TARTU ÜLIKOOL
Loodus- ja täppisteaduste valdkond
Arvutiteaduse instituut
Informaatika õppekava

Hjalmar Vaiküll

Andmeturbe kursuse praktikumimaterjalide värskendamine ja täiendamine

Bakalaureusetöö (9 EAP)

Juhendaja: Alo Peets, MSc

Tartu 2025

Andmeturbe kursuse praktikumimaterjalide värskendamine ja täiendamine

Lühikokkuvõte

Kübermaastiku kiire muutumise tõttu on tarvis tagada küberturvalisust käsitlevate õppematerjalide asjakohasus ja toimivus. Bakalaureusetöö raames värskendati ja täiendati Tartu Ülikooli kursuse LTAT.06.002 „Andmeturve“ praktikumimaterjale, mida sooritab igal aastal üle 300 tudengi. Lõputöö eesmärk oli testida ja kaasajastada õppeaine kõigi 15 praktikumi juhendeid ja seonduvaid ressursse nagu virtuaalmasinad, veebirakendused, praktilised testid ja hindamisjuhend. Lõputöö olulisemate saavutustena võib välja tuua 4 värskendatud eelseadistatud virtuaalmasinat, 3 automaathinnatavate praktiliste harjutustega Moodle'i testi, mitmete juhendis kasutatud tarkvarade ja nende konfiguratsioonifailide kaasajastamist ning kõigi juhendite sisu ja väljanägemise läbivat uuendamist. Töö kirjalikus osas kirjeldatakse kõiki praktikumidega seotud tegevusi üksikasjalikult ning tuuakse välja tehtud uuenduste ja täienduste põhjendused.

CERCS teaduseriala: P175 Informaatika, süsteemiteooria

Märksõnad: andmeturve, küberturvalisus, õppematerjalid, testimine, uuendamine, täiendamine, virtuaalmasinad

Renewing and updating Computer Security course lab materials

Abstract

Due to the rapidly evolving cyber landscape, it is essential to ensure the relevance and effectiveness of educational materials related to cybersecurity. As part of this bachelor's thesis, the lab materials for the University of Tartu course LTAT.06.002 "Computer Security", which is taken by over 300 students annually, were updated and enhanced. The goal of the thesis was to test and modernize all 15 lab guides and associated resources, such as virtual machines, web applications, practical tests and the grading guide. Key achievements of the thesis include the update of 4 preconfigured virtual machines, the creation of 3 Moodle quizzes with automatically graded practical tasks, modernization of various software tools and their configuration files, and a comprehensive overhaul of the content and layout of all lab guides. The thesis provides a detailed description of all activities related to the practicals and explains the reasoning behind the updates and improvements made.

CERCS: P175 Informatics, systems theory

Key Words: data security, cybersecurity, educational materials, testing, renewing, enhancing, virtual machines

Sisukord

Sissejuhatus

Kaasaegses maailmas ei ole võimalik koolitada pädevaid IT-spetsialiste küberturvalisuse valdkonda käsitlemata. Aina keerulisemate infotehnoloogiliste lahenduste keskel on turvalise käitumise vajalikkus aastatega üha enam kasvanud. Seetõttu on Tartu Ülikooli informaatika bakalaureuseõppekava kohustuslikus IT erialamoodulis õppeaine „Andmeturve“ (ainekoodiga LTAT.06.002), mida läbib iga-aastaselt ligikaudu 300 tudengit, et omandada alusteadmised turvalisest arvutikasutusest töövahendina ja käitumisest küberruumis.

Kübermaastiku kiire muutumise tõttu on oluline üle vaadata varasematel aastatel loodud õppematerjalid, veendumaks nende toimivuses ja kaasajastamaks neid vastavalt muutunud oludele. Seda kinnitab ka Riigi Infosüsteemi Ameti (RIA) peadirektori asetäitja küberturvalisuse alal, Gert Auväärt: „Kümme aastat tagasi ei osanud keegi karta, et küberkuritegevus võtab sellised mastaabid – praeguseks on tegu maailma suuruselt kolmanda *majandusega* USA ja Hiina järel. Oleme jõudnud ajajärku, kus igaüks – olgu ta üksikisik, ettevõte või riik – peab vaatama küberturvalisust ühe esmavajadusena“ [1, lk 6]. Seetõttu on tarvis värskendada ja vajadusel täiendada ka Andmeturbe kursuse praktikumides kasutatavaid materjale, et need vastaksid muutunud aja nõuetele.

Kursus koosneb kahest osast: praktiline ja teoreetiline. Bakalaureusetöös keskendutakse ainult kursuse praktilisele osale, mis koosneb 15 praktikumist. Iga praktikumi täieliku sooritamise eeldatav ajamaht on 4 tundi, mille jooksul tutvutakse käsitletavate teemadega, praktiseeritakse õpitut ning lahendatakse hindelisi ülesandeid. Õppeaine auditoorsetes praktikumides kohalolu ei kontrollita, vaid iga praktikumi sooritusse tõestuseks esitatakse lahendused Moodle'i õpikeskkonda, mida hindavad nii automaatkontrollid kui ka kursuse õppejõud.

Praktikumi ülesannetes kasutatakse mitmeid päriselulisi Tartu Ülikooli IT-süsteeme, mis on pidevas uuenemises. Mitmete tarkvarade paigaldamine on internetipõhine (näiteks APT tarkvarahalduse tööriist), mistõttu on tarvis iga aasta kontrollida praktikumijuhendite ja -materjalide toimivust sel hetkel aktiivsete versioonidega. Täiendavalt on mitmete süsteemide, nagu näiteks Linuxi tuuma, kestustuge (ingl *long-term support*) vähendatud paariaastaseks [2] ning kestus-

toeta versioonide aega kuni paarikuuseks [3], mis sunnib süsteemid välja vahetama varasemast tihemini. Pea igapäevaselt muutuvas küberruumis [4] pole ka tavatu, et materjalides peab muudatusi sisse viima semestri käigus peale materjalide esmast avalikustamist.

Bakalaureusetöö eesmärk on Andmeturbe kursuse praktikumimaterjale läbivalt testida, värskendada ajale vastavaks, täiendada või koostada uusi juhendeid ja ressursse, ning luua õppejõude abistavaid materjale.

Bakalaureusetöö koosneb kahest osast:

1. kursuse tutvustus ja murekohad, kus kirjeldatakse kursuse ülesehitust, õpiväljundeid ja -eesmärke, sõnastatakse probleemid ning tuuakse välja lõputöö eesmärgid, mille tulemusena peaksid probleemid lahenema või leevenema;

2. praktiliste tegevuste kirjeldus, kus selgitatakse detailselt iga praktikumi tegevusi ja eesmärke, tehtud värskendusi ja täiendusi, kõikide kasutatavate virtuaalmasinate loomisprotsessi ning loodud abistavaid materjale.

Mõisted ja terminid

Agent on esindaja või vahendaja kontekstist sõltuvas tähenduses[1].

ARP-pete (ingl *ARP spoofing*) on rünne, mis põhineb protokolli ARP nõrkustel, püüab siduda ründaja MAC-aadressi ründe sihtmärgi IP-aadressiga, et suunata endale selle sõlme liiklus[1].

Brauserikook (ingl *cookie*) on väike fail, mis salvestatakse kasutaja veebimällu olekuteabe hoiuks, kasutajate identifitseerimiseks ja toimingu sidususeks[1].

CTF ehk *Capture-the-flag* on levinud kübervõistluste formaat, kus osalejad peavad lahendama ülesandeid erinevate päris-eluliste turvanõrkuste kohta[2].

Digitaalsertifikaat on elektrooniline dokument, mis seob kasutaja avaliku võtme kasutajat identifitseerivate andmetega[1].

Distributiiv, distro on tarkvarakomponentide kogumi versioon, mis on funktsioonidelt terviklik[1].

HTTPS (ingl *Hypertext Transfer Protocol Secure*) on võrgu rakenduskihis töötava veebiprotokolli HTTP ja transpordikihi protokolli SSL/TLS kombinatsioon, mis loob turvalise krüpteeritud kanali läbi ebaturvalise võrgu[1].

IPv4 (ingl *Internet Protocol version 4*) on IP protokolli neljas versioon, millel praegu põhineb Internet. IPv4 aadressid koosnevad neljast omavahel punktidega eraldatud kümnendarvust[3].

IPv6 (ingl *Internet Protocol version 6*) on IP-protokolli versioon 6, tugevaim pretendent asendamaks juba alates 1981. aastast kasutusel olevat IP-protokolli IPv4. IPv6 peamiseks eesmärgiks on lahendada IP-aadresside defitsiidi probleem ning sellel on 8-rühmalised 128-bitised aadressid ja tugevam andmeturve[3].

Jõurünne (ingl *brute-force-attack*) on parooli, krüptovõtme vm salajase mõistatamine kõiki võimalikke väärtusi läbi proovides[1].

[1] AKIT. Andmekaitse ja infoturbe portaal. https://akit.cyber.ee/.
[2] CTF101. What is a CTF? https://ctf101.org/intro/what-is-a-ctf/ (14.06.2025)
[3] e-Teatmik: IT ja sidetehnika seletav sõnaraamat. http://www.vallaste.ee.

Kahjurvara (ingl *malware*) on vahend infosüsteemi töö või kasutaja otseseks või kaudseks kahjustamiseks, häirimiseks[1].

Klahvinuhk (ingl *keylogger*) on liik nuhkvara, mis talletab salaja kasutaja klahvivajutusi ja muid sisestustoiminguid[1].

Ohusubjekt on olem (isik või organisatsioon, sisemine või väline), kes osaleb toimingutes, mis tekitavad organisatsiooni turvalisust ohustava või ohustada võiva sihiliku või tahtmatu intsidendi[1].

Otspunktkrüpteerimine (ingl *end-to-end encryption*) on andmete krüpteerimine nende edastamiseks nii, et nad läbivad võrku krüptogrammina, kuid marsruutimisteave jääb nähtavaks[1].

Port on interneti protokollides TCP- või UDP-ühenduse loogilise kanali otspunkt[1].

Pimeveeb (ingl *dark web*) on Interneti üks pealisvõrke, mis ühendab veebisaite, on avalikult nähtavad, kuid varjavad neid majutavate serverite IP-aadresse, seega ka majutajaid[1].

Räsi (ingl *hash*) on püsipikkusega sõnumilühend, mis on andmetest saadud räsifunktsiooni abil, ühesuunalise krüpteerimisega, st pöördumatu tihendusega[1].

Skript on väike kompileerimata käsujada, mida kasutaja sekkumiseta interpreteerib või täidab teine programm, mitte vahetult arvuti protsessor[1].

Seansikaaperdus (ingl *session hijacking*) on rünne, mis põhineb protokolli nõrkustel: eelnevalt on loodud seaduslik sideühendus, mille seansi identifikaatori saab ründaja koogist või URList ja teeskleb lubatavat kasutajat[1].

SSH (ingl *Secure Shell*) on protokollisari, mis võimaldab turvalist krüpteeritud kaugpöördust[1].

Sõnastikrünne (ingl *dictionary attack*) on krüptosüsteemi rünne, mis rakendab otsingut mingis etteantud parooliloendis ja võib kasutada salvestatud paroolivääртuste loendit või loomuliku keele sõnastikku[1].

Transpordikihi turbeprotokoll (ingl *transport layer security*) ehk TLS on protokoll selliste andmete krüpteerimiseks, mida edastatakse rakenduste vahel ebaturvalise võrgu kaudu[1].

Troojan (ingl *trojan*) on liik kahjurvara, varjatud kood näiliselt kasulikus programmis, seahulgas

viirusetõrjeprogrammis, mille ründefunktsioonid võimaldavad enamasti kaugpöördust kasutaja arvutisse ja sealt andmete väljasaatmist[1].

Tulemüür (ingl *firewall*) on turvatõke võrgukeskkondade vahel eraldi seadmena või mitme komponendi ja meetodi ühendina, mille kaudu kulgeb kogu liiklus mõlemas suunas ühest võrgukeskkonnast teise ning läbi lastakse ainult lubatav liiklus, mis on määratletud kohaliku turvapoliitikaga[1].

Tunneldus (ingl *tunneling, port forwarding*) on ühe protokolli järgi struktureeritud andmete edastus teise protokolli vormingus, mis võimaldab ühel võrgul edastada andmeid teise võrgu ühenduste kaudu[1].

Uuend (ingl *update*) on olukorrast sõltuv süsteemi muutev programmikood, näiteks nõrkuse kõrvaldamiseks: parandus, paik, versioonitäiend, konfiguratsioonimuudatus[1].

Vahendusrünne (ingl *man-in-the-middle attack*) on suhtluspoolte teabevahetust manipuleeriv rünne[1].

Vastukest, tagasiühendav kestakood (ingl *reverse shell*) on kaugkestakood, mis loob ründeks ühenduse ohvri arvutilt ründaja arvuti kuulavale pordile[1].

Virtuaalmasin on tegeliku või hüpoteetilise arvuti arhitektuuri ja funktsioonide emuleering[1].

1 Kursuse tutvustus ning murekohad

Järgnevates alampeatükkides kirjeldatakse LTAT.06.002 Andmeturve kursuse õppe-eesmärke ja ülesehitust. Lisaks tuuakse välja bakalaureusetöö eesmärkide püstitused, mille põhjal hilisem praktiline töökäik on üles ehitatud.

Kursust[4] puudutav ametlik info on leitav arvutiteaduse instituudi õppeainete veebirakendusest *Courses*[5] ning Tartu Ülikooli õppeinfosüsteemi veebirakendusest *ÕIS II*[6].

1.1 Õppeaine Andmeturve kirjeldus

Kursuse LTAT.06.002 Andmeturve eesmärk on anda kuulajale arusaam tänapäeva küberturbe probleemidest ning nende lahendamise viisidest. Kursuse läbimisel omandatakse selge arusaam küberturbe eesmärkidest ja vajadusest ning ohtudest ja riskianalüüsist. Omandatakse teadmised autentimisest, turvamudelitest, võrguturbest, krüptograafia rakendamisest, pahavarast, turvalisest programmeerimisest ning andmeturvet puudutavast seadusandlusest. Omandatakse praktilised kogemused võrguturbest ning andmeturbe teemal eneseväljendamisest. [5]

Õppeaine käigus antakse ülevaade küberturbe probleemidest (turvaeesmärgid, ohud, riskianalüüs, turvapoliitika, turbestrateegiad). Lähemalt käsitletakse autentimismeetodeid, juurdepääsukontrolli mehhanisme, UNIX'i ja Windowsi turvaarhitektuuri, võrguturvet (tulemüürid, virtuaalsed privaatvõrgud), krüptograafia rakendusi, turvalist programmeerimist (C, PHP, SQL jms), rünnakute avastamist, pahavara, seadusandlust ning privaatsust ja anonüümsust. [5]

Kursus on õpiväljundite poolest jagatud kaheks eraldiseisvaks osaks: praktiline ja teoreetiline. Kummastki osast tuleb omandada positiivse hinde saamiseks vähemalt 50% õpiväljunditest. Kursuse läbimiseks on kõik aine kuulajad kohustatud lahendama praktikumides praktilisi küberturbealaseid harjutusi. Kokku on aines 15 praktikumi, millest igaühele võiks tudeng keskmiselt kulutada umbes 4 tundi. Iganädalaselt on tudengitel võimalus osaleda kahetunnises auditoorses

[4] Lõputöö vältel kasutatakse väljendeid *kursus* ja *õppeaine* samatähenduslikena.
[5] Andmeturve, kevad 2025. https://courses.cs.ut.ee/2025/turve/spring/Main/HomePage.
[6] Andmeturve (6 EAP), LTAT.06.002. https://ois2.ut.ee/#/courses/LTAT.06.002/details.

praktikumis, kus saab küsida praktikumijuhendajatelt abi ja täiendavaid seletusi ülesannete lahendamiseks. Praktikumides kohalkäimist ei kontrollita, kuid iga praktikumi lõpus tuleb esitada tõestus materjalide eduka läbimise ja harjutuste lahendamiste kohta *moodle.ut.ee* keskkonda. Iga praktikumi eest saab tudeng teenida kuni 4 punkti, mis teeb kokku 60 punkti (60%) aine lõpphindest.

