakaa oppimisympäristön vyöhykeperiaatteella neljään alueeseen, jotka näkyvät kuvassa 7:

- Vihreä on oppimisympäristön ulkopuolinen alue, johon kuuluu kampuksen ulkona oleva parkkialue ja sisällä oleva käytävä.
- Sininen on oppimisympäristön sisällä olevat huoneet, joissa on vähintään yksi sisäänkäyntireitti ulkopuolelta.
- Punainen on oppimisympäristön sisällä olevat huoneet, joissa ei ole ulkopuolelta tulevia sisäänkäyntireittejä.
- Keltainen on huone BK0139 eli datakeskus, joka on murtautumisyrityksissä kohteena.

Oppimisympäristössä on myös viides alue, johon kuuluu tilojen katot ja lattiat, joita tunkeilija voi käyttää murtautumisessa. Alueen tutkimisen jälkeen arvioin, että tunkeilija pystyy murtautumaan katon kautta käyttämällä luokan BK0131 kattoikkunaa. Hänen pitää kuitenkin tuoda mukanaan työkaluja, esimerkiksi vasaran lasin rikkomiseen ja köyden luokkaan laskeutumiseen. Oppimisympäristön sisäisen vyöhykkeen luokat BK0124, 0125, 0126, 0137, 0139, 0140 ja 0142 ovat kaikki yhdistetty kampuksen kokonaisuuteen ja sen eri kerroksiin. Tämä tarkoittaa, että tunkeilija pystyy murtautumaan näihin huoneisiin kampuksen sisällä rikkomalla ylhäällä olevien huoneiden lattiat. Tunkeilija siis pystyy esimerkiksi datakeskukseen murtautumisessa ohittamaan kaikki

oppimisympäristön turvajärjestelmät, eli ovet ja lukot sisäänmenossa. Hän pystyy myös pakenemaan näiden huoneiden kautta luomalla reiän lattiaan ja kulkemalla alemman kerroksen kautta.



Kuva 7 Ylhäältä katsottu näkökulma oppimisympäristön mallista

5.2 Tunkeutumisreitit

Tunkeutumisreittejä pohtiessa tutkijan kannattaa analysoida tarkoin kaikki yleisesti käytetyt sisäänkäyntiovet ja arvioida, kuinka hyvin ne voivat estää murtautumista. Tämä analysointi voidaan jakaa kahteen osaan, joista ensimmäiseen kuulee se, miten ovi on suunniteltu ja oven materiaalit. Murtautumisyrityksessä monilukkoinen teräsovi kestää paremmin fyysisiä iskuja kuin puinen ja siten sen läpikulkeminen on hitaampaa, joka nostaa tunkeilijan havaitsemisen mahdollisuutta. On kuitenkin yhtä tärkeää etsiä näistä ovista suunnitelmallisia vikoja, sillä laminoitu lasi ei voi estää tunkeilijaa, jos hän esimerkiksi pystyy rikkomaan oven saranat ja kaatamaan sen. Toinen osa taas

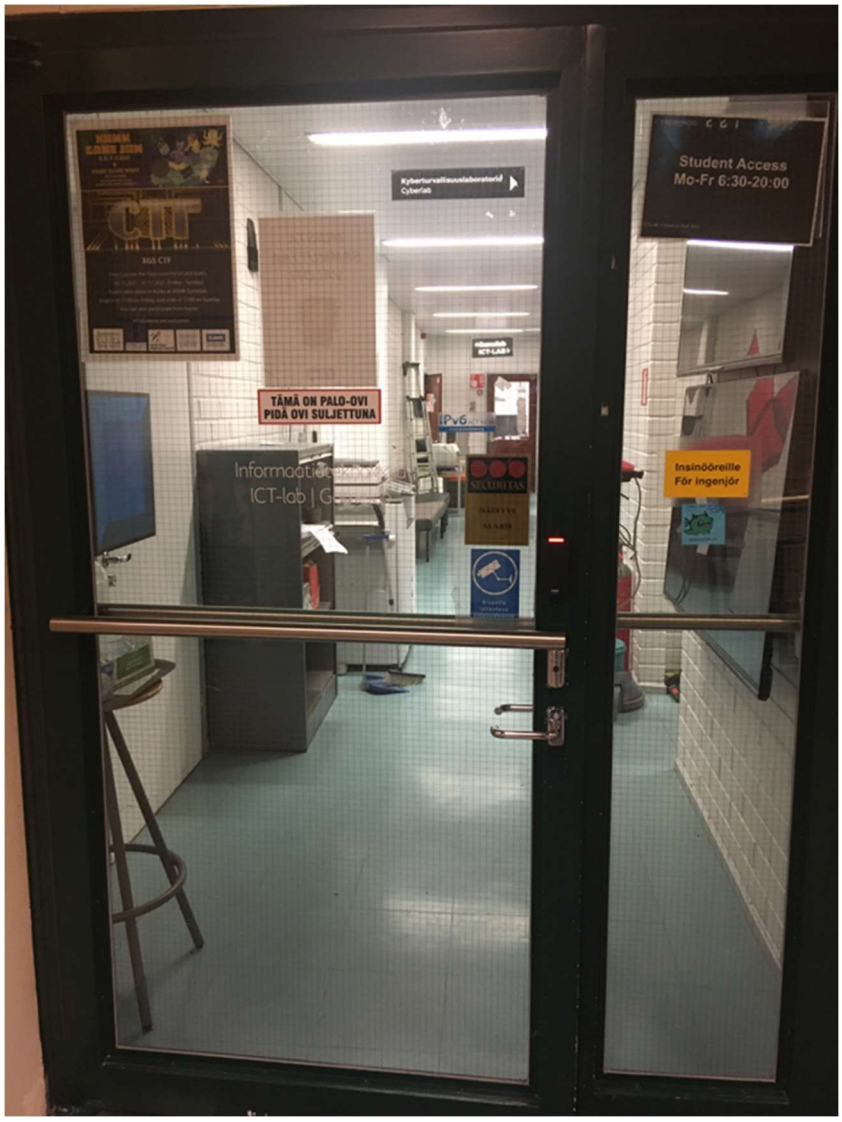
sisältää oven havaitsemislaiteet, eli sensorit, turvakamerat ja hälytysjärjestelmät, jotka huomauttavat rakennuksen turvajärjestelmälle laittomasta läpikulkemisesta. Näiden olemassaolo taas vähentää vastevoimien aikaa saapua tunkeilijan luokse ja näin pystytään paremmin estämään pakoa.