Aine vastutaval õppejõul Alo Peetsil on veendumus, et küberturvalisuse tõustes süsteemi kasutusmugavus väheneb. Näiteks kaksikautentimise (ingl *two-factor authentication*) kasutamisel on vaja lisaks paroolile omada täiendavat autentimisvahendit, mille haldamine on lisakohustus. Samuti on ta veendunud, et inimesed on loomu poolest laisad ja enamik neist ei ole vabatahtlikult nõus oma mugavast ebaturvalisest arvutikasutusest loobuma. Seetõttu on ta aine praktikumid koostanud eesmärgiga, kus läbi häkkimise näidatakse, kui kerge on ohvriks langeda. Seejärel on aine kuulajad oluliselt vastuvõtlikumad turvalise käitumise püsivale omandamisele. Seega algavad praktikumid enamasti näidisrünnetega ja lõppevad turvalise käitumise näidetega. Praktikumide teemadega saab tutvuda jooniselt 1.

LTAT.06.002 Andmeturve praktikumid – courses.cs.ut.ee

Kuidas rünnata? - Häkkimine	Kuidas kaitsta? - Küberturvalisus
Linuxi masinasse parooli teadmata sisenemine (*edit grub*)	Andmete krüpteerimine Linuxi keskkonnas (*veracrypt*)
Windows masinasse parooli teadmata sisenemine ja andmetele ligipääs (*edit SAM, sticky keys*)	Operatsioonisüsteemi ja seal olevate andmete krüpteerimine (*Bitlocker*)
Teise isiku nimel e-kirja saatmine (telnet mail.ut.ee 25)	Küberhügieenitest, turvaline e-mail ja sõnumivahetus (Signal)
Levinud paroolide katsetamine veebilehele sisselogimiseks (*OWASP ZAP proxy , parooli räsi*)	Paroolihalduri ja turvaliste paroolide kasutamine (*KeePass, haveibeenpwned.com*)
Võrguliikluse pealtkuulamine (*Man In the Middle rünne, arp spoofing*) TÜ kasutajatunnuse lekkimise näide (*SSH*)	Ühenduste signeerimine, masin-masin autentimine sertifikaatidega (*RootCA, isikusertifikaat, fingerprinting*)
Seansikaaperdus küpsiste näitel (*kuidas sisse logida kasutajatunnust ja parooli omamata*), *cookie stealing*	Administraator saab kõike teha arvutis, **põhikasutajal EI TOHI olla administraatori õigusi**
Liba veebilehed ja nende tuvastamine	Kuidas tuvastada, et veebileht on legitiimne (*sertifikaadid*)
Avatud portide (*turvaaukude*) otsimine (tulemüür)	*Local Port Forwarding (LPF) ja Remote Port Forwarding (RPF)*
Kuidas pahavara ennast sinu arvutis käima paneb	Pahavara otsimise näited (*autoruns, Process Explorer*)
Kali + metasploit framework abil pool-automatiseeritud võrguründed uuendamata arvuti vastu	Tulemüüri seadistamise näited (*Windows Firewall*), Operatsioonisüsteemi uuendamise vajalikkuse illustreerimine
"*Viirusega*" faili loomine	Viirusetõrje kasutamine (*virustotal.com pahavara analüüs*)
Jälgede ajamine (*forensics*), Kuidas sa vahele jääd?	Kuidas enda jälgi kustutada, **iga tegevus jätab endast jälje**

Joonis 1: LTAT.06.002 Andmeturbe kursuse praktikumide teemade ülevaade.

Õppeaine teoreetiline pool koosneb kolmest alamosast: 10 Moodle'i testi loenguteemade kohta, referatiivne uurimustöö ühe konkreetse turvaaugu kohta ja kirjalik auditoorne eksam aine lõpus. 2025. aasta kevadel on aine vastutavaks õppejõuks Alo Peets, kes ühtlasi vastutab aine praktilise poole eest. Aine peamine loengupidaja on hetkel Tarmo Oja, kes ühtlasi tegeleb aine teoreetiliste harjutuste koostamise ja hindamisega.

Alates 2024. aasta kevadest on kursus suunatud just informaatika bakalaureuse esmakursuslastele, mitte enam teise ja kolmanda kursuse tudengitele nagu varasematel aastatel. Seetõttu on kursuse õpetamisel veel üleminekuperiood, kuna 2025. aastal on õppeaine kuulajate seas nii esimese kui ka vanemate kursuste informaatika bakalaureuse tudengeid.

1.2 Eesmärgid

Aitamaks suunata kursuse arendusprotsessi õiges suunas, on tarvilik sõnastada eesmärgid, mille põhjal materjalide värskendamine ning täiendamine läbi viiakse. Eesmärgid on paika pandud tulenevalt õppeainega seotud probleemidest, kursuse õppejõudude[7] soovidest, lõputöö autori enda nägemustest ning õppeaine muutmisest esimese aasta tudengitele suunatuks.

Lõputöö üldised eesmärgid on järgnevad:

1. Tagada kõikide praktikumidega seotud materjalide toimivust läbi põhjaliku testimise.
2. Kaasajastada kõik praktikumides kasutatavad operatsioonisüsteemid, tarkvarad, abisüsteemid ja tööriistad.
3. Luua abistavad materjalid õppejõududele iga praktikumi ja nendega seonduvate süsteemide ülesseadmiseks.
4. Vajadusel koosatada uusi praktilisi harjutusi olemasolevate asendamiseks, täiendamiseks või kaasajastamiseks.

Praktiliste tegevuste peatükis selgitatakse lisaks tegevustele ka praktikumispetsiifilisi eesmärke. Seeläbi saadakse aimu, mida arendusprotsessi käigus saavutada sooviti.

[7] Lõputöö autor on samuti 2024/2025. õppeaastal kursuse praktikumijuhendaja.

2 Praktiliste tegevuste kirjeldus

Käesolevas peatükis kirjeldatakse lõputöö praktilisi tegevusi ning nendega seonduvaid ressursse. Kuna tegemist on lõputöö kõige mahukama peatükiga, siis on see jaotatud kaheks alampeatükiks: (1) praktikumimaterjalide loomine ja täiendamine, (2) virtuaalmasinate loomine. Peatüki eesmärk on anda aimu lõputöö autori praktilise töö mahust ja keerukusest, mis on 2025. aastal Andmeturbe kursuse raames tehtud.

2.1 Praktikumimaterjalide värskendamine ja täiendamine

Alampeatükis käsitletakse praktikumimaterjalide värskendamise ja täiendamise protsessi iga praktikumi kohta eraldi. Välja tuuakse iga praktikumi eesmärk ning lühikirjeldus tehtavatest tegevustest, mille käigus selgitatakse tehtud muudatusi ja täiendusi. Täiendavalt loodi tabel, kus on toodud välja lõputöö käigus tehtud uuendused, muudatused ja täiendused iga praktikumi kohta (vt tabel 1). Iga praktikumi tegevustele on eelnenud põhjalik testimine, mida tabelis eraldi välja ei tooda.

Tabel 1: Praktikumides tehtud tegevused

	Praktikum	**Tegevused, muudatused, täiendused**
1.	Sissejuhatus töökeskkonda	Linux Mint virtuaalmasina loomine, boonuspunktide tabeli loomine, juhendite vormistuse malli loomine
2.	Paroolide murdmine	Praktikumi viimine Moodle'i testi vormi, küsimusi automaatselt loovate skriptide tegemine, Crypt teegi asendamine OpenSSL teegiga, jõuründe veebilehe uuendamine
3.	OpenSSL & sertifikaadid	Kohandatud openssl.cnf uuendamine, kuvatõmmiste uuendamine
4.	Windowsi ründed	Windows 10 virtuaalmasina loomine ja seadistamine, boonuspunktide tabeli loomine
5.	Andmete kaitsmine VeraCrypt & Bitlocker näitel	Silmaringi ülesannete lisamine, Veracrypt uuema versiooni kasutusele võtmine

6.	Turvaline suhtlus	Liba e-kirja konto ning mitmete problemaatiliste ülesannete eemaldamine, turvatud e-kirja saatmise ülesande lisamine, Signal konto ja numbri uuendamine, libakirjade ja -sõnumite analüüs, küberhügieeni kursuse ülesande lisamine
7.	SSH kasutamine & turvalisus	SSH kaugühenduse masina ülesseadmine, tunnelduse ülesannete situatsioonikirjelduste lisamine
8.	Võrguliikluse pealtkuulamine	Telnet konfiguratsiooni uuendamine, ssh-mitm programmi errorite eemaldamine
9.	Kahjurvara & Windows forensics	Varasema Windows XP virtuaalmasina täiustamine, vajalike tööriistade lisamine
10.	Tulemüür, iptables, nmap & IPv6	IPv6 materjalide lisamine, IP-aadresside analüüs, asukoha määramise praktilise ülesande loomine, kuvatõmmiste uuendamine
11.	Veebirakenduse turvalisus & WebGoat	WebGoat uuendatud versiooni kasutusele võtmine, PDF-vormingu nõudmine
12.	E-ITS (Eesti Infoturbestandard)	Moodle'i testi varieeruvate küsimuste loomine ja täiendamine, testi mahu ja kaalu suurendamine
13.	Turvaaukude ärakasutamine	Tiny11 operatsioonisüsteemi kasutusele võtmine, reverse shell ülesande loomine, pahavara loomise ülesande uuendamine, pahavara pildifailiks maskeerimise ülesande loomine, IPv6 abil teenusetõkestuse ründe ülesande loomine
14.	ID-kaart & e-hääletamine	Praktikumijuhendi info uuendamine
15.	Küberturbe harjutused enesekontrolliks	Moodle'i kordamistesti kasutusele võtmine, praktilise suunitlusega automaatkontrollitavate küsimuste loomine

Kogu kursuse vältel loodi õppejõude abistavaid materjale nagu praktikumide ülesseadmise ju-

hendid, *Courses* keskkonna praktikumijuhendite mall ning hindamisjuhendi koostamine igale praktikumile. Lõputöö jooksul abistavaid materjale ei käsitleta, kuid nende osalised näidised on leitavad lõputöö lisade seast (vt lisa 1).

Täiendavalt soovitatakse tehtud tegevuste mõistmiseks tutvuda õppeaine 2025. aasta praktikumijuhenditega: *Praktikumid 2025*, https://courses.cs.ut.ee/2025/turve/spring/Main/Praktikumid.

2.1.1 Praktikum 1 - Sissejuhatus töökeskkonda

Esimese praktikumi eesmärk on valmistada tudengid ette järgnevateks praktikumideks nii töökeskkonnalt kui ka eelteadmistelt. Praktikumi jooksul paigaldatakse virtualiseerimistarkvara VirtualBox[8] ja eelvalmistatud Linux Mint virtuaalmasin, millele on õppejõud loonud kasutaja, kuid pole tudengitele täpsustanud selle parooli. Ülesanneteks on asendada imporditud virtuaalmasina kasutaja parool virtuaalmasinasse sisse logimata ning lahendada Linuxi käskude harjutamise ülesandeid.

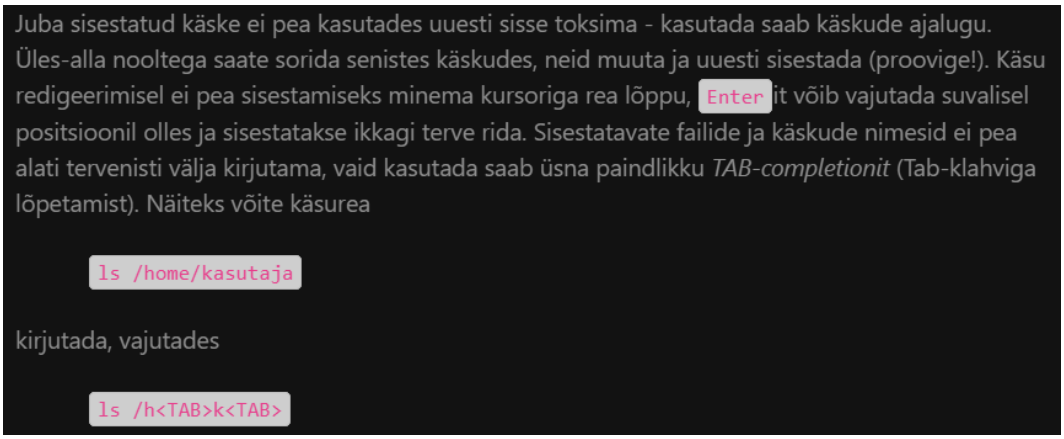
Praktikumi ettevalmistamisel loodi Linux Mint virtuaalmasin ja testiti sellega juhendis tehtavaid tegevusi. Samuti lisati virtuaalmasinasse n-ö *peidetud boonuspunktid*. Kursuse üldine tava on peita kasutatavate masinate sisse faile, kohandatud sätteid või sündmusi, mille avastamisel on tudengitel võimalik teenida õppejõududelt boonuspunkte. Need on paigutatud virtuaalmasinates üldjuhul turvalisusega seotud kohtadesse nagu süsteemi- ja konfiguratsioonifailid, mis innustavad tudengeid süsteemiga tutvuma. Lõputöö raames loodi erinevaid boonuspunktide lahendusi ning kaardistati need eraldi tabelisse. Tabel annab tulevikus ülevaate varasemalt kasutatud boonuspunktidest ning läbi selle on võimalik neid aastati vahetada, et takistada nende levimist tudengite vahel.

Praktikumijuhendis tutvustatakse erinevaid Debianil baseeruvaid Linuxi käske ja võimalusi. Kuna tegemist on sissejuhatava praktikumiga, mille eesmärk on Linuxi operatsioonisüsteemi oskuste ja teadmiste ühtlustamine, siis on juhend pigem tehniline kui praktiline. Tudengitelt eeldatakse baasoskusi Linuxi operatsioonisüsteemidega, kuna kursuse üks eeldusaineid on LTAT.06.001

[8] Oracle VirtualBox. https://www.virtualbox.org/ (02.05.2025)

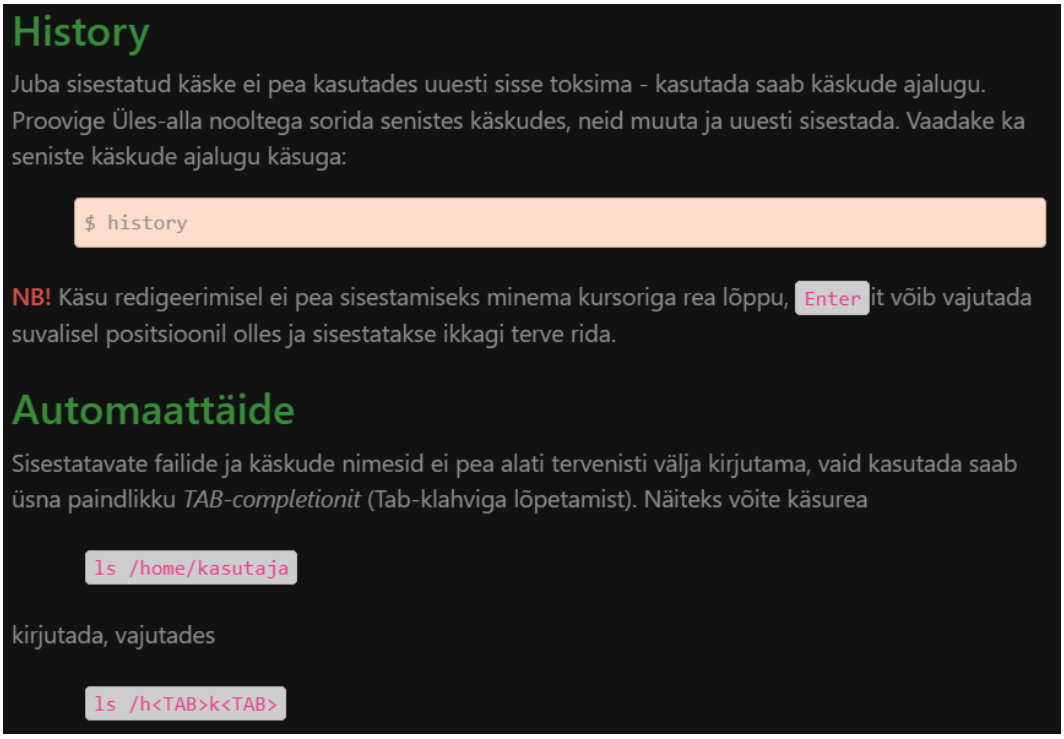
Operatsioonisüsteemid, kus keskendutakse UNIX-tüüpi operatsioonisüsteemide õpetamisele ja kasutamisele [6].