Ikkunoita tulee myös suojata, joko asentamalla niiden ympärille valvonta- ja hälytyslaitteita tai vahvistamalla ne esimerkiksi metalliristikoilla. Kumpikin menetelmä parantaa rakennuksen fyysistä turvallisuutta ja toimii tunkeilijalle esteenä murtautumisyrityksessä.

On myös olemassa harvemmin ajateltuja reittejä kuten seiniä, lattioita ja kattoja, joiden materiaalit eivät ole tarpeeksi vahvoja estääkseen kulkuaukon tekemistä, varsinkin jos tunkeilija pystyy käyttää äärimmäisiä työkaluja, kuten lekaa, katuporaa tai jopa räjähteitä. Näiden reittien kautta tunkeilija pystyy luomaan oikoreittejä ja samalla ohittaa monia rakennuksen turvajärjestelmiä. Pahimmissa tapauksissa tunkeilija pystyy luomaan sisääntulo- ja ulkoreitin hänen kohteeseensa ja pakenemaan ennen kuin vastevoimat ehtivät paikan päälle.

5.2.1 Ovet

Tutkimuksen oppimisympäristössä on kolme ovea, jotka yhdistävät ulkopuolisen alueen sisäiseen. Kuvassa 8 näkyy ensimmäinen, joka sijaitsee kampuksen sisällä BK0001-käytävässä. Se on metallinen ovi, jossa on HID-iClass-SE lukijaan kulunvalvontaa varten, joka sallii sisäänpääsyn ainoastaan ihmisille, joilla on sähköinen avain. Sähköisen avaimen haltijat ovat koulun henkilökuntaa ja opiskelijoita. Tietyt ihmiset voivat myös avata oven fyysisellä avaimella. Ovessa on myös suojalasi, jonka arvioin olevan SFS-EN 356 mukaisella luokituksella vähintään P4A kestävyysluokkaa perustuen lasin tiheyteen.



Kuva 8 BK0128 käytävän sisäänkäynti

Kuvassa 9 ovat toiset kaksi ovea, jotka sijaitsevat oppimisympäristön vastapäätä ja liittävät kampuksen parkkitilan huoneisiin BK0128 ja BK0135. Ne ovat myös metallisia, mutta rakennettu eri tavalla ja BK0128 ovessa on lasi-ikkuna, joka on arvioni mukaan ensimmäistä heikompi. Niissä on samat suojausmenetelmät kuin ensimmäisessä ovessa.

Kuva 9 Huoneiden BK0135 (Vasen) ja BK0128 (Oikea) ulko-ovet

Oppimisympäristön sisällä olevat ovet on jaettu metallisiin ja puisiin, ja myös niiden turvallisuustoimenpiteet vaihtelevat. Näitä ovia käytetään alueiden erottelemiseen, kuten esimerkiksi erottamaan luokkatilat ja opettajien huoneet toisistaan. Näiden ovien lukitus perustuu sähköisten lukijoihin, joissa kaikilla avaimilla päästään luokkiin, mutta vain henkilökuntaan kuuluvien avaimilla päästään myös opettajien huoneisiin.

Murtautumisyrityksien kohteena olevan datakeskuksen ovi on metallinen ja siinä on poikkeuksellinen L-1 Identity Solutions sormenjäljenlukija sisäänpääsyä varten.

Arvioin näiden ovien hidasteajat käyttäen kuvassa 6 olevaa yhteenvetoa apuna. Sitä käyttämällä ja vertaamalla datakeskuksen ovea Schneiderin & Pesosen kuvaukseen metallisesta ulko-ovesta päättelin, että datakeskuksen oven läpimurto tulee kestämään korkeintaan yhtä kauan aikaa kuin metallirakenteisen oven kanssa, eli 103 sekuntia.

Kuvassa 8 olevan oven hidasteaika on hankalampi tulkita, koska sen reunat ovat metallisia, jonka takia sen läpimeno voi olla samanlainen kuin datakeskuksen oven kanssa, sillä on myös huomattava määrä suojalasia. Mainitsin aiemmin, että tämän lasi voidaan luokitella vähintään P4A kestävyysluokkaan, jonka hidasteaika standardin mukaan on 7,5 sekuntia. Lasi pystytään luokittelemaan korkeintaan P8A luokkaan, jolloin sen hidasteaika on yli 175 sekuntia. Tämän hidasteajan vaihtelun takia on vaikeaa saada tarkka aika lasin rikkomiselle. Lisäksi Oras kertoi minulle, että turvalasiin kiinnittävät listat ovat oven ulkopuolella, joten tunkeilija voi avata ne käytävän puolelta epätarkassa ajanmäärässä. Näiden tuntemattomien aikojen takia voin antaa tälle ovelle yhden varman hidasteajan, joka on metalliselle ovelle 103 sekuntia.

Kuvassa 9 olevilla ulko-ovilla BK0135 ja BK0128 on eri hidasteajat, koska niin kuin mainitsin aiemmin BK0128 oven lasi-ikkuna tekee siitä arvioinnin mukaan heikomman. Näin siksi että oven lasi on kevytlasista, joten sen hidasteaika muuttuu yksinkertaiseen ikkunaan, eli 75 sekuntiin. Tämä muutos johtuu siitä, että lasien paikka ovessa on tarpeeksi matalalla ja niiden rikkomisen jälkeen tunkeilijalla on mahdollista kurottaa kätensä kääntämään kahvaa toiselta puolelta. Hän pystyy myös kiipeämään näiden ikkunoiden läpi tekemällä tarpeeksi ison aukon lasiin.

BK0135-ovessa ei ole tätä heikkoutta, joten tunkeilijalla on vain yksi tapa murtautua oven kautta, eli rikkoa se työkaluilla. Se on tehty metallista, joten sille voidaan antaa sama hidasteaika kuin muille metallisille oville, eli 103 sekuntia.

5.2.2 Ikkunat

Oppimisympäristössä on 19 ulkoikkunaa, jotka ovat samanlaisia niiden pituuden, leveyden ja materiaalien kannalta. Esimerkki näistä ikkunoista näkyy kuvassa 10. Arvioinnin mukaan näiden ikkunoiden materiaali on samanlainen kuin BK0128 oven lasi, mikä tekee niistä kaikista kevyempiä ja heikompia kuin suojalasi. Näille ikkunoille annetaan myös hidasteeksi yksinkertaisen ikkunan aika, eli 75 sekuntia.

Kuva 10 Huoneen BK0128 ikkunat

5.2.3 Seinät

Oppimisympäristön ulkoiset seinät jakautuvat kahteen materiaaliin, tiileen ja betoniin. Mittauksien mukaan yksittäisen tiilen koko on 257 × 123 × 57 mm ja betoniseinän paksuus oli 205 mm. Oppimisympäristön sisätilojen seinät ovat samoja tiiliseiniä kuin ulkonakin. Huomasin tutkimuksessa, että kaikki huoneet ovat erotettu toisistaan tiiliseinillä, joiden tiheys on 246 mm. Tämä muuttaa seinien hidasteajan kaksinkertaiseksi eli 410 sekunniksi.

5.3 Oppimisympäristön arvionti

Oman tutkimisen kautta arvioin, että oppimisympäristössä on seitsemän huonetta, joita murtautuja voi käyttää tunkeutumisessa sisäänpääsyssä ja pakoreittinä. Nämä huoneet ovat BK0127, BK0128, BK0131, BK0132, BK0135, BK0136 ja BK0001. Näistä huoneista BK0128, BK0135 ja BK0001 sisältävät ulko-ovia, joiden läpi voidaan murtautua. Huoneissa BK0127, BK0128, BK0131, BK0132, BK0135 ja BK0136 on ikkunoita, joita tunkeilija voi käyttää samalla tavalla.

Päätin olla laskematta tunkeilijan murtautumista ulkopuolisten seinien läpi, sillä käytännössä, jos tunkeilija ei halua käyttää ovea, niin oppimisympäristön ikkunat ovat nopeampi lähestymistapa ja niiden havainnoinnin todennäköisyys on sama kuin seinissä. Ainoat seinät, joita tunkeilija voi hyödyntää murtautumisessa, ovat rakennuksen sisällä.

TUREAN-työkalun käytössä tarvitaan hidasteiden lisäksi tietää kolme asiaa oppimisympäristöstä: sen tekniikan toimintavarmuus, vasteajan odotusarvo ja vasteajan keskihajonta. Tekniikan toimintavarmuus tarkoittaa, kuinka todennäköistä on, että tieto tunkeutumisesta lähetetään oikeille henkilöille, jotka voivat siten aloittaa omat toimenpiteet tunkeutumisen keskeyttämiseksi. Annoin tämän onnistumisen todennäköisyyden arvoksi 90 %. Vasteajan odotusajalla tarkoitetaan sitä, kuinka kauan kestää vastevoimilla saapua paikalle ja estää murtautuminen. Tämän arvoin olevan vähintään viisi minuuttia, eli 600 sekuntia. Vasteajan keskihajontaa ei ole kuitenkaan mitattu usean mitatun saapumisajan kautta, joten se on oletettu olevan 30 % vasteajan odotusarvosta eli 180 sekuntia.

Lisäksi jokaisessa murtautumisen yksittäisessä tapahtumassa tarvitsee tietää sen tyyppi, mikä on tapahtuman havainnoinnin todennäköisyys ja minkä on tapahtuman hidasteen keskihajonta. Tyyppi voidaan antaa tapahtumalle, kun siinä on samanaikaisesti havainnoinnin mahdollisuus ja hidaste.

Näissä tilanteissa laitetaan taulukkoon, kuinka paljon hidasteen aikaa on jäljellä havainnon alkaessa. TUREAN-työkalussa on kolme tyyppiä, jotka ovat merkitty kirjaintunnuksilla H, K ja J.