Praktikumijuhendi põhjal tegevuste läbi testimisel selgines juhendi vormistuse tähtsus. Alampeatükis *Linuxi käsurea meeldetuletus* käsitletakse erinevaid käske, tekstiredaktoreid, käsurea parameetreid, kiirklahve jpm, mille järjestikune vormistus juhendis muutis teemade käsitluse segaseks (vt joonis 2).



Joonis 2: Katkend 2024. aasta praktikumijuhendist.

Lugemise hõlbustamiseks eraldati alampeatükis käsitletav info teemadeks. Muudatuse eesmärk oli muuta juhend arusaadavamaks ning soodustada info otsimist. Samuti lisati juhendisse juurde käske, mis võivad tudengeid edasiste praktikumide jooksul aidata (vt joonis 3).



Joonis 3: Katkend 2025. aasta eraldatud teemadega praktikumijuhendist.

Esimese praktikumi juhendi vormistamise käigus loodi vastav mall, mis sisaldab erinevaid juhendites kasutatud komponentide vormistuse näiteid (vt lisa 1, joonis 21). Mall oli etaloniks kõigi järgnevate praktikumide vormistuse ja ülesehituse paika seadmisel, et kõik juhendid oleksid visuaalselt sarnased. Malli on lisatud ka lühikirjeldused iga komponendi kasutusalade kohta.

2.1.2 Praktikum 2 - Paroolide murdmine

Teise praktikumi eesmärk on anda ülevaade paroolide turvalisusest, näidata kui lihtne neid on murda ning kuidas paroolidega turvaliselt ümber käia. Ülesannete käigus asendatakse kasutaja salasõna räsi muutmise abil, murtakse lihtsamaid soolatud parooliräsisid, viiakse läbi sõnastiku- ja jõurünne ning tutvutakse paroolihaldustarkvaradega.

Arvestuslike ülesannete lahendusi tõestatakse kursuse vältel enamasti kuvatõmmistega, kus on üldjuhul märgiseid, mille abil on võimalik tuvastada lahenduse autorit. Näiteks on Joonas Ha-

lapuu loodud esimese praktikumi Linuxi käsurea keskkonnas näha lahendaja nime ja matriklinumbrit, mis palutakse arvestust tõestava kuvatõmmise peal esile tuua [7, lk 24]. Paraku on osade ülesannete puhul raske luua autorile viitavaid märgiseid, mistõttu on nende esituste autentsuse tõestamine raskendatud.

Teise praktikumi seni suurim mure oli parooliräside murdmise ülesande vastuste samasus. Varasemalt oli võimalik teenida neljandik praktikumi punktide mahust 6 parooliräsi murdmisega isevalmistatud Pythoni koodi abil (vt joonis 4), mille korrektsed vastused olid kõigil identsed. Seetõttu ei olnud võimalik vastuste pealt lahenduste autentsust tõestada, mis soodustas tudengite seas vastuste jagamist.

- **Ülesanne 1a**: Modifitseerige programmi otsima 2, 3 ja 4-täheliste DES paroolidega ning leidke paroolid (DES puhul 2 esimest tähemärki on sool näiteks "aa" esimese räsi korral, paroolide pikkused on vastavalt 2, 3, 4 tähemärki):

```
aaYnY9JY1skVY
abpNtJ15XGZyU
XZkMWgaNMr552
```

- **Ülesanne 1b**: Modifitseerige programmi otsima 2, 3 ja 4-tähelisi paroole ning leidke paroolid, mis vastavad räsidele:

```
$1$SoolSalt$6kodg6UCOHV2owr1QxUX60
$5$Andmeturve$aRN3yaCA0QP4tgVRUF6u8NxZS7o.OD2gAoSzj66wyS1
$6$SomethingHere$L5zuxicIHC90jGVZ9xgoOjUw36DjduwH1nPGJ.uwcgLqCvhlGe6wWp55eojE9jAIXxDbcsmbAKLXuXg2AbKZo0
```

Joonis 4: Varasema aasta 2. praktikumi fikseeritud parooliräsid.

Lisaks kasutatakse praktikumis jõuründe demonstreerimiseks Java Spring Boot[9] raamistikul põhinevat lokaalset veebilehte, kuhu olid senini sisestatud kursusel osalevate tudengite matriklinumbritele põhinevad kasutajad ning nendele vastavad juhuslikud salasõnad 10 000 levinud parooli andmestikust. Veebilehe eelloomisel oli iga-aastaselt põhiprobleemiks kursusele hilinemisega teisel nädalal registreerinud tudengid. Seetõttu pidi lokaalse veebilehe looma võimalikult hilja, et hiljem liitunud tudengite kasutajad saaksid veebilehe andmebaasi lisatud.

Mõlema eelnevalt kirjeldatud probleemi lahendusena nähti ülesannete viimist Moodle'i testi vormi, kus iga tudeng saab testi alustamisel juhuslikud parooliräsid ja kasutajakontod. Seetõttu loodi lõputöö käigus Moodle'i test, kus on kokku 9 küsimust. Küsimused moodustavad kokku neli suuremat ülesannet:

[9] Spring Boot. https://spring.io/projects/spring-boot (07.05.2025)

1. soolatud parooliräside murdmine;
2. sõnastikründega paroolide leidmine;
3. lokaalse Java veebilehe paroolide leidmine jõurünnetega;
4. KeePass2 paroolide andmebaasifaili esitamine.

Kõik testi ülesanded peale neljanda on automaatkontrollitavad, mille abil suudeti vähendada praktikumi esituste kontrollile kuluvat aega enam kui poole võrra. Kõik testi automaatkontrollitavad küsimused on genereeritud Pythoni skriptide abil, mis loodi lõputöö käigus. Järgnevalt kirjeldatakse olemas olnud praktikumi ülesandeid detailsemalt ning skripte, mis testi küsimusi automaatselt loovad.

Esimeses ülesandes on vaja leida viis erinevat parooli, mis on soolatud ja räsitud kas DES, MD5, SHA-256 või SHA-512 räsimisalgoritmidega. Ülesande parooliräsid genereeriti ingliskeelse tähestiku suvaliste tähemärkide kombinatsioonidest, millele lisati soolad. Skriptid kirjutavad kõik testi küsimused automaatkontrollitavas lühivastuse formaadis, kuhu on vaja esitamisel kirjutada dekrüpteeritud parool (vt joonis 5). Kokku loovad skriptid automaatselt 500 erinevat 2- kuni 4-kohalist parooliräsi iga räsimisalgoritmi kohta (vt joonis 6). Seega on küsimustepangas kokku 2000 taolist küsimust.

```
def write_to_file(filename, entries, hash_type):
    with open(filename, "w") as file:
        for i, entry in enumerate(entries, 1):
            if hash_type == 'DES':
                vihje = "2-4 "
            elif hash_type == 'MD5':
                vihje = "4-"
            elif hash_type == 'SHA-512':
                vihje = "2-"
            elif hash_type == 'SHA-256':
                vihje = "3-"
            file.write(f"::{hash_type.upper() + '_'}{str(i).zfill(3)}::\n")
            file.write(f"[html]Leidke 2. praktikumi juhendis olevatele näidetele toetudes järgmise "
                       f"{hash_type} tüüpi räsi parool. "
                       f"Vihjeks võime öelda, et parool on {vihje}täheline ja sisaldab ainult ladina "
                       f"tähestiku väiketähti (string.ascii_lowercase). "
                       f"Räsi <b>{entry['hash']}</b> parool on {{={entry['password']}}}.\n\n")
```

Joonis 5: Lõputöö käigus loodud skripti meetod, mis kirjutab Moodle'i testi räsitud paroolide küsimused HTML vormingus faili.

```
::DES_001::
[html]Leidke 2. praktikumi juhendis olevatele näidetele toetudes
järgmise DES tüüpi räsi parool. Vihjeks võime öelda, et parool on
2-4 täheline ja sisaldab ainult ladina tähestiku väiketähti
(string.ascii_lowercase). Räsi <b>arIkosT1IdQ7k</b> parool on {=fy}.
```

Joonis 6: Skripti loodud küsimuse näidis, mis on sobivas formaadis Moodle'isse importimiseks.

Teises ülesandes on tarvis läbi viia sõnastikrünne kasutajate ja nende räsitud paroolide andmestikel, kasutades John the Ripper[10] tarkvara. Andmestikud on loodud Linuxi */etc/passwd* paroolifaili formaadis, mis sisaldavad 149 MD5 ning 50 DES algoritmiga räsitud kasutaja parooli. Ülesandes kasutati esmakordselt eestikeelset ründesõnastikku *yhend.txt*, mis on valminud Anett Pärismaa lõputöö käigus [8]. Kokku on küsimustepangas 7 DES ja 19 MD5 andmestiku parooli, mida saab antud sõnastikuga tudengitelt küsida ja automaatkontrollida.

Kolmandas ülesandes on vaja leida ühe juhusliku kasutaja parool jõuründe abil kasutades ZAP[11] tarkvara. Kokku on veebirakenduse andmebaasi salvestatud 1000 sellist kasutajakontot. Kuna *yhend.txt* ründesõnastikus on ligikaudu 170 000 erinevat eestikeelset sõna, siis loodi lihtne Pythoni skript, mis valib sõnastikust suvalised 5000 sõna ning tekitab väiksema ründesõnastiku *alamosa.txt*. Seeläbi vähendati ründele kuluvat maksimaalset aega ligikaudu 34 korda, mille tulemusel muutus see veerandtunniseks. Valminud väiksemamahulise ründesõnastiku põhjal seati skripti abil veebirakenduse kõikidele kasutajakontodele *bcrypt* algoritmiga räsitud paroolid. Veebirakendus kompileeriti koos loodud kasutajate andmebaasifailiga Java arhiivifailiks (JAR-fail), mida saavad tudengid iseseisvalt virtuaalmasinates käitada.

Lisaks uuendati kasutatava lokaalse veebirakenduse versioon Java 11 pealt Java 17 peale, mille kestustugi kestab 2027. aasta lõpuni. Tulenevalt osade kasutatavate teekide ühildumatusest uuemate Java versioonidega ei peetud mõistlikuks hakata rakendust suurel määral ümber tegema ning jäeti Java 17 uuendamise peale. Rakenduse ja teekide uuendamise käigus moderniseeriti ka veebirakenduse kasutajaliides.

[10] John the Ripper password cracker. https://www.openwall.com/john/ (06.05.2025)
[11] ZAP. https://www.zaproxy.org/ (06.05.2025)

Neljandas ülesandes on vaja esitada Keepass2[12] tarkvaraga isetehtud paroolide andmebaasifail, mis on loodud vastavalt juhendis mainitud kriteeriumitele. Erinevalt ülejäänud ülesannetest jäi see kursuse õppejõududele kontrollida, kuna Moodle'sse on keeruline luua kontrollsüsteemi spetsiifilises formaadis andmebaasifaili kontrollimiseks.

Praktikumi läbiviimise käigus ilmnes probleem Moodle'i testi hilinenud esituste lubamisega. Õppeaines on lubatud esitada praktikumide lahendusi ka peale tähtaega, kuid neid hinnatakse sel juhul õigeaegsetest erineva, vähendatud täispunktide mahuga (75% kuni nädalase hilinemise puhul ja 50% rohkema hilinemise puhul). Seega ei olnud võimalik jätta testi tavapärase punktide mahuga avatuks peale tähtaega. Sellest tulenevalt lisati testi tähtajalisel sulgemisel kirje, et hilinenud esitajatel palutakse küsida erandkorras testi avamist. Seeläbi säilis ülevaade hilinenud esitustest ja oli võimalik nende testi hinnet tagantjärele käsitsi korrigeerida.

2.1.3 Praktikum 3 - OpenSSL & sertifikaadid

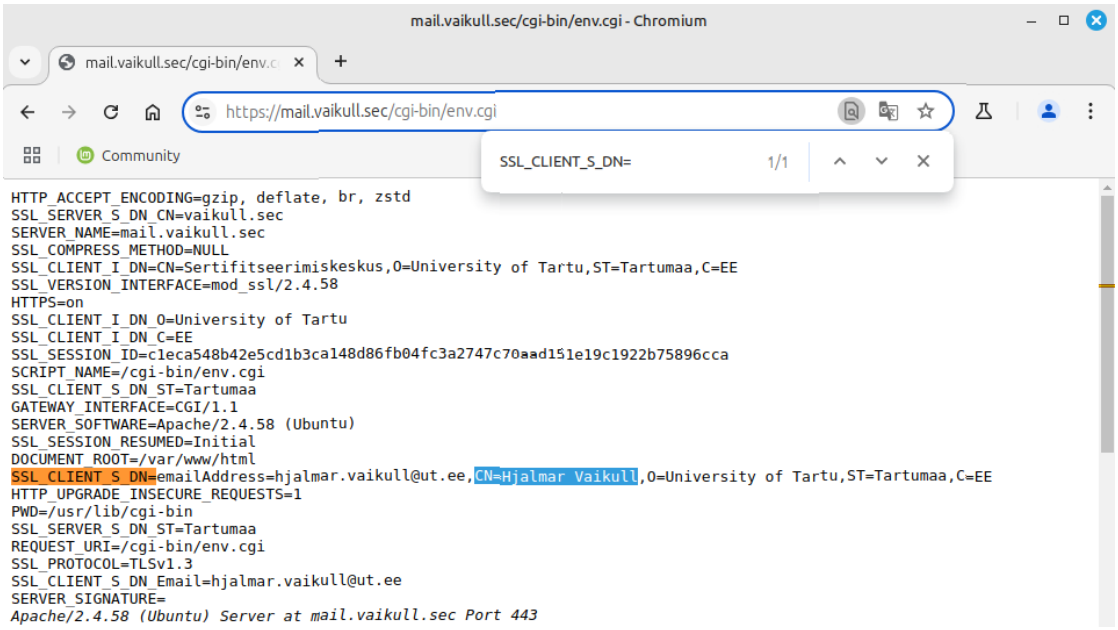
Kolmanda praktikumi eesmärk on tutvustada TLS krüpteerimist, sealhulgas digitaalsertifikaatide kasutusalasid, ning brauserikooke ja nendega seonduvaid turvariske. Praktikumi jooksul luuakse kasutaja enda signeeritud sertifikaat (ingl *self-signed certificate*), kliendisertifikaat ning viiakse läbi seansikaaperdus seansikoogi väärtuste abil.

Harjutustes kasutatakse sertifikaatide loomiseks OpenSSL[13] tarkvara, mis võimaldab standarditele vastavaid sertifikaate luua. Praktikumis kasutati senimaani 2018. aasta OpenSSL 1.1.1 kestustoe versiooniga kohandatud konfiguratsioonifaili. Uuendusena tuli 2021. aastal välja OpenSSL 3.0, mistõttu 1.1.1 versiooni töötavus ei ole enam 2023. aastast garanteeritud [9]. Seetõttu uuendati konfiguratsioonifail koos kohandustega uuema 3.0 kestustoega versiooni peale, et vältida lähitulevikus vana versiooni kehtivuse lõpuga kaasnevaid probleeme.