- H-tyypissä murtautumisen tapahtuma havaitaan ennen kuin hidasteaikaa voi alkaa mitata, joten hidaste lasketaan sen kokonaisuudessa. Käytännön esimerkki tällaisesta vaiheesta on, kun valvoja huomaa turvakameran kautta tunkeilijan lukitun oven ulkopuolella ja hälyttää vastevoimat, ennen kun tunkeilija pääsee ovesta läpi.
- K-tyypissä hidasteajasta on kulunut puolet, joten vain loput hidasteesta lasketaan tapahtumassa. Käytännön esimerkki tällaisesta vaiheesta on, kun tunkeilija tulee vastaan lukitun oven, jossa on lasi ikkuna, jonka

hän voi rikkoa ja kiivetä läpi sisään. Rikkoessaan lasin oven tunnistimet hälyttävät rakennuksen henkilökunnalle murtautumisesta.
Tunkeilija on siis pystynyt aloittaa murtautumisensa, mutta ei ole pääs-syt oven toiselle puolelle ennen hälytyksen alkua.

- J-tyypissä hidasteaika on jo tapahtunut, kun se havaitaan, jonka seurauksena hidastetta ei lasketa tapahtumassa. Käytännön esimerkki tällaisesta vaiheesta on, kun tunkeilija pystyy avaaman lukitun oven havainnoimatta. Avaamisen jälkeen kuitenkin oven magneettisesti käynnistyvä hälytin aktivoituu ja hälyttää henkilökunnalle murtautumisesta. Tunkeilija pystyi siis pääsemään oven toiselle puolelle ennen hälytyksen alkua.

Minä en pystynyt tutkimuksen aikana testaamaan, missä vaiheessa murtautuja pystytään todennäköisemmin havaitsemaan alueelle tunkeutumiseen liittyvissä yksittäisissä kohdissa, kuten ovien tai lasien läpikulussa. Tämän vuoksi en voinut tietää tarkasti yksittäisten tapahtumien tyyppejä ja Excel-laskentataulukko muuttaa ns. tuntemattomat tyypit automaattisesti h-tyypeiksi.

Murtautumiseen liittyvän havainnon todennäköisyyden arvioin itse. Arvioinnissa otettiin huomioon olemassa olevien hälytysjärjestelmien reagointi murtautumiseen ja kuinka todennäköisesti se muutoin tulisi havaituksi. Tämä taas voi riippua monesta tekijästä, kuten tapahtuman sijainnista ja kuinka paljon ääntä siitä syntyy. Testissä annoin suuremman havainnoinnin todennäköisyyden oville, jotka pitää avata lukkojen rikkomisella, kuin oville, jotka voidaan avata sisältäpäin. Uskon myös, että oppimisympäristön sijainnin takia ikkunoiden rikkominen tulee olemaan hankalampi havaita varsinkin yöllä, jolloin kampuksen lähistöllä ei kulje yhtä paljon liikennettä. Oppimisympäristön sisäisellä alueella tapahtuvan melun arviointi on hankalaa, mutta se voidaan tulkita periaatteellisesti niin, että mitä kauempana se tapahtuu BK0001-käytävästä ja mitä syrjäisemmässä huoneessa se tapahtuu, sitä epätodennäköisemmin se havaitaan.

Tapahtumien keskihajonnan mittaaminen tehdään samoin, kuin vasteajan kanssa, eli jokaisen yksittäisen tapahtuman odotusarvo on 30 %.

5.4 TUREAN-työkalun tulokset

Ottaen huomioon kaikki oppimisympäristön sisäänkäyntireitit ja datakeskusta ympäröivät tilat pystyin keksimään kolme erilaista lähestymistapaa, joita käyttämällä tunkeilija voi päästä datakeskukseen.

Ensimmäinen oli murtautuminen datakeskuksen oven kautta. Tässä tapahtumassa murtautujalla on käytössä esimerkiksi sorkkarauta, jota hän voi käyttää ikkunoiden ja datakeskuksen oven rikkomiseen. Yhdessä onnistuvimmista yrityksistä tunkeilija murtautuu BK0128-luokkaan ikkunan kautta käyttäen sorkkarautaa. Seuraavaksi hän kulkee huoneen läpi BK0123-käytävään, jota varten hänen ei tarvitse rikkoa mitään. Tämän jälkeen hän on pääsyt datakeskuksen ovelle ja murtautuu huoneeseen rikkomalla oven samalla sorkkaraudalla. Tässä vaiheessa tunkeilija on todennäköistä havaittu, mutta hän pystyy pääsemään datakeskukseen ja pakenemaan ennen kuin vastevoimat saapuvat paikan päälle. Tunkeilijan murtautumisen keskeyttäminen on tässä tapauksessa alle 1 %. Tämän esimerkin tulos näkyy kuvassa 11 Excel-laskentakaaviona, jossa tunkeilija onnistuu murtautumisessa käyttäen hyväksi hänen nopeuttansa ja oikeita työkaluja.

TUNKEUTUMISREITTIANALYYSI

TUREAN v1.0 Jere Peltonen 2003

	1	2	3	4	5	6	7	8	9	10
Vyöhyke:										
Tapahtumaketju:	**2**	**1**		**1**						**1**

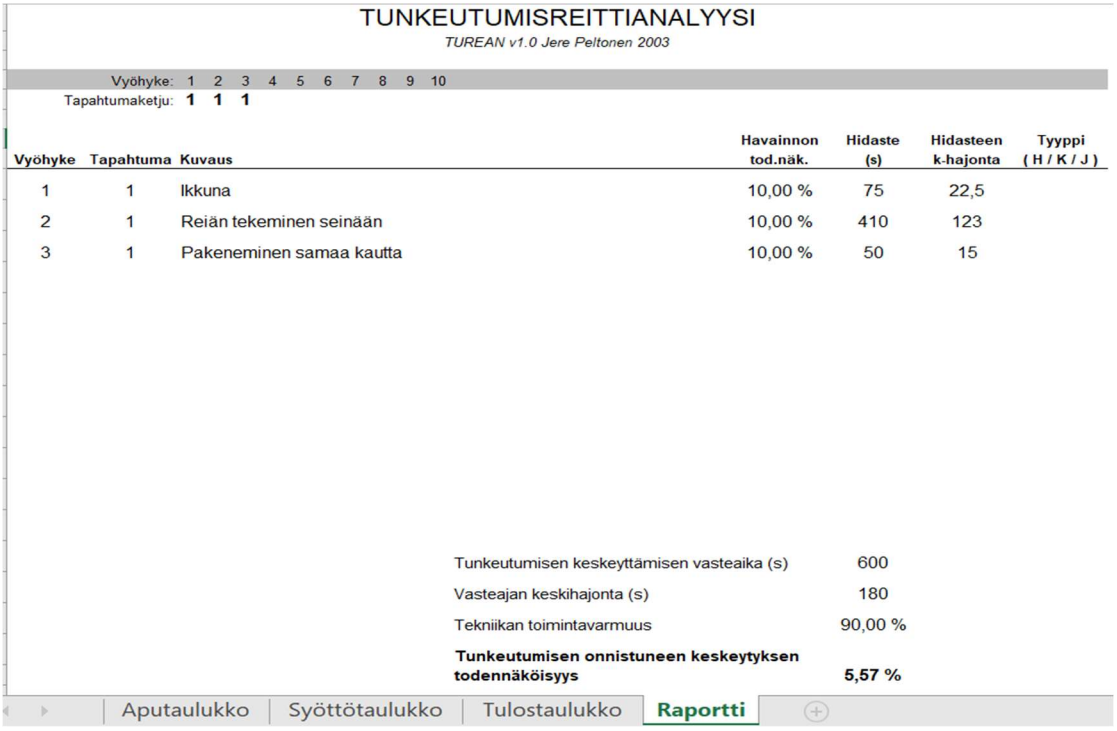
Vyöhyke	Tapahtuma	Kuvaus	Havainnon tod.näk.	Hidaste (s)	Hidasteen k-hajonta	Tyyppi (H / K / J)
1	2	BK0128 gamelab ikkuna	10,00 %	75		
2	1	Bk0123 Käytävän käyttö	10,00 %	50		
4	1	BK0139 oven rikkoaminen	90,00 %	103		
10	1	Pakeneminen samaa kautta	10,00 %	50		

Tunkeutumisen keskeyttämisen vasteaika (s)	600
Vasteajan keskihajonta (s)	180
Tekniikan toimintavarmuus	90,00 %
Tunkeutumisen onnistuneen keskeytyksen todennäköisyys	**0,98 %**

Aputaulukko | Syöttötaulukko | Tulostaulukko | **Raportti**

Kuva 11 Tulokset Bk0139 murtautumisyrityksestä oven kautta

Toinen murtautuminen datakeskukseen tapahtuu rikkomalla seinä sen ja BK0136-huoneen välillä. Tässä tilanteessa murtautuja murtautuu BK0136-huoneeseen, joko ikkunan tai sen oven kautta ja luo reiän näiden huoneiden väliin työkalun avulla. Tässä esimerkissä murtautuja käyttää pajavasaraa. Onnistuvin murtautuminen tämän kautta tapahtuu murtautumalla suoraan BK0136-huoneeseen ikkunan kautta.
Tämän murtautumisen tulokset näkyvät kuvassa 12, jotka ovat huomattavasti hitaampia verrattuna ensimmäiseen esimerkkiin. Sillä on silti vain 5,57 % havainnoin mahdollisuudet, koska BK0136 on riittävän syrjäinen huone, joten tunkeutumista ei voi helposti havaita sen tapahtuessa.