Samuti vahetati praktikumijuhendis kasutatud näidispildid välja uuemate vastu. Eelnevad ekraanitõmmised olid pärit aastast 2019, mistõttu olid nendelt kuvatavad näidised vananenud brauseri kasutajaliidesega. Seega oli tarvis vahetada need uuemate vastu välja, et lihtsustada tudengitel

[12] KeePass Password Safe. https://keepass.info/ (06.05.2025)
[13] OpenSSL. https://www.openssl.org/ (12.05.2025)

oma lahenduste võrdlemist näidislahendustega (vt joonis 7).



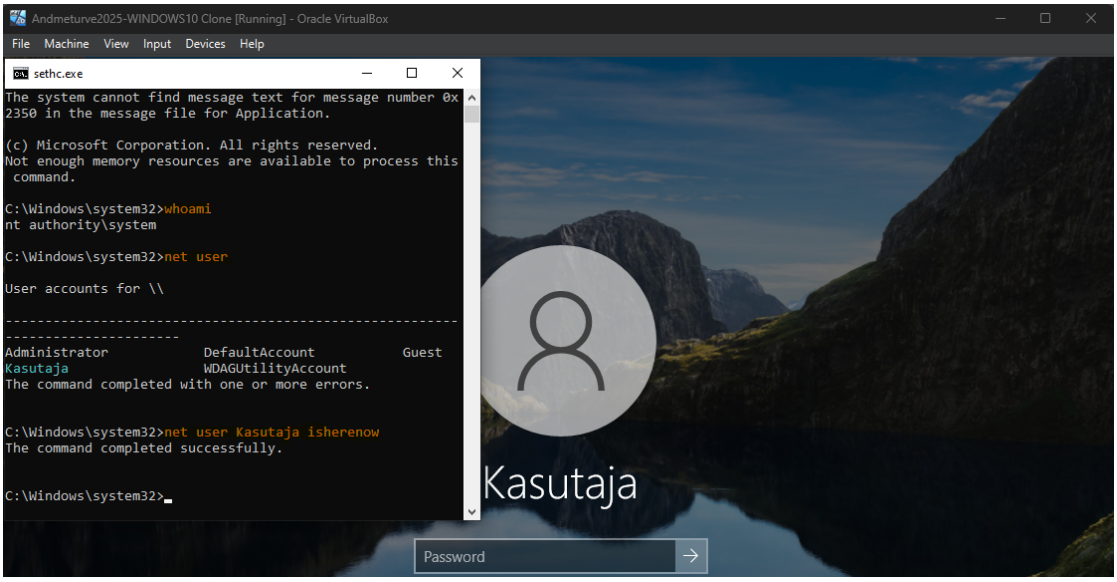
Joonis 7: Väljavõte loodud sertifikaatide kuvatõmmisest.

2.1.4 Praktikum 4 - Windowsi ründed

Neljanda praktikumi eesmärk on õpetada Windowsi operatsioonisüsteemide turvalist kasutamist ning tuvastama süsteemist kahjurvara. Praktikumi ülesanneteks on murda sisse Windows 10 virtuaalmasinasse kahel viisil: kleepklahvide kaaperduse (ingl *Sticky Keys hijack*) ja *chntpw* tööriista[14] abil. Seejärel tuvastatakse ja eemaldatakse süsteemis olev klahvinuhk ning muudetakse Windowsi kasutajate privileege, turvapoliitikat ja süsteemikonfiguratsiooni väärtusi.

Sarnaselt esimesele praktikumile oli neljanda praktikumi tegevuste jaoks tarvis luua Windows 10 virtuaalmasin, mille parooli ei täpsustata. Tudengid peavad muutma eelseadistatud salasõna ära kleepklahvide kaaperduse käigus, misjärel saadakse masinasse edaspidi tavapäraselt sisse logida (vt joonis 8).

[14] chntpw | Kali Linux Tools. https://www.kali.org/tools/chntpw/ (07.05.2025)



Joonis 8: Kuvatõmmis kleepklahvide ründega edukast parooli muutmisest.

Iga-aastaselt on loodud masinasse boonuspunkti ülesandena krüpteeritud fail, mille ligipääsetavus sõltub kasutaja krüptovõtme olemasolust [10]. Aastatel 2021 kuni 2023 ei olnud võimalik failile peale esimeses ülesandes tehtud kleepklahvide kaaperdust ligi pääseda, kuid alates 2024. aastast pääses failile ligi ka peale seda, mis viitab sellele, et kaaperduse käigus vahetatakse süsteemi õigustes lisaks paroolile välja ka krüptovõti. Erinevus selgus 2025. aastal peale *chntpw* tööriistaga parooli vahetamist, mistõttu ei uuenenud parooli vahetamisega enam dekrüpteerimiseks vajalik turvavõti. Sellest tulenevalt lisati boonuspunkti ülesanne praktikumijuhendisse sisse, kuid esituse kriteerium muudeti selliselt, et esitama peab lisaks krüpteeritud faili sisule ka kirjelduse, kuidas sellele ligi pääseti peale *chntpw* tööriistaga parooli jõuga muutmist.

Praktikumi ülesannete jooksul tuuakse välja, et ründed, millega Windowsi masinasse sisse saadi (kleepklahvide kaaperdus ja *chntpw* tööriistaga parooli jõuga muutmine), toimivad ainult krüpteerimata andmekandjaga masinate peal. Sellest tulenevalt mainitakse, et efektiivseim võimalus taoliste rünnete vastu kaitsta on masina andmekandja krüpteerimine, millest räägitakse lähemalt järgnevas praktikumis.

2.1.5 Praktikum 5 - Andmete kaitsmine VeraCrypt & Bitlocker näitel

Viienda praktikumi eesmärk on selgitada andmete krüpteerimise vajalikkust ning demonstreerida erinevaid andmekandjate krüpteerimise võimalusi. Praktikumi käigus seatakse üles krüpteeritud andmekandja vabavaralise tarkvaraga VeraCrypt ning krüpteeritakse terve süsteemiketas VeraCrypt'i ja Bitlocker'i utiliitidega.

Praktikumi ülesanded on loodud andmekandjate krüpteerimiseks mõeldud utiliitide kasutamisele, mille protseduurid pole eelnevast aastast alates muutunud. Samuti ei leitud testimise käigus märkimisväärseid tehnilisi probleeme. Seetõttu puudus vajadus suuri muudatusi juhendis teha. Lisaks on praktikumi töömaht vastav ettenähtud nelja tunni mahule, mistõttu ei olnud võimalik luua ülesandeid juurde.

Täiendava muudatusena kirjutati peidetud andmete partitsiooni loomise ülesanne ümber situatsiooniülesande vormi. Tegevuse tähtsuse selgitamiseks täiendati olukorra kirjeldust, kus on vaja peita andmekandjal krüpteeritud andmeid kolmanda osapoole eest. Kirjelduses tuuakse välja krüptograafia impordi keeluga riikide olemasolu ning vajadus kaitsta tundlikke andmeid väljapressimise eest. Ülesande jooksul luuakse andmekandjale Veracrypt'i abil välimine krüpteeritud failikonteiner, mille sisse luuakse teine sisemine krüpteeritud failikonteiner. Seeläbi on võimalik peita tegelikud tundlikud andmed erineva parooliga sisemisse konteinerisse, säilitades nende turvalisuse ka pärast välimise konteineri salasõna loovutamist. Ülesande kirjelduse käigus pannakse tudengid ettekujutuslikku olukorda, kus neilt nõutakse krüpteeritud andmete loovutamist kolmandale osapoolele, mille käigus avaldatakse salasõna välimisele petteandmetega krüpteeritud konteinerile.

2.1.6 Praktikum 6 - Turvaline suhtlus

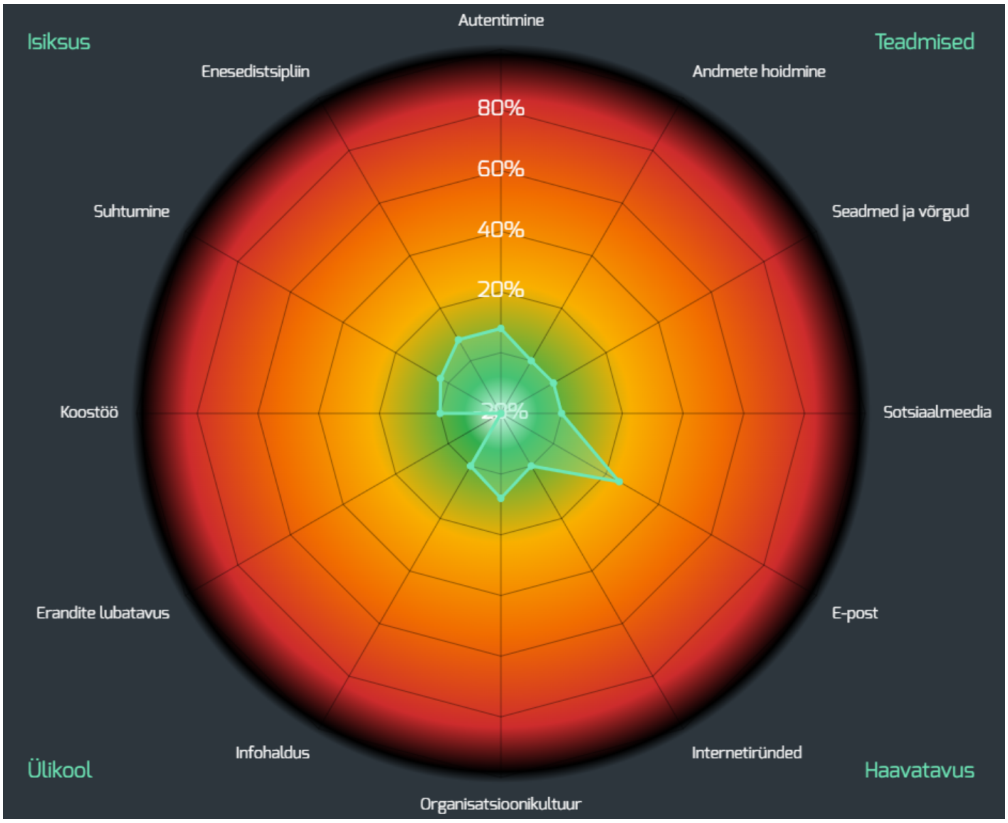
Kuuenda praktikumi eesmärk on viia tudengid kurssi erinevate e-kirja turvalisuse probleemidega ning õpetada, kuidas tuvastada libakirja tunnuseid. Lisaks tutvustatakse praktikumis Signali sõnumivahetuse rakendust ning pimeveebi veebilehitsejat Torbrowser. Praktikumi ülesanneteks on krüpteeritud e-kirja ja libameili saatmine, e-kirjade detailse vaate analüüsimine, otspunkt-

krüpteeritud sõnumi saatmine, pimeveebi veebilehtede külastamine ning Tartu Ülikooli küberhügieeni kursuse läbimine.

Kuues praktikum oli 2024. aastal kursuse kõige problemaatilisemate ülesannetega. Näiteks pidid tudengid saatma praktikumi harjutusena kursuse õppejõududele krüpteeritud ja signeeritud e-kirja, mille saatmine läbi GPG[15] osutus tehniliste probleemide tõttu ebastabiilseks ning osad korrektselt koostatud kirjad ei jõudnud kohale. Samuti oli vaja ühe harjutusena saata SMTP e-kiri Linuxi käsurealt, kuid seoses sSMTP[16] adressaadi kontrolli karmistumisega ei olnud enam võimalik autentimata meilikontode nime alt libakirju saata. Lisaks olid tudengid kohustatud ülesannete lahendamiseks looma uue meiliaadressi, kuna sSMTP ülesande käigus oli vaja konfiguratsioonifaili lisada enda meilikonto parool avatekstina (ingl *plaintext*).

Varasemate probleemide kõrvaldamiseks otsustati problemaatilised harjutused asendada suhtlusrünnete (ingl *social engineering*) temaatikaga. Seega loodi uus ülesanne, mille alguses peavad tudengid analüüsima erinevate libakirjade sisu ja leidma märke, mis vihjavad nende ebaautentsusele. Seejärel peavad tudengid läbima DeLRAP keskkonnas oleva Tartu Ülikooli küberhügieeni koolituse[17], mille käigus käsitletakse nii suhtlusründeid, paroolide turvalisust kui ka turvalisuse hea tava reegleid. Peale koolituse edukat läbimist palutakse tudengitel esitada kordamisküsimuste tulemused leheküljelt allalaetava PDF-dokumendina (vt joonis 9). Viimase sammuna palutakse tudengitel analüüsida eelnevaid libakirju uuesti ning kirjutada üles vihjed, mida nad esimesel vaatlusel ei leidnud, aitamaks kinnistada kursusel omandatud teadmisi.

[15]The GNU Privacy Guard. https://gnupg.org/ (08.05.2025)
[16]sSMTP - Simple SMTP. https://wiki.debian.org/sSMTP (08.05.2025)
[17]DeLRAP - Tartu Ülikool. https://cyberhygiene.ut.ee/ (08.05.2025)



Joonis 9: Näide küberhügieeni testi eduka lahendamise tulemuste graafikust.

Eelnevatest aastatest jäeti alles näiteks Signal[18] sõnumivahetuse rakenduse ja tumeveebi külastamise ülesanded. Esimese puhul peavad tudengid paigaldama endale Signali rakenduse ning saatma õppejõudude ülesseatud kasutajakontole ühe sõnumi oma nimega ning teise nii, et see kustub 30 sekundit pärast avamist. Lõputöö käigus seati Signali kasutaja uue kõnekaardi ja numbri peale, mis kehtib 6 kuud. Sellest tulenevalt on vaja kõnekaarti ja kontot iga-aastaselt uuendada. Teise allesjäetud ülesande jooksul on tarvis paigaldada Tor brauser[19], millega külastatakse üht turvalisusega seotud veebilehte ning selgitatakse, miks see turvalisusega seotud on.

Praktikumi läbi viies selgus, et keskmine praktikumile kuluv ajamaht on madalam kui esialgu prognoositi. Klassiruumis ilmnes, et enamik kohal olnud tudengeid said kogu praktikumi tehtud ligikaudu kahe tunniga, mis on poole võrra madalam ettenähtud neljatunnisest ajamahust.

[18] Signal. https://signal.org/ (14.05.2025)
[19] Tor Project | Anonymity Online. https://www.torproject.org/ (15.05.2025)

Seetõttu otsustati, et praktikumi on tarvis lisada järgmisteks aastateks ülesandeid juurde. Samuti selgus 2024/2025. õppeaasta aprillikuu lõpus, et SMTP e-kirja saatmine Telneti abil läbi *adalberg.ut.ee* serveri ei tööta enam, kuna serverist on eemaldatud Telneti võimekus ning puuduvad juurkasutaja õigused selle paigaldamiseks (vt joonis 10).

```
hvaikull@adalberg:~$ date
Fri May  9 12:41:47 AM EEST 2025
hvaikull@adalberg:~$ telnet
Command 'telnet' not found, but can be installed with:
apt install telnet            # version 0.17-44build1, or
apt install inetutils-telnet  # version 2:2.2-2ubuntu0.1
apt install telnet-ssl        # version 0.17.41+0.2-3.3build2
Ask your administrator to install one of them.
```

Joonis 10: Telnet kliendi puudumine adalbergi serveris.

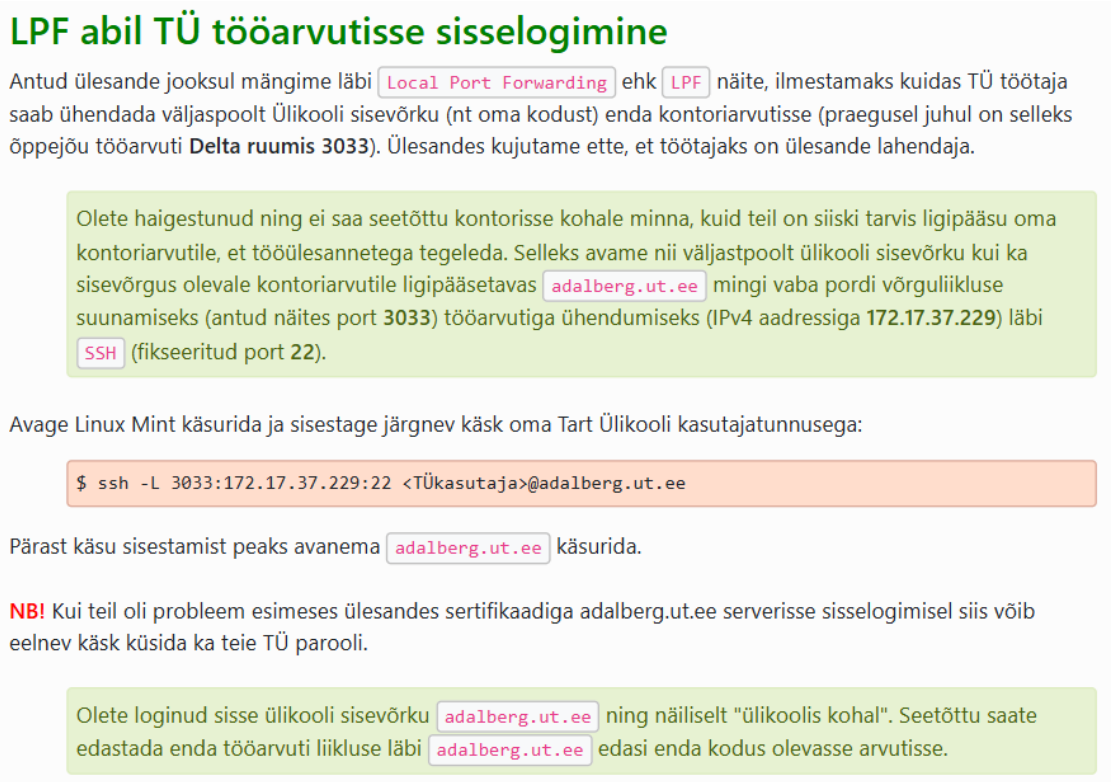
Antud ülesande asendamiseks loodi CTF stiilis ülesanne metaandmete analüüsimiseks, mille käigus peavad tudengid failide andmetest leidma vihjete abil peidetud väärtuseid. Ülesannet plaanitakse testida kursuse viimases praktikumis maikuu lõpus. Täiendavalt plaanitakse järgnevaks aastaks tuua praktikumi juurde e-kirja metaandmete teema.

2.1.7 Praktikum 7 - SSH kasutamine & turvalisus

Seitsmenda praktikumi eesmärk on tutvustada üle arvutivõrgu seadmetega ühendumise võimalusi ning juhtida tähelepanu nende turvariskidele. Praktikumi jooksul tehakse läbi SSH-tunneldus teise arvutisse ühendumiseks, seejärel tutvutakse erinevate rünnetega nagu võtmevarguse rünne, tunnelduse rünne, SSH-pöördühenduse rünne ja pealtkuulamine.

Praktikumis kasutatakse SSH tunneleid masinate kaugühenduse loomiseks. Harjutuste jaoks on varasemalt loodud kaks Linuxi virtuaalmasinat avatud SSH ühendusega, kuhu on töö käigus vaja tunneldada ning seeläbi ülesandeid lahendada. Seoses ühe emulaatormasina tehnilise rikkega oli tarvis selle peal jooksev virtuaalmasin ümber tõsta teise füüsilise masina peale. Seega eksporditi varasemalt kasutatud Linuxi virtuaalmasin OVA formaadi paketiks ning imporditi koos varasemate seadistustega uue masina peale.

Praktikumi ülesannetena on tudengitel vaja läbi viia nii lokaalne kui ka kaugtunneldus, mis on algtasemel õppijatele keerulised teemad. Seetõttu kirjutati vastavad harjutused ümber situatsioonülesanneteks kaugtöötaja vaatepildist, et mängida läbi konkreetne olukord, kus mainitud tunneldusviise on võimalik ära kasutada.



Joonis 11: Katkend LPF situatsioonülesandest.

Pärast situatsioonülesandeid on vaja tudengitel teha läbi sarnane tunnelduse harjutus iseseisvalt. Seeläbi on võimalik toetuda eelnevate ülesannete situatsioonipõhistele näidetele, et omandada teemast parem ülevaade.

2.1.8 Praktikum 8 - Võrguliikluse pealtkuulamine

Kaheksanda praktikumi eesmärk on demonstreerida lokaalse võrgu turvaprobleeme ning mängida läbi vahendusründed ja aadressiteisenduse protokolli (ARP) pete. Praktikumi ülesanneteks

on võrgupakettide pealtkuulamine tarkvaraga Wireshark[20] ning ARP-pette, SSH ja HTTPS vahendusrünnete läbi mängimine.

Praktikumi testimise käigus avastati, et Telneti kliendi ülesseadmisel on osad tehtavad sammud ebavajalikud. Juhendis olid jäänud sisse sammud nii *inetd* kui ka *xinetd* deemonitega (ingl *daemon*) Telnet võrguühenduse haldamiseks, kuid *xinetd* on *inetd* täiendatud funktsionaalsustega järeltulija. Seega ei olnud tarvis mõlemat ümber seadistada. Samuti olid *xinetd* Telneti halduse konfiguratsioonid aasta jooksul muutunud, mistõttu oli tarvis luua uus näide konfiguratsioonifaili sisust tehtud muudatustega (vt joonis 12). [11]

```
service telnet
{
    socket_type = stream
    wait        = no
    user        = root
    server      = /usr/sbin/telnetd
    log_on_failure  += USERID
    disable     = no
}
```

Joonis 12: */etc/xinetd.d/telnet* konfiguratsioonifaili näidis.

Lisaks selgus testimise käigus, et vahendusründe ülesandes kasutatava *ssh-mitm* läbistustestimise tööriista[21] installimisel tekib viga zlib teegi vananenud versiooni tõttu ka siis, kui on paigaldatud selle kõige uuem versioon. Veana tuvastati programmiviga (ingl *bug*) teegi versioonikontrolli formaadis[22]. Tekkinud anomaalia lihtsaimaks lahenduseks osutus tööriista konfiguratsioonifailis erandi lisamine versioonikontrolli eiramiseks.

2.1.9 Praktikum 9 - Kahjurvara & Windows forensics

Üheksanda praktikumi eesmärk on tutvustada erinevaid kahjurvarasid ning katsetada jälgede ajamist. Praktikumi jooksul kasutatakse erinevaid tööriistasid ja utiliite kahjurprogrammide te-

[20] Wireshark. https://www.wireshark.org/ (12.05.2025)
[21] SSH MITM v2.3-dev. https://github.com/jtesta/ssh-mitm (08.05.2025)
[22] FreeBSD Bugzilla – Bug 273578. https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=273578 (08.05.2025)

gevuse uurimiseks ning nende kõrvaldamiseks. Viimase tegevusena on välja toodud erinevaid küberturvalisusega seotud TED keskkonna videosid, mille vaatamise järgselt peavad tudengid tooma välja kasulikke teadmisi iga video kohta.

Praktikumis kasutatakse Windows XP virtuaalmasinat, mille peale on paigaldatud kolm kahjurvara sisaldavat programmi. Praktikumiülesannete jooksul käivitatakse iga programm ükshaaval, misjärel uuritakse nende tegevust masina süsteemis GMER ja NirSofti tarkvarade abil. Varasematel aastatel on tudengitel olnud vaja iseseisvalt Internetist paigaldada NirSofti tööriistu ja utiliite, mis käesoleval aastal muudeti ära.

2025. aastal töötas virtuaalmasinas olev *Firefox 48.0*[23] ebastabiilselt: (a) ei laadinud lehte ära, (b) otsingumootor kustutas aadressiribal päringu ära, (c) otsingumootor leidis päringule vasted mitmeminutilise ooteajaga, (d) otsingumootor leidis päringule vasted tavapärase ooteajaga. Kuna varasemalt oli tarvis tudengitel Internetist tööriistad ise alla laadida, siis muutis ebastabiilsus selle protsessi tülikaks. Seetõttu oli vaja 2025. aastal need tööriistad masinasse paigaldada enne virtuaalmasina jagamist. Kuna tööriistad tulid valmis programmidena, siis oli võimalik neid virtuaalmasinasse transportida läbi jaoskausta (ingl *shared folder*). Jaoskaust on emulaatorarvuti (ingl *host machine*) andmekandjal olev kaustasüsteem, mille kasutamiseks virtuaalmasinas on luba antud, töötades seeläbi failivahetuspunktina.

2.1.10 Praktikum 10 - Tulemüür, iptables, nmap & IPv6

Kümnenda praktikumi eesmärk on tekitada arusaam tulemüürist ning õpetada tundma ja kasutama IPv4 ja IPv6 aadresse. Praktikumi käigus seatakse üles tulemüür iptables[24] tööriista ja skriptimise abil, mida testitakse *nmap* utiliidi abil. Praktikumi viimases osas kirjeldatakse IPv6 erisusi võrreldes IPv4-ga, misjärel tuleb vastata iseseisvalt kontrollküsimustele õpitud teemade kohta.

Kümnenda praktikumi suurim probleem oli seni IPv6 materjalide pinnapealne käsitlus juhendis,

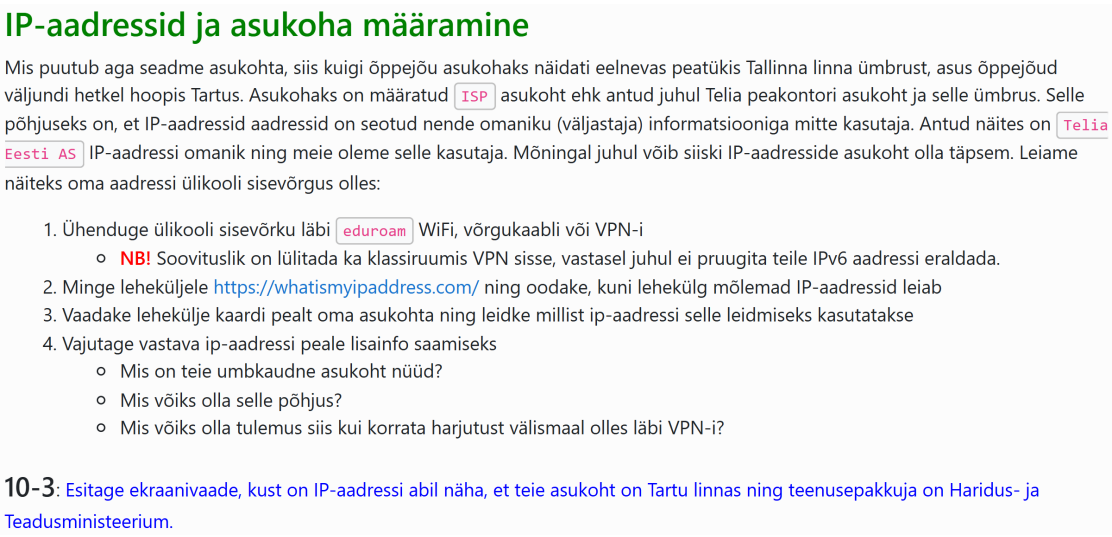
[23] Firefox System Requirements. https://www.mozilla.org/en-US/firefox/48.0/system-requirements/ (02.05.2025)

[24] iptables(8) - Linux man page. https://linux.die.net/man/8/iptables (12.05.2025)

mis piirdus sissejuhatava lõigu ja kahe teemakohase videoga. Lõputöö käigus täiendati materjale nelja alampeatüki ja ühe praktilise ülesandega:

1. IPv6 loomise vajalikkus;
2. IP-aadresside analüüs;
3. IP-aadressid ja asukoha määramine;
4. ohud IPv6 puhul.

Esimeses alampeatükis (1) selgitatakse esmalt IPv4 aadresside olemust ning nendega seotud probleeme, kus tuuakse välja nende piiratud arvust tingitud mured ja ajutise lahendusena loodud NAT. Seejärel selgitatakse IPv6 aadresse ning kuidas nende loomine IPv4 probleemid pikemaks ajaks lahendas. Teises (2) analüüsitakse Windows masina IP-aadresse ning uuritakse, mis infot on võimalik erinevate IP-aadresside abil saada. Kolmandas (3) selgitatakse, kuidas on võimalik leida avalike IP-aadresside abil seadme asukohta ning miks see on ebatäpne. Samuti loodi alampeatüki teema lihtsamaks mõistmiseks praktiline ülesanne, kus on vaja esitada kuvatõmmis IP-aadressi abil saadud asukohast, mis on VPN-ühenduse tõttu Tartu linna ümberkaudsetel aladel (vt joonis 13). Neljandas (4) tuuakse välja ohud ja muutunud ründed IPv6 puhul ning lisatakse, et NAT-teisendust ei tohiks võtta kui tulemüüri.



IP-aadressid ja asukoha määramine

Mis puutub aga seadme asukohta, siis kuigi õppejõu asukohaks näidati eelnevas peatükis Tallinna linna ümbrust, asus õppejõud väljundi hetkel hoopis Tartus. Asukohaks on määratud `ISP` asukoht ehk antud juhul Telia peakontori asukoht ja selle ümbrus. Selle põhjuseks on, et IP-aadressid aadressid on seotud nende omaniku (väljastaja) informatsiooniga mitte kasutaja. Antud näites on `Telia Eesti AS` IP-aadressi omanik ning meie oleme selle kasutaja. Mõningal juhul võib siiski IP-aadresside asukoht olla täpsem. Leiame näiteks oma aadressi ülikooli sisevõrgus olles:

1. Ühenduge ülikooli sisevõrku läbi `eduroam` WiFi, võrgukaabli või VPN-i
   - **NB!** Soovituslik on lülitada ka klassiruumis VPN sisse, vastasel juhul ei pruugita teile IPv6 aadressi eraldada.
2. Minge leheküljele https://whatismyipaddress.com/ ning oodake, kuni lehekülg mõlemad IP-aadressid leiab
3. Vaadake lehekülje kaardi pealt oma asukohta ning leidke millist ip-aadressi selle leidmiseks kasutatakse
4. Vajutage vastava ip-aadressi peale lisainfo saamiseks
   - Mis on teie umbkaudne asukoht nüüd?
   - Mis võiks olla selle põhjus?
   - Mis võiks olla tulemus siis kui korrata harjutust välismaal olles läbi VPN-i?

10-3: Esitage ekraanivaade, kust on IP-aadressi abil näha, et teie asukoht on Tartu linnas ning teenusepakkuja on Haridus- ja Teadusministeerium.

Joonis 13: Väljavõte IPv6 asukoha tuvastamise ülesandest.

Õpitu kinnistamiseks on praktikumijuhendi lõpus kolm kirjalikku ülesannet. Esimese küsimuse vastuseks tuleb esitada 3 uut IPv6 põhist rünnet, mida IPv4 puhul ei ole võimalik läbi viia. Teiseks tuleb arutleda selle üle, miks Linux ja MacOS on vaikimisi välja lülitatud tulemüüriga. Kolmandaks tuleb leida, mis on ARP-pette analoogne rünne IPv6 aadressiruumis.