TUNKEUTUMISREITTIANALYYSI

TUREAN v1.0 Jere Peltonen 2003

Vyöhyke: 1 2 3 4 5 6 7 8 9 10
Tapahtumaketju: **1 1 1**

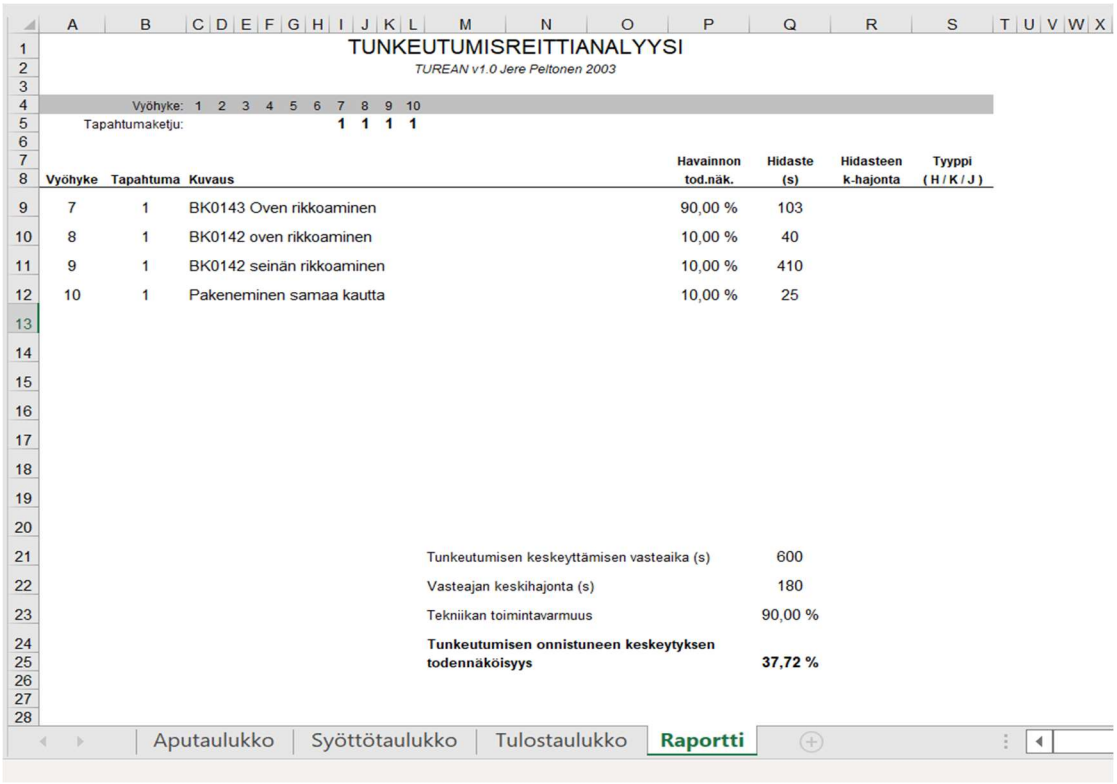
Vyöhyke	Tapahtuma	Kuvaus	Havainnon tod.näk.	Hidaste (s)	Hidasteen k-hajonta	Tyyppi (H / K / J)
1	1	Ikkuna	10,00 %	75	22,5	
2	1	Reiän tekeminen seinään	10,00 %	410	123	
3	1	Pakeneminen samaa kautta	10,00 %	50	15	

Tunkeutumisen keskeyttämisen vasteaika (s)	600
Vasteajan keskihajonta (s)	180
Tekniikan toimintavarmuus	90,00 %
Tunkeutumisen onnistuneen keskeytyksen todennäköisyys	**5,57 %**

Aputaulukko | Syöttötaulukko | Tulostaulukko | **Raportti**

Kuva 12 Tulokset BK0139 murtautumisyrityksestä Bk0136 seinän kautta

Kolmas murtautuminen tapahtuu myös seinän kautta, mutta se tehdään datakeskuksen toisella puolella huoneessa BK0142. Onnistuvin murtautuminen, jonka tulokset näkyvät kuvassa 13 tapahtuu käyttäen BK0143-ulko-ovea, joka johtaa BK0001-käytävään. Sen jälkeen murtautuja rikkoo BK0142-huoneen puuoven ja tekee reiän sen huoneen ja datakeskuksen välillä. Tätä varten tunkeilija tarvitsee ainakin pajavasaran onnistuakseen ja silti hänen murtautumisen keskeyttämisen todennäköisyys on 37,42 %, eli merkittävästi korkeampi kuin aiemmat lähestymistavat.



TUNKEUTUMISREITTIANALYYSI

TUREAN v1.0 Jere Peltonen 2003

Vyöhyke: 1 2 3 4 5 6 7 8 9 10

Tapahtumaketju: 1 1 1 1

Vyöhyke	Tapahtuma	Kuvaus	Havainnon tod.näk.	Hidaste (s)	Hidasteen k-hajonta	Tyyppi (H / K / J)
7	1	BK0143 Oven rikkoaminen	90,00 %	103		
8	1	BK0142 oven rikkoaminen	10,00 %	40		
9	1	BK0142 seinän rikkoaminen	10,00 %	410		
10	1	Pakeneminen samaa kautta	10,00 %	25		

Tunkeutumisen keskeyttämisen vasteaika (s)	600
Vasteajan keskihajonta (s)	180
Tekniikan toimintavarmuus	90,00 %
Tunkeutumisen onnistuneen keskeytyksen todennäköisyys	**37,72 %**

Aputaulukko | Syöttötaulukko | Tulostaulukko | Raportti

Kuva 13 Tulokset BK0139 murtautumisyrityksestä Bk0142 seinän kautta

6 JOHTOPÄÄTÖKSET

Tässä luvussa käydään läpi erilaisia ratkaisuja, joilla voidaan parantaa oppimisympäristön ja datakeskuksen fyysistä turvallisuutta. Näiden ratkaisujen tarkoituksena on nostaa tunkeilijan murtautumisyrityksien hidasteaikoja ja samalla nostaa tunkeilijan havaitsemisen todennäköisyyttä niissä. Nämä ratkaisut perustuvat käytännön tutkimuksessa käytetyn TUREAN-työkalun avulla löytyviin fyysisiin heikkouksiin ympäristöstä.