2.1.11 Praktikum 11 - Veebirakenduse turvalisus & WebGoat

Üheteistkümnenda praktikumi eesmärk on juhtida tähelepanu veebilehtede turvalisusele, levinumatele turvavigadele ning meetmetele neid ära hoida. Tegevus põhineb veebirakenduse WebGoat[25] ülesannetel, mille valitud ülesannete edukast sooritamisest tuleb esitada arvestuse saamiseks tõestus.

WebGoat on spetsiaalselt ebaturvaliseks loodud veebirakendus, mis põhineb OWASP Top Ten[26] kõige kriitilisemate veebirakendustega seotud ohtude nimekirjal [12]. Rakenduses on ohtude õppimiseks loodud CTF-tüüpi ülesanded, mida peavad tudengid praktikumi jooksul lahendama kokku 22 tükki.

[25] OWASP WebGoat. https://owasp.org/www-project-webgoat/ (09.05.2025)
[26] OWASP Top Ten. https://owasp.org/www-project-top-ten/ (09.05.2025)

Tulenevalt rakenduse v2025.3 uuendist oli tarvis uuendada selle paigaldamise juhiseid ning ühe ülesande järjekorda. Praktikumi toimumise hetkeks polnud veel avalikustatud 2025. aasta ohtude nimekirja, mistõttu põhinesid praktikumi ülesanded veel 2021. aastal avalikustatud nimekirjal. Sellest tulenevalt jäeti ülesanded eelneva aastaga võrreldes samaks.

Kursuse käigus tekkis õppejõududel idee nõuda järgmistel aastatel kõikide praktikumide lahenduste esitamist PDF-vormingus. Seni on esitatud kõik ülesannete kuvatõmmised ja kirjalikud lahendused vabalt valitud formaadis, mille tagajärjel on ülesannete kontrollimine ühtse süsteemi puudumise tõttu aeganõudvam, sest kuvatõmmised ei pruukinud tudengitel olla harjutuste järjekorras. Esitusviisi nõudmist otsustati katsetada üheteistkümnendas praktikumis, kuna kõikide ülesannete lahenduste tõestamiseks on vastavas praktikumis vaja esitada 8 kuvatõmmist.

2.1.12 Praktikum 12 - E-ITS (Eesti Infoturbestandard)

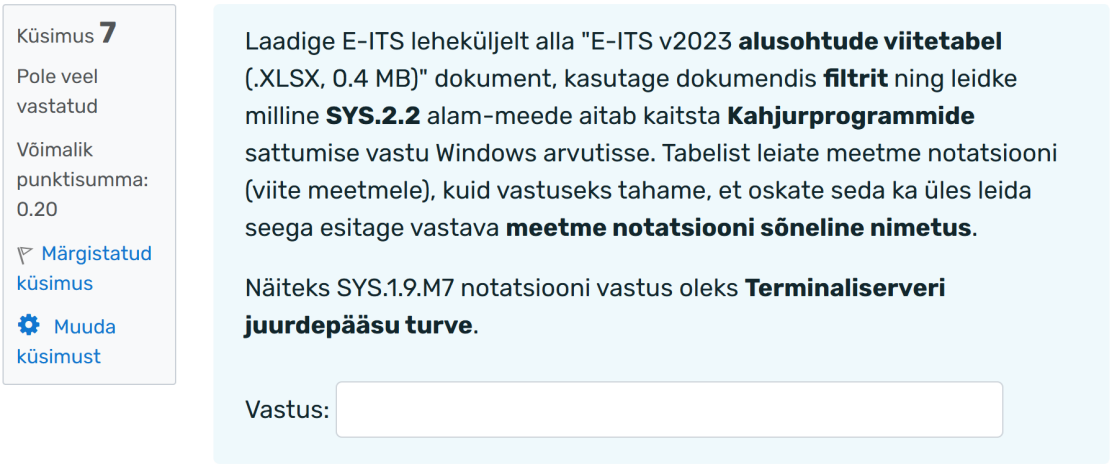
Kaheteistkümnenda praktikumi eesmärk on tuua välja, et küberturvalisus ei ole ainult tehniline, vaid oluline on ka omada tervikpilti enda varadest ning turvameetmetest. Tervikpildi omandamiseks on soovitatav rakendada standardeid ja kontrollmehhanisme, mis peaksid aitama turvaspetsialistidel kontrollida, ega midagi ära ei ole unustatud. Seetõttu õpetatakse käesolevas praktikumis kasutama Eesti Infoturbestandardit ja lahendatakse selle põhjal Moodle'i testi vormis praktilisi ülesandeid.

Praktikumis lahendatakse ülesandeid Eesti infoturbestandardi (E-ITS) 2024. aasta versiooni põhjal, mis on loodud avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kaitse tagamiseks [13]. Praktikumi käigus on tarvis lahendada kaks Digiriigi Akadeemia kursust: *Eesti Infoturbestandardi (E-ITS) ABC*[27] ja *E-ITS rakendamine: kaitsetarbest rakendusplaanini*[28]. Kummagi kursuse lahendamine võtab keskmiselt 45 minutit ning nende edukal läbimisel väljastatakse tudengitele PDF-formaadis tõendid, mis tuleb esitada praktikumi arvestuse saamiseks.

[27] Eesti Infoturbestandardi (E-ITS) ABC. https://digiriigiakadeemia.ee/enrol/index.php?id=50 (09.05.2025)

[28] E-ITS rakendamine: kaitsetarbest rakendusplaanini. https://digiriigiakadeemia.ee/course/view.php?id=74 (09.05.2025)

Kolmanda ülesandena on vaja lahendada ära Moodle test, mis koosneb kümnest küsimusest E-ITS etalonturbe kataloogi kohta (vt joonis 14). Testi küsimused on koostatud niiviisi, et lisaks teooriale peavad tudengid leidma üles küsitud info Eesti infoturbestandardist. Selle abil on võimalik muuta teoreetilise kallakuga teema praktilisteks harjutusteks, millest enamik on ka automaatkontrollitavad. Seeläbi välditakse kattuvust õppeaine loengute osaga, mis kontrollib pigem teoreetilisi teadmisi valikvastustega Moodle'i testi vormis.



Joonis 14: 12. praktikumi Moodle'i testi ülesande näide.

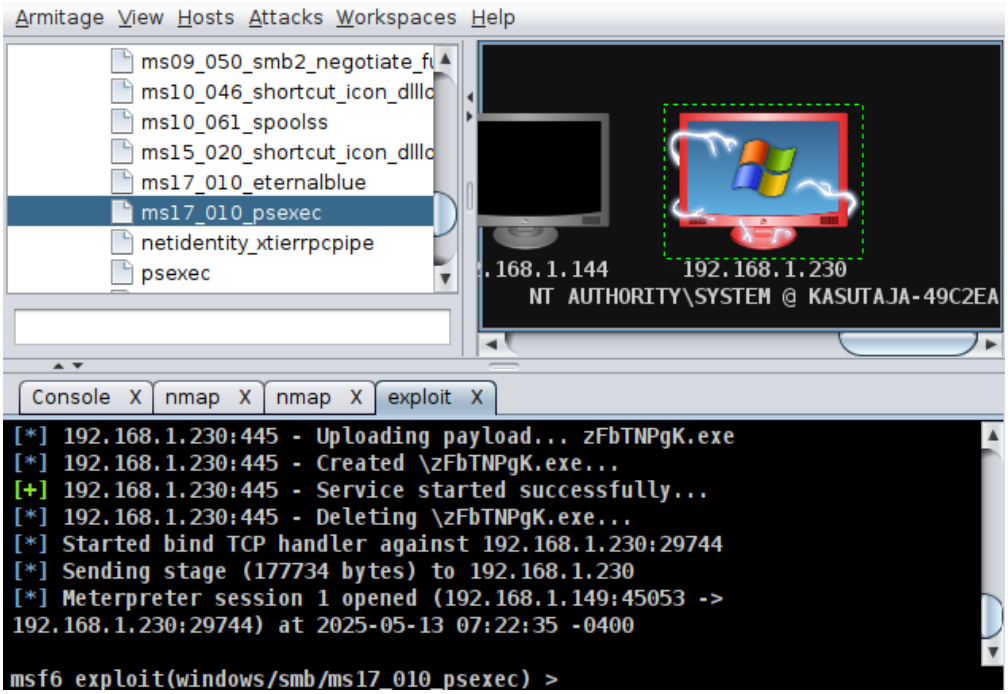
Tulenevalt 2023/2024. õppeaasta kogemustest muudeti praktikumi ülesannete punktide kaalu selliselt, et pool ettenähtud mahust teenitakse Digiriigi Akadeemia kursuste eest ning ülejäänud pool Moodle'i testist. Eelnevatel aastatel oli võimalik kolmveerand praktikumi punktidest teenida Digiriigi Akadeemia kursuste eduka sooritusе eest, mistõttu oli suur hulk tudengeid jätnud Moodle'i testi lahendamata selle vähese kaalu pärast. Muudatusega kaasnevalt loodi testi jaoks automaatkontrollitavaid küsimusi juurde, mis tõstis küsimuste arvu kümneni. Küsimused loodi varieeruvate variantidega selliselt, et iga tudeng saab testi käivitamisel sarnase tegevusega ülesande, kuid erineva juhtumi kirjeldusega. Seeläbi on võimalik vältida olukorda, kus test tehakse üksteise pealt maha, sest vastused erinevad olenevalt juhtumi kirjeldusest. Samuti täiendati enamik varasemaid küsimusi variatsioonidega ning muudeti automaatkontrollitavateks, et vähendada testide kontrollimiseks kuluvat aega.

2.1.13 Praktikum 13 - Turvaaukude ärakasutamine

Kolmeteistkümnenda praktikumi eesmärk on demonstreerida nõrkusi, mis tulenevad turvaaukudest ning süsteemi ja programmide uuendamata jätmisest. Praktikumi esimeses pooles paigaldatakse Windows XP SP3 virtuaalmasin, millel avatakse mitu ründevektorit. Seejärel kasutatakse neid ära üle võrgu rünnete jaoks Armitage tarkvaraga. Praktikumi teises pooles paigaldatakse Windows 11 operatsioonisüsteemil põhinev Tiny11, mida rünnatakse isetehtud kahjurvaraga ja IPv6 aadressiruumi teenusetõkestusründega.

Praktikumi esimeses pooles paigaldatakse ründavale masinale (Kali Linux) Metasploiti raamistik ning ohvri masinal (Windows XP) lülitatakse tulemüür välja ja lubatakse kaugpöördus (ingl *remote acccess*). Seejärel otsitakse turvanõrkuste andmebaasist sobilik rünne, millega masinale ligi pääseda. Varasematel aastatel viidi Armitage'i abil läbi MS08-067 turvanõrkuse rünne[29], mis käesoleva aasta versiooni peal ei töötanud stabiilselt. Seetõttu asendati see MS17-010, EternalBlue ründega[30], mille tulemusena pääsetakse Windows XP süsteemile ligi (vt joonis 15). Täiendavalt omandatakse administraatori kasutaja parooliräsi ja murtakse see lahti. Samuti kasutatakse klahvilogerit klahvivajutuste pealt kuulamiseks.

[29]Microsoft Security Bulletin MS08-067 - Critical.
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067 (13.05.2025)
[30]Microsoft Security Bulletin MS17-010 - Critical.
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (13.05.2025)



Joonis 15: Edukas *ms17_010_psexec* rünne Windows XP masinale.

Varasematel aastatel on käsitletud kogu praktikumi jooksul ainult Windows XP operatsioonisüsteemiga masinat, mille aegunud süsteemi kasutati rünnete jaoks ära. See ei andnud tudengitele piisavat ettekujutust sellest, kui lihtne on ohvriks langeda kasutades moodsamaid uuendamata masinaid. Seetõttu vähendati praktikumis Windows XP harjutuste mahtu ning asendati moodsama Tiny11 masina ülesannetega.

Tiny11[31] on kolmanda osapoole kohandatud Windows 11 operatsioonisüsteem, mis on väiksema ressursikulu ja mahuga. Lisaks puuduvad masinal automaatsed süsteemiuuendid, mistõttu on masina versioon siiani 22H2. Sellest tulenevalt on võimalik Tiny11 peal läbi viia viimase kahe aasta jooksul avalikustunud turvanõrkuste ründeid.

Teise osa esimeseks ülesandeks loodi tagasiühenduva kestakoodi rünne. Esimese ülesande eesmärk on tutvustada tagasiühenduvaid kahjurvarasid lihtsama näite abil, misjärel on järgmiste ülesannete tegevused arusaadavamad, kui luuakse tagasiühenduvaid troojane.

[31] Tiny 11. https://archive.org/details/tiny-11-NTDEV (13.05.2025)

Tudengitele antakse esmalt PowerShelli kaugkestakoodi näidis[32], mida on tarvis täiendada nende ründava masina (Kali Linux) IP-aadressi ja avatud pordinumbriga (vt joonis 16). Seejärel käivitatakse ründekood, mille tulemuseks saab ründav masin ligipääsu ohvri masina (Tiny11) käsureale. Tudengitel palutakse katsetada kaugühendusega käsureal Windowsi käske ning esitada nende tulemusest kuvatõmmis arvestuse saamiseks.

```
$ip = "AAA.BBB.CCC.DDD"
$port = 20XXX

$client = New-Object System.Net.Sockets.TCPClient $ip, $port
$stream = $client.GetStream()
[byte[]]$bytes = 0..65535|%{0}

while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
    $data = (New-Object -TypeName System.Text.ASCIIEncoding)`
        .GetString($bytes, 0, $i)
    $sendback = (Invoke-Expression $data 2>&1 | Out-String)
    $sendback2 = $sendback + 'PS ' + (pwd).Path + '> '
    $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
    $stream.Write($sendbyte, 0, $sendbyte.Length)
    $stream.Flush()
}
```

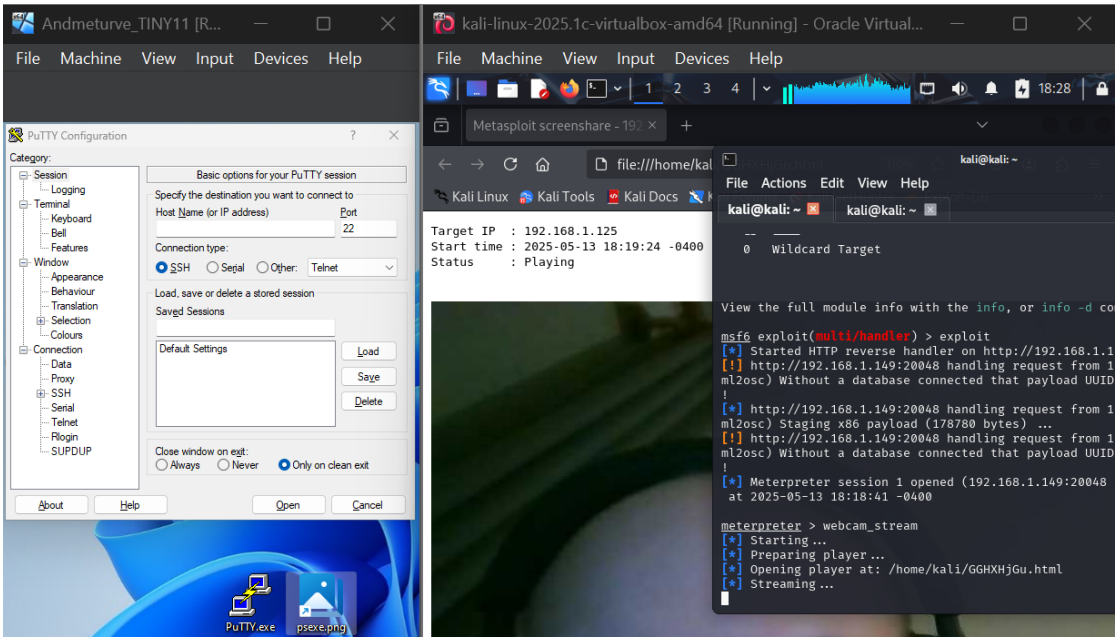
Joonis 16: Windows PowerShelli kaugkestakoodi näidis.