6.1 Datakeskus

TUREAN-työkalun kautta tulkittiin, että paras läpikulkureitti datakeskuksen sisälle ilman suurta havainnoinnin riskiä olisi sen tiiliseinien kautta, varsinkin huoneen BK0136 kautta. Tämän heikkouden ehkäisemiseksi paras vaihtoehto olisi uusien seinien rakentaminen. Nämä uudet seinät tulisi olla rakennettu vahvemmasta materialista, kuten teräsbetonista. Kuvassa 6 olevassa taulukossa lukee, että teräsbetoniseinän läpimurtoaika kestää 35 sekuntia kauemmin, kuin tiiliseinän kanssa. On kuitenkin tärkeä huomauttaa, että tämä ei tarkoita, että kaikkien tiiliseinien ja teräsbetoniseinien läpimurtojen ajoilla tulee olemaan myös 35 sekunnin ero. Tämä johtuu teräsbetoniseinän

sisäänrakennetuista tukiraudoista, jotka tunkeilijan pitää katkaista siihen soveltuvalla työkalulla, kuten esimerkiksi betonisahalla tai voimapihdeillä. Tämä tarkoittaa, että toisin kuin tiiliseinän kanssa, tunkeilija ei voi yhtä yksinkertaisesti luoda reikää seinään esimerkiksi vasaralla ja kulkea sen läpi. Tämä voi mahdollisesti estää täysin joitain tunkeilijoita.

Toinen sisäänkäyntireitti datakeskukseen on sen oven kautta, jonka läpimurtautuminen on TUREAN-työkalun mukaan myös hyvin mahdollista. Sen L-1 Identity Solutions sormenjäljenlukija on hyvä tapa estää tunkeilijoita pääsemästä sisälle huomaamattomasti, mutta se voidaan ohittaa suoranaisesti murtamalla ovi työkalujen avulla. Tämän takia olisi hyvä idea vaihtaa myös oven vahvempaan malliin. Tämä voi olla esimerkiksi teräksestä tehty turvahuoneen ovi, joka voidaan rakentaa samanaikaisesti uusien seinien kanssa. Tämän kautta ovenkarmi voidaan suoraan kiinnittää teräsbetoniseinään, jolloin ovi on lukittu vahvemmin paikalleen.

Ovessa voi myös olla uppolukko, joka on yhdistetty sormenjäljenlukijaan tai muuhun sähköiseen lukkoon ja uppolukkoa ei voi aukaista ulkopuolelta ilman, että on saatu hyväksyntä sähköisiltä lukoilta.

6.2 Oppimisympäristö

Oppimisympäristön sisäisen alueen heikoimmat sisäänkäyntireitit ovat tutkimusten perustella kaikki ulkoikkunat, joita voidaan vahvistaa eri tavoin. Näiden ikkunoiden vahvistamisen kautta voidaan estää tai hidastaa varsinkin impulsiiviset murtautumiset, joissa tunkeilijalla ei ole mukana minkäänlaisia työkaluja. Niin kuin näkyy kuvassa 5 kampuksen pihalla lojuu monia raskaita esineitä, joita kuka tahansa voi käyttää murtautumisessa työkaluna ja siksi on erittäin tärkeää, että ympäristön ikkunat pystyvät kestää iskuja niiltä. Näiden avulla voidaan mahdollisesti vähentää murtautumisia, joiden syynä on ilkivallan aiheuttaminen koulua kohtaan. Näissä murtautumisissa tunkeilijan ei tarvitse päästä datakeskukseen, vaan hän haluaa aiheuttaa vahinkoa koululle missä tahansa luokassa, tai huoneessa, jossa hän on käyttäen samoja esineitä, joita hän otti pihalta.

Ikkunat voidaan vahvistaa aluksi turvakalvoilla, kuten Safetyset Oy:n myynnissä olevilla sirpalesuojakalvoilla. Nämä kalvot pystytään asentaa kaikkiin ikkunoihin ja luokan BK0128 ulko-oven lasiin, joka näkyy kuvassa 9. Ikkunoihin voidaan myös asentaa kalterit, jotka voivat estää tunkeilijan kiipeämästä sisälle rikotun ikkunan kautta. Nämä kalterit voivat olla esimerkiksi Pedelux Ab Oy:n tarjoamat alumiinista ja teräksestä tehdyt kiinteät kalterit.

Kummatkaan näistä suojausmenetelmistä eivät siis pysty estämään ammattilaista, joka tuo mukanaan kunnollisia työkaluja, mutta ne pystyvät estämään tai hidastamaan valmistautumattomia tunkeilijoita.

7 YHTEENVETO

Tutkimuksen tavoitteena oli löytää fyysisiä heikkouksia Xamkin Tieto- ja viestintätekniikan oppimisympäristöstä ja löytää niitä varten uusia turvallisuusmenetelmiä ja ratkaisuja. Oppimisympäristö tutkittiin läpikohtaisesti käyttäen TUREAN-Tunkeutumisreittianalyysia, jolla saatiin tietää eri murtautumisyrityksiin kuuluvat ajat ja kuinka todennäköistä oli niiden havainnointi.

Tämän työn teoriaosuudessa tutustuttiin TUREAN-malliin, jossa esitettiin mihin aiempaan menetelmään se perustuu ja mitä ohjelmaa se soveltaa toiminnassa. Mallista esitettiin myös käytännön esimerkki keksitystä murtoyrityksestä yksinkertaiseen ympäristöön. TUREAN-mallin lisäksi käytiin läpi yleisesti fyysistä tietoturvaa, jossa käytiin läpi eri tapoja, miten murtautuminen voi aiheuttaa vahinkoa yritykselle, tai henkilölle ja miten niitä vastaan voidaan yleisesti suojautua.

Käytännön tutkimuksessa käytiin läpi kaikki oppimisympäristön sisäänkäyntireitit paikan päällä ja laskettiin, kuinka kauan kestää tunkeilijalle päästä datakeskukseen käyttäen jokaista reittiä. Seuraavaksi analysoitiin TUREAN-mallin Excel-laskentakaavion avulla, kuinka todennäköistä on, että tunkeilija huomataan jokaisen murtautumisyrityksen aikana. Näistä testeistä saatiin tulokseksi monta esimerkkiä, joissa tunkeilija onnistui murtautumaan datakeskukseen ilman tai ennen kuin vastevoimat saapuvat kampukselle. Näiden testien lisäksi pohdittiin mahdollisia ratkaisuja tutkimuksen esittämien turvallisuusheikkouksien korjaamiseksi.