Teise ja kolmanda ülesandega arendatakse esimeses ülesandes loodud tagasiühilduva ründe näidet edasi. Tuuakse välja, et erinevalt eelnevast näitest on kahjurvarad üldjuhul peidetud mingi muu programmkoodi sisse, mistõttu ei ole ohver enamasti kursis sellega, mida pahatahtlik programm tegelikult teeb. Seetõttu luuakse ülesande jooksul kaks troojanit ning katsetatakse nendest tekkivaid võimalusi ohvrile kahju tekitamiseks.

Ülesande algul luuakse ründaval Kali Linux masinal kaks kaugpääsutroojanit, millest üks peidetakse PuTTY tarkvara programmikoodi sisse ning teine maskeeritakse hiljem pildifailiks. Troojanid luuakse *msfvenom* tarkvaraga käsureal ning seatakse üles käivitamise korral võtma ründava masinaga ühendust läbi kindlaksmääratud pordi, mille kolm viimast numbrit vastavad tudengite matriklinumbrile. Peale kahjurvarade loomist edastatakse need ohvri arvutisse SSH-tunneli

[32]Hacking windows 11 with Powershell. https://youtu.be/UeBvI278Na8?si=4v4K9dJggQy4B43I (13.05.2025)

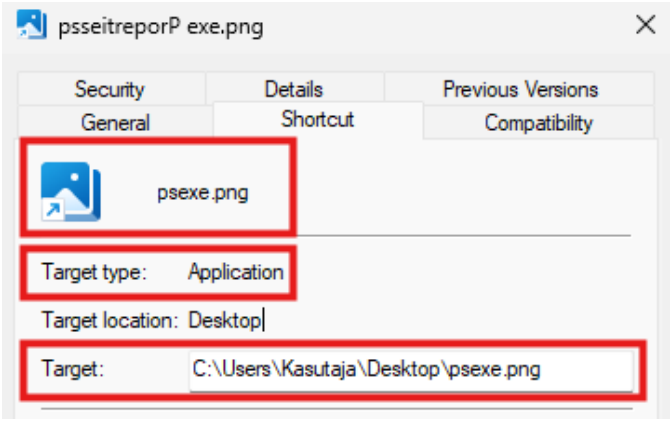
kaudu. Seejärel lülitatakse ründav Kali Linux masin tagasiühenduse porti kuulama ning ohvri masinal käivitatakse esmalt pahatahtlik PuTTY tarkvara. Käivitamise tagajärjel on näha, et ohvri masinas töötab programm ootuspäraselt ning esmapilgul ei ole ühtegi kahtlustekitavat märki, et tegemist oleks kahjurvaraga. See-eest on ründavas masinas näha, et ohvri masinaga on ühendus loodud ning selle käsurida on kasutatav, mistõttu on võimalik nuhkida masinas ringi ja võtta kontroll masinale üle. Peale ülesande lahendusest kuvatõmmise tegemist lülitatakse täiendava tegevusena sisse ohvri veebikaamera ning edastatakse selle otsepilt ründavasse masinasse (vt joonis 17).



Joonis 17: Ründav masin (paremal) jälgimas ohvermasina veebikaamera otsepilti.

Kolmandas ülesandes maskeeritakse tagasiühilduva kaugpääsuprogrammi töölaua otsetee (ingl *shortcut*) pildifailiks. Seda tehakse RLO ehk *right-to-left* unicode juhtmärgi abil[33], mis tõstab sunniviisiliselt teksti paremalt-vasakule suunaliseks. Seeläbi tekib sõna tagurpidi kujutis ja on võimalik kuvada „gnp.exe“ graafilises kasutajaliideses kujul „exe.png“ (vt joonis 18). Täiendavalt muudetakse ära ka otsetee ikoon.

[33]RIGHT-TO-LEFT OVERRIDE. https://unicode-explorer.com/c/202E (013.05.2025)

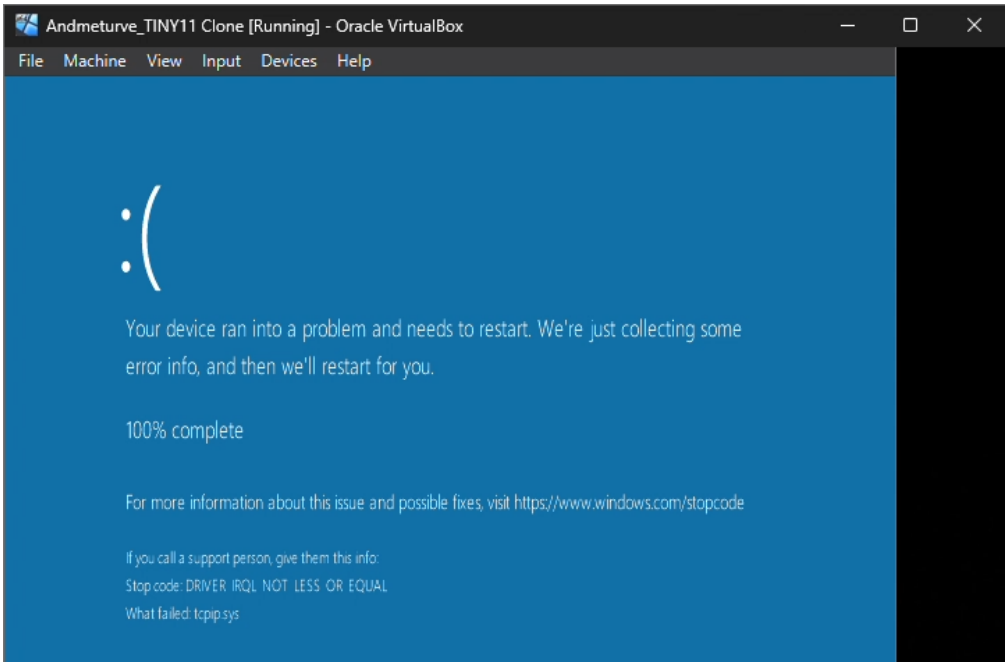


Joonis 18: Pildifailiks maskeeritud kahjurvara.

Loodud neljas ülesanne toetub kümnendas praktikumis käsitletud IPv6 teemale. Ülesandes kasutatakse ära CVE-2024-38063 turvanõrkust[34], et viia läbi teenusetõkestuse rünne. Nõrkus avastati 2024. aasta augustis ning see paigati (ingl *patched*) turvauuendusega juba sama aasta septembris, kuid tulenevalt Tiny11 22H2 versioonist on nõrkus ohvri masinas veel ära kasutatav.

Ülesandes kasutatakse GitHubist avalikult saadavat kontseptsiooni tõendust (ingl *proof of concept*), mis on loodud Pythoni programmeerimiskeeles [14]. Tudengitel on tarvis GitHubi hoidlast kood ründavasse Kali Linuxi masinasse paigaldada ja täpsustada seejärel käivituskoodis arvutivõrguga ühendatud võrguliides ning sihtmärgi IPv6- ja MAC-aadress. Lisaks palutakse käivitada Wireshark ning panna see IPv6-aadressiruumis võrguliiklust jälgima, et anda ründe ajal toimuvast ülevaade. Koodi käivitamisel saadetakse suures koguses fragmenteeritud IPv6 päringuid ohvri masinasse, koormates selle üle. Ründe tulemusena tekib ohvri masinal krahh (ingl *crash*). Peale masina taaskäivitust peavad tudengid Windowsi sündmusevaaturist leidma konkreetse sündmuse, mis kirjeldab juhtunud krahhi, ning sellest kuvatõmmise esitama lahenduse tõestuseks.

[34]CVE-2024-38063. https://nvd.nist.gov/vuln/detail/cve-2024-38063 (13.05.2025)



Joonis 19: Teenusetõkestusründe tagajärjel tekkinud krahh.

Praktikumi teises pooles kasutatud Tiny11 masinas tehakse Windows Defenderi erandid kaustadele, kus kahjurvara käivitatakse. Tegevus ei ole rünnete läbiviimiseks kohustuslik, kuna testimise käigus selgus, et Windows Defender tuvastas kahjurvara vaid ühel korral neljast. Seega on tegevus ennetuslik, et vältida tehnilisi probleeme praktikumi jooksul. Järeldusena tuuakse välja, et kõik masinale tehtud ründed on seetõttu tehtavad ka vaikeseadetega uuendamata Windows 11 masinatele.

2.1.14 Praktikum 14 - ID-kaart & e-hääletamine

Praktikumi eesmärk on tutvustada eID ja elektroonilise hääletamise lahendusi ning tuua välja lahenduste head ja problemaatilised pooled. Praktikumi jooksul peab looma digitaalselt allkirjastatud tekstifaili, uurima selle lühendväärtust (ingl *digest value*) ning kirjutama teemakohase essee, mis vastab etteantud küsimustele.

Praktikumijuhendis tutvustatakse erinevaid isikutuvastuse lahendusi ja tarkvarasid nagu ID-kaart, Mobiil-ID ja Smart-ID. Lisaks paigaldatakse DigiDoci programm, millega krüpteeritakse ja sig-

neeritakse erinevaid faile. Seejärel uuritakse signeeritud faili digitaalsignatuuri ning verifitseeritakse seda, toetudes varasemates praktikumides õpetatud räsimisalgoritmidele.

Digitaalsignatuuri teema on algtasemel õppijatele keeruline, mistõttu ei käsitleta seda väga tehniliselt. Seega on viimase ülesandena vaja tudengitel kirjutada essee, kus kirjeldatakse detailselt e-valimiste protseduure ning arutletakse nende turvalisuse üle. Lisaks on välja toodud mõisted, mida peab essee jooksul kasutama nagu näiteks *ümbrik*, *krüpteerimine*, *valimiste server* jne.

Praktikumijuhendis uuendati läbivalt viimaste aastate jooksul muutunud infot. Näiteks on valimistel alates 2025. aastast võimalik valimisrakenduses tuvastada end Smart-ID abil [15]. Samuti lõpetati 01.05.2025 Digi-ID väljastamine, kuid varem väljastatud isikutunnistused jäävad kasutatavaks kuni kehtivusaja lõpuni [16].

2.1.15 Praktikum 15 - Küberturbe harjutused enesekontrolliks

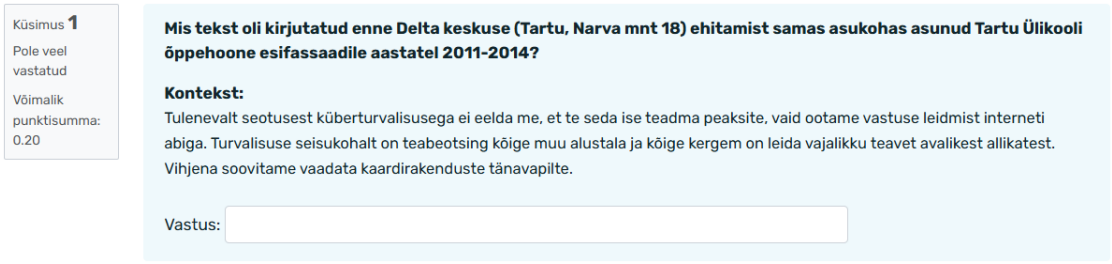
Viimase praktikumi eesmärk on korrata praktilise Moodle'i testi vormis kursuse jooksul õpitud teemasid ning kontrollida kursuse käigus omandatud teadmisi ja oskusi praktilisest küberturvalisusest. Test sisaldab 20 küsimust, millest igaühe lahendamiseks võiks keskmisel tudengil kuluda 10 minutit.

Varasematel aastatel on praktikum olnud CTF-stiilis ülesannetega, kus korrati küll osasid seni õpitud teemasid, kuid peamiselt olid ülesanded ülesehitatud teemadele, mida ei oldud senise õppetöö jooksul käsitletud. Seetõttu olid harjutused tudengite sõnul liiga keerulised ja osad neist jätsid keerukamad probleemülesanded lahendamata. Samuti tehti varasemalt koostööd ettevõttega CTF Tech[35], kelle veebirakenduses kogu praktikumi tegevus toimus. Kahjuks käesoleval aastal ei jõutud nende pakutud keskkonna kasutamise tingimustes kokkuleppele, mis andis täiendavalt sundluse muuta vastava praktikumi ülesehitust ja teemasid.

Eelnevalt mainitud murede lahendamiseks loodi uus Moodle'i test, mis sisaldab 20 automaatkontrollitavat küsimust. Testi ülesanded loodi sarnaselt varasemale peamiselt mängulises CTF-stiilis, kus ei ole samm-sammulisi juhiseid nende lahendamiseks (vt joonis 20). Ülesannete koos-

[35] CTF Tech. https://ctftech.com/ (14.05.2025)

tamisel arvestati igas praktikumis õpituga ning nende õpiväljunditele vastavalt loodi küsimused, millele tudengid peaksid oskama vastuseid leida omandatud teadmiste ja minimaalse info otsimise põhjal. See aitab kinnistada ja meelde tuletada senini käsitletud teemasid.



Joonis 20: Moodle'i testi CTF stiilis Internetiarhiivide ajaloo ülesanne.

Kursuse viimaste praktikumide sooritamise määr on iga-aastaselt olnud madalam kui esimeste, mille tingib semestri lõpuga seotud kiire aeg[36]. Kõige vähem sooritatakse seetõttu just viimases praktikumis käsitletud ülesandeid. Seega sooviti vältida uute teemade õppimist ning keskenduda teemade kordamisele, mis aitab tudengitel õppeaine eksamiks valmistuda.

2.2 Virtuaalmasinate loomine

Peatükis kirjeldatakse kursusel kasutatavaid virtuaalmasinaid ning nende loomise protsessi. Kuna praktikumide käigus avatakse tarkvaral ja seadmetel mitmeid erinevaid ründevektoreid, siis ei ole realistlik ega mõistlik viia tegevusi läbi tudengite endi arvutisüsteemide peal. Seetõttu tehakse enamik kursuse praktilisi tegevusi erinevates virtuaalmasinates. Nii on võimalik ühe füüsilise arvuti peal katsetada erinevaid ründeid ja tegevusi, ilma et tudengid oleksid kohustatud omama mitut seadet või ühele arvutile paigaldama mitut operatsioonisüsteemi. Samuti väheneb virtuaalsüsteemide eraldatuse tõttu oht, et tudengid tegevuste käigus enda arvutisüsteemi kahjustaksid. Lõputöö raames loodi kõigi virtuaalmasinate jaoks detailsed juhendid, kus on samm-sammulised juhised virtuaalmasinate paigaldamiseks, seadistamiseks ning nendes ettevalmistavate tegevuste

[36]Väide põhineb õppeaine vastutava õppejõu, Alo Peetsi, varasemate aastate tudengitelt küsimisele, miks nad viimaseid praktikume lahendatud ei jõua. Peamised põhjused on olnud tema sõnul semestri lõpuga seotud kiire aeg ja liiga rasked ülesanded.

tegemiseks. Järgnevalt selgitatakse põgusalt erinevate kursusel kasutuses olevate virtuaalmasinate loomise ja täiendamise protsessi.

2.2.1 Linux Mint 22

Kursuse enimkasutatud virtuaalmasin on Debianil põhinev Linux Mint distributiiv. 2025. aastal on kasutusel Linux Mint 22 redaktsioon (ingl *edition*) koodnimetusega „Wilma“[37], mis lasti välja 2024. aasta juulis. Kuigi 2025. aasta alguses avalikustati Linux Mint 22.1 „Xia“[38], oli selleks ajaks virtuaalmasin juba loodud. Mint 22.1 uuendiga kaasnesid peamiselt graafilise kasutajaliidese ja APT (*Advanced Package Tool*) sõltuvuste moderniseerimine, mis ei mõjuta praktikumides tehtavat tööd. Seega uue versiooni marginaalsete uuenduste tõttu ei hakatud kogu protsessi enam algusest peale tegema.

Virtuaalmasinad loodi ja jooksutati Oracle VirtualBox virtualiseerimistarkvaraga. Operatsioonisüsteemi VirtualBox tarkvaras paigaldamise jaoks on tarvis seadistada sellele kohased seaded, mida tarkvara ise automaatselt tuvastada ning seadistada üritab. Paraku aga ei suuda VirtualBox kõiki seadeid korrektselt just eriti Linuxi operatsioonisüsteemidel seada. Näiteks on tüüpprobleem videomälu eraldamise seaded, mille VirtualBox seab üldjuhul automaatselt 64 MB peale [17]. Väljalaske teates kirjutatakse, et seetõttu kipuvad virtuaalmasinad vähese videomälu tõttu virvendama ning kokku jooksma. Tuuakse välja, et lahendus selleks on eraldada videomälu 128 MB või enamgi.

Linux Mint masina installimisel tuleb paika seada sobilik kasutajanimi ning parool selliselt, et selle lahti murdmine tudengitele poleks triviaalne protsess, kuna esimene ülesanne masinasse sisenemisel on logida kasutajasse sisse parooli teadmata. Viimase sammuna tuleb virtuaalmasin eksportida OVA (*Open Virtual Appliance*) paketiks ning avalikustada kursuse materjalides.

[37] Linux Mint 22 "Wilma". https://linuxmint.com/edition.php?id=316 (02.05.2025)
[38] Linux Mint 22.1 "Xia". https://linuxmint.com/edition.php?id=321 (02.05.2025)

2.2.2 Kali Linux

Kali Linux[39] on Debianil põhinev Linuxi distributsioon, mis on loodud turvatestimise ja -analüüsimise eesmärgil. Kursuse raames kasutatakse virtuaalmasinat peamiselt eetilise häkkimise (ingl *ethical hacking*) eesmärgil, kuna sellel on eelinstallitud mitmed tööriistad, mida praktikumide jooksul vaja läheb.

Praktikumides kasutatakse Kali kodulehelt allalaetavat virtuaalmasinat, mis on eelvalmistatud VirtualBox tarkvarale. 2025. aastal kasutati 11. praktikumis (*Veebirakenduse turvalisus & WebGoat*) Kali 2025.1a versiooni, kuid seoses *kali-archive-keyring* muutmisega enne 13. praktikumi (*Turvaaukude ärakasutamine*), soovitati paigaldada selleks praktikumiks uus 2025.1c versioon [18].

2.2.3 Windows 10

Windows 10 Education redaktsiooniga virtuaalmasinat kasutatakse kursusel Windowsi põhiste masinate turvalisuse käsitlemiseks. Windows 10 operatsioonisüsteemi kasutatakse Windows 11 asemel, kuna selle vaba talletusruumi nõuded on poole väiksemad kui Windows 11 nõuded. Lisaks on Windows 11 andmekandja vaikeseadena krüpteeritud alates 24H2 uuendist [19], mille tagajärjel on süsteemiketta sisu lugemine harjutuste mõttes raskendatud.

Windows 10 virtuaalmasina loomine on enamjaolt analoogne Linux Mint masina loomisega. Lisasammuna on tarvis operatsioonisüsteem aktiveerida KMS (Key Management Services) klientvõtmega[40]. Suurim erinevus seisneb praktikumi ülesanneteks vajalike materjalide ülesseadmises. Näiteks on tarvis paigaldada masinasse klahvinuhk, mille peab ühe ülesande käigus süsteemist üles leidma ning esitama arvestuseks tõestuse sellest, et nende seniseid tegevusi on n-ö pealt kuulatud. Viimased sammud on jällegi *boonuspunktide* peitmine süsteemi ning eksportimine.

[39] Kali Linux. https://www.kali.org/ (04.05.2024)
[40] KMS. https://learn.microsoft.com/en-us/windows-server/get-started/kms-client-activation-keys (02.05.2024)

2.2.4 Windows XP

Windows XP virtuaalmasin loodi kursuse raames juba 2014. aastal ning seda on peale loomist täiendatud aastatel 2016, 2017 ning 2025. Kuna Windows XP tugi lõpetati 2014. aastal, siis uuendite puudumise ja tarkvara muutumatuse tõttu pole senini olnud vajadust masinas täiendusi teha. Virtuaalmasinat kasutatakse peamiselt praktikumides *Kahjurvara & Windows forensics* ning *Turvaaukude ärakasutamine*, kus käivitatakse erinevat pahavara ja kasutatakse digitaalkriminalistika tööriistu juhtumite analüüsiks.

Käesoleval aastal täiendati virtuaalmasinat NirSofti utiliitide paigaldamisega, mida kirjeldati detailsemalt 9. praktikumi tegevuste seas (2.1.9).

2.2.5 Tiny11

Tiny11[41] on kolmanda osapoole kohandatud Windows 11 operatsioonisüsteem, milles on vähendatud mullvara (ingl *bloatware*). Kursusel kasutatakse Tiny11 operatsioonisüsteemi seetõttu, et sellel puuduvad automaatsed turvauuendused, mis tähendab, et masinal saab kergekäelisemalt uuemaid ründeid läbi viia. Lisaks sellele on masina kogu ressursikulu ja maht väiksem, mistõttu on seda kergem paigaldada ja virtuaalmasinana jooksutada.

Tiny11 on esmapilgul atraktiivne valik n-ö tavakasutajate seas oma vähese ressursikulu tõttu. Kuna aga tegemist pole Microsofti poolt heaks kiidetud ametliku operatsioonisüsteemiga, siis ei tohiks seda täielikult usaldada ning on soovituslik vältida tundlike andmete hoiustamist selle operatsioonisüsteemiga masinates. Seetõttu on tarvis viia tudengid kurssi potentsiaalsete riskidega, mis sellist tüüpi operatsioonisüsteemiga kaasnevad. [20]

Kursusel kasutatav Tiny11 virtuaalmasin on teadlikult jäetud täiendamata, et tudengid saaksid huvi korral avastada ilma lisadeta masinat. Selle soodustamiseks on praktikumijuhendis välja toodud ka silmaringi ülesanded otsimaks võrdlusi ametliku Windows 11 operatsioonisüsteemiga. Virtuaalmasina loomise käigus on tehtud ainult lokaalne kasutajakonto ning seadistatud keel, klaviatuur ja esmased Microsoftiga andmete jagamise küsimused.

[41] Tiny 11. https://archive.org/details/tiny-11-NTDEV (05.05.2024)

Tulenevalt operatsioonisüsteemide perioodilistest versiooniuuenditest, säilib vajadus luua virtuaalmasinad uuesti igal aastal. Samuti on vaja virtuaalmasinate *boonuspunktide* ülesandeid vahetada, et need ei läheks tudengite seas levima. Eelnevale mõeldes loodi õppejõude abistavate materjalidena ka virtuaalmasinate loomise ja seadistamise käigus teostatud tegevuste dokumentatsioon. Sama tehti ka nende testimisprotsessist praktikumide käigus tehtavate tegevustega. Seeläbi on loodetavasti edaspidine virtuaalmasinate loomine lihtsustatud ning aitab vältida valeseadistustest tulenevaid probleeme.

Kokkuvõte

Bakalaureusetöö eesmärk oli värskendada ja täiendada Tartu Ülikooli bakalaureuse õppekavas oleva kursuse LTAT.06.002 Andmeturve praktikumimaterjale. See hõlmas kõiki kursuse praktikumijuhendeid, praktilisi teste, kasutatavaid ressursse ning administratiivseid abimaterjale. Lõputöö tulemusel tagati 2025. aasta kevadel toimunud praktikumide harjutuste toimivus ning materjalide asjakohasus kiirelt muutuvas küberruumis.

Kursuse kõik 15 praktikumi läbisid lõputöö käigus põhjaliku testimisfaasi, mille jooksul kaardistati värskendamist või täiendamist vajavad materjalid. Töö käigus uuendati läbivalt kõik praktikumijuhendid ning kasutuses olevad rakendused, virtuaalmasinad ja tarkvarad. Samuti täiendati ja kaasajastati olulisel määral praktikumide teemasid nagu turvaline suhtlus, IPv6 ning turvaaukude ärakasutamine.

Lõputöö märkimisväärsemad saavutused olid 4 värskendatud eelseadistatud virtuaalmasinat, 3 automaathinnatavate praktiliste harjutustega Moodle'i testi, 4 oluliselt täiendatud tegevustega praktikumi ja õppejõude abistavad materjalid praktikumide ülesseadmisel. Näiteks võeti õppeaines esmakordselt kasutusele Windows 11 operatsioonisüsteemil põhinev kohandatud operatsioonisüsteem Tiny11, mille põhjal kaasajastati turvaaukude ründamise praktikumi tegevused moodsama masina põhiseks.

2025. aasta kevadel testisid loodud ja täiendatud materjale iganädalaselt umbes 250 tudengit aine praktikumides. Tudengite praktikumiülesannete sooritamise käigus olulisi probleeme juhendites ja ülesannetes ei tuvastatud ning üksikud tekkinud probleemid lahendati juba esimeste praktikumide jooksul juhendi uuendamisega.

Bakalaureusetöö tulemusena on edaspidine kursuse praktikumide ülesseadmine mõnevõrra lihtsustatud, kuna loodud juhendite abil on kergendatud materjalide testimise ja värskendamise protsess. Samuti on loodud skriptide abil võimalik automatiseerida kursuse testiküsimuste uuendamist. Kokkuvõtvalt on aine vastutav õppejõud Alo Peets tehtud tööga väga rahul ja varasemad head praktikumijuhendid muutunud veelgi paremaks ning kvaliteetsemaks.

Viidatud kirjandus

[1] Riigi Infosüsteemi Amet. Küberturvalisuse aastaraamat 2025. . https://www.ria.ee/sites/default/files/documents/2025-02/RIA-kuberturvalisuse-aastaraamat-2025.pdf. (13.04.2025).

[2] Vaughan-Nichols S. Long-term support for linux kernel to be cut as maintenance remains under strain. *ZDNET*, 2023. https://www.zdnet.com/article/long-term-support-for-linux-kernel-to-be-cut-as-maintenance-remains-under (10.05.2025).

[3] endoflife.date. Linux kernel. https://endoflife.date/linux. (10.05.2025).

[4] Allan K. The threat landscape is constantly changing. *Cyber Magazine*, 2023. https://cybermagazine.com/articles/the-threat-landscape-is-constantly-changing. (10.05.2025).

[5] LTAT.06.002 Andmeturve 2024/2025 kevad. https://ois2.ut.ee/#/courses/LTAT.06.002/version/bf2fa85f-8e3b-3bc8-3bbe-fa32b69e36ec/details. (12.05.2025).

[6] LTAT.06.001 Operatsioonisüsteemid. https://ois2.ut.ee/#/courses/LTAT.06.001/details. (12.05.2025).

[7] Halapuu J. Eestikeelse veebipõhise linuxi käsurea õpikeskkonna loomine, 2022. https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=74682. (07.05.2025).

[8] Pärismaa A. Eestikeelsete paroolide mustrite uurimine ja ründesõnastiku koostamine, 2024. https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=79489. (08.05.2025).

[9] OpenSSL Corporation. Openssl 1.1.1 end of life, 2023. https://openssl-corporation.org/post/2023-09-11-eol-111/. (07.05.2025).

[10] Microsoft. File encryption. https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df (12.05.2025).

[11] Inc. KxSystems. inetd, xinetd. https://code.kx.com/q/kb/inetd/. (08.05.2025).

[12] OWASP. Owasp webgoat. https://owasp.org/www-project-webgoat/. (09.05.2025).

[13] Riigi Infosüsteemi Amet. Eesti infoturbestandard, . https://eits.ria.ee/. (14.05.2025).

[14] ynwarcs. cve-2024-38063, 2024. https://github.com/ynwarcs/CVE-2024-38063. (13.05.2025).

[15] Valimised Eestis. E-hääletamise tuvastusvahendite hulka lisandus smart-id, 2025. https://www.valimised.ee/et/e-haaletamise-tuvastusvahendite-hulka-lisandus-smart-id. (12.05.2025).

[16] Politsei ja Piirivalveamet. Digi-id. https://www.politsei.ee/et/juhend/digi-id-taotlemine. (12.05.2025).

[17] Linux Mint. Linux mint 22 release notes. https://www.linuxmint.com/rel_wilma.php. (05.05.2025).

[18] OffSec. Kali linux release history. https://www.kali.org/releases/. (04.05.2025).

[19] Von Peery. Bitlocker by default: A game-changer for windows 11 security, 2024. https://www.sikich.com/insight/

bitlocker-by-default-a-game-changer-for-windows-11-security/. (02.05.2025).

[20] Jasper Hawthorne. Tiny11 hands-on. https://www.devx.com/how-tos/tiny11-hands-on/. (05.05.2025).

Lisa 1

Järgnevalt on välja toodud osa lõputöö käigus loodud õppejõude abistavatest materjalidest, juhenditest ja mallidest:

1. *Courses* keskkonna praktikumijuhendite mall[42] (vt joonis 21);
2. virtuaalmasinate loomise käigus koostatud dokumentatsioon (vt joonis 22);
3. praktikumimaterjalide kontrollimise juhend;
4. avaldamise piiranguga praktikumide hindamislehekülg.

```
(:praktikumi_number:<XX>:)
(:tahtaeg:<AA>-<BB>. <KUU>:)

!%green% Praktikum {$:praktikumi_number} - <Praktikumi pealkiri>

<Praktikumi sissejuhatav tekst>

!!%green% Ettevalmistus

<Ettevalmistavad tegevused enne ülesandeid, ei ole kohustuslik>

!!%green% <Teema 1>

<Teemasid selgitav tekst, samm-sammulised juhised ja ülesanded>

...

!!%green% Praktikumi ülesanded
Praktikumi ülesannete lahendamine annab neli punkti ja esitamiseks on
kaks nädalat alates praktikumi toimumisajast (%red%Personaalne tähtaeg
vahemikus {$:tahtaeg}%%).
* '''[++{$:praktikumi_number}-1:++]'''%blue% <ülesande kirjeldus>
%%- <punktisumma>p
```

Joonis 21: Väljavõte praktikumijuhendite mallist.

[42] LTAT.06.002 praktikumijuhendite mall. https://courses.cs.ut.ee/2025/turve/spring/Main/Mall (15.05.2025)

PRAKTIKUM 13

Ettevalmistused

Eeldused

- Installeeritud on viimase versiooniga Oracle VM VirtualBox;
    - https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html
- Virtuaalmasina testimine peaks toimuma Windows masina peal.
- ISO faili jaoks on vaba vähemalt 4 GB

Paigaldamine ja installimine

1. Laadida alla **Tiny11 22H2 ISO** (https://archive.org/details/tiny-11-NTDEV)
2. Käivitada VirtualBox ning luua uus masin:
    a. **Name:** Andmeturve_Tiny11
    b. **ISO Image:** <Allalaetud Tiny11 ISO>
3. Virtualbox masina sätted:

    Hardware:

    a. **Base Memory:** 4096 MB
    b. **Processors:** 2

    Hard Disk:

    c. 20 GB
    d. **Type:** VDI (mitte pre-allocate full size)
4. Enne virtuaalmasina käivitamist:

    Settings -> Display -> Screen:

    a. **Video Memory:** 128 MB
    b. **Graphics Controller:** VBoxSVGA
    c. **Extended Features:** 3D Acceleration ✓ (kontrollida, et ei oleks linnukest lisatud)

Joonis 22: Väljavõte 13. praktikumi ülesseadmise ja kontrollimise juhendist.

Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Hjalmar Vaiküll**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

   „Andmeturbe kursuse praktikumimaterjalide värskendamine ja täiendamine“,

   mille juhendaja on **Alo Peets**,

   reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Hjalmar Vaiküll

15.05.2025