Käytännön tutkimuksen tulosten perusteella voidaan todeta, että johdannossa esitettyihin tutkimuskysymyksiin on vastattu. Tämä tarkoittaa, että opinnäytetyö on onnistunut.

Opinnäytetyöhön voidaan perehtyä myös teorian ja käytännön tutkimuksen mukaan. Teoriassa voidaan saada parempi ymmärrys TUREAN-mallista konseptina ja myös fyysisen tietoturvan ominaisuuksista. Käytännön tutkimuksessa taas saadaan hyvä esimerkki tutkimusmenetelmäanalyysista oikeassa ympäristössä, koska tutkimus on todettu onnistuneeksi. Täten tiedetään, miten tutkimus voidaan toteuttaa vaiheittain ja minkälaisia laskuja mallin Excel-laskentataulukkoon kuuluu. Tämä ennalta tiedetty tieto voidaan hyödyntää tulevissa kehitysprojekteissa.

Yksi mahdollinen kehitysprojekti olisi tutkia, kuinka kauan tutkimuksen hidasteiden läpimenossa oikeasti kestäisi eri työkalujen avulla, jotta ne saisivat lopullisen tuloksen. Kehityksessä voitaisiin myös käydä läpi hidasteet, jotka jäivät tutkimatta, kuten katot ja lattiat.

LÄHTEET

Aaltio-Marjosola, I. 1999. Casetutkimus metodisena lähestymistapana. Metodix. WWW-dokumentti. Saatavissa: https://metodix.fi/2014/05/19/aaltio-marjosola-casetutkimus/.[Viitattu 20.4.2022].

Bennett, H.A. 1977. EASI approach to physical security evaluation. Kansainvälinen atomienergiajärjestö. WWW-dokumentti. Saatavissa: https://inis.iaea.org/search/searchsinglerecord.aspx?recordsFor=SingleRecord&RN=8328658. [Viitattu 16.4.2022].

Cherry, K. 2021. What Is a Case Study? Verywell Mind. WWW-dokumentti. Saatavissa: https://www.verywellmind.com/how-to-write-a-psychology-case-study-2795722. [Viitattu 20.4.2022].

Eriksson, P, Koistinen, K. 2014. Monenlainen tapaustutkimus. Kuluttajatutkimuskeskuksen tutkimuksia ja selvityksiä. PDF-dokumentti. Saatavissa: http://hdl.handle.net/10138/153032 [Viitattu 20.4.2022].

Levine, S. 1978 Research Information Letter 0023, “EASI” Adversary Sequence Evaluation Model (Computer Graphics Version). United States Nuclear Regulatory Commission. Pdf-dokumentti. Saatavissa: https://www.nrc.gov/docs/ML1726/ML17261A004.pdf. [Viitattu 16.4.2022].

Mitä on fyysinen tietoturvallisuus? 2021. Seclion Oy. WWW-dokumentti. Saatavissa: https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus. [Viitattu 20.4.2022].

Peltonen, J. 2003. Tunkeutumisreittianalyysi, seminaariesitys. Powerpoint-esitys. Saatavilla: http://www.yhteisturvallisuus.net/download/TUREANseminaari.pps. [Viitattu 15.4.2022].

Rakenteellinen murtosuojaus III. 2017. Finanssiala. Pdf-dokumentti. Saatavissa: https://www.finanssiala.fi/wp-content/uploads/2017/12/Rakenteellinen20murtosuojaus20III.pdf. [Viitattu 17.4.2022].

Resolver, 2022. https://www.resolver.com/blog/physical-and-cybersecurity-defense-hybrid-attacks/. Päivitetty 16.3.2022. WWW-dokumentti. Saatavissa: https://www.resolver.com/blog/physical-and-cybersecurity-defense-hybrid-attacks/. [Viitattu 16.4.2022].

Saaranen-Kauppinen, A, Puusniekka ,A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto 5.5 Tapaustutkimus.Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L5_5.html. [Viitattu 20.4.2022].

Tirronen, H, 2003. Tietoturvan osa-alueet. WWW-dokumentti. Saatavissa: http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html. [Viitattu 16.4.2022].

Toimitilojen tietoturvaohje. 2013. Valtionhallinnon tietoturvallisuuden johtoryhmä. WWW-dokumentti. Saatavissa: https://docplayer.fi/1682308-Toimitilojen-tietoturvaohje-2-2013-vahti-valtionhallinnon-tietoturvallisuuden-johtoryhma.html. [Viitattu 16.4.2022].

Vilpas, P. 2013. Moniste. Metropolia Ammattikorkeakoulu Pdf-dokumentti. Saatavissa: https://users.metropolia.fi/~pervil/kvantsu/Moniste.pdf/. [Viitattu 14.5.2022].

Wadoud A.A, Adail A.S, Saleh A.A, 2017. Physical protection evaluation process for nuclear facility via sabotage scenarios. Aleksandrian yliopisto. Pdf-dokumentti. Saatavissa: https://www.researchgate.net/publication/314017463_Physical_protection_evaluation_process_for_nuclear_facility_via_sabotage_scenarios. [Viitattu 16.4.2022].

KUVALUETTELO