Tartu Ülikool

Loodus- ja täppisteaduste valdkond

Tehnoloogiainstituut

Jander Metsma

arvutitehnika 1. aasta

Probleemipõhine õpe

Arvutiriistvara praktikumi (LOTI.05.021) aruanne

Juhendajad: Toomas Plank

Laur Edvard Lindmaa

Tartu 2023

Sisukord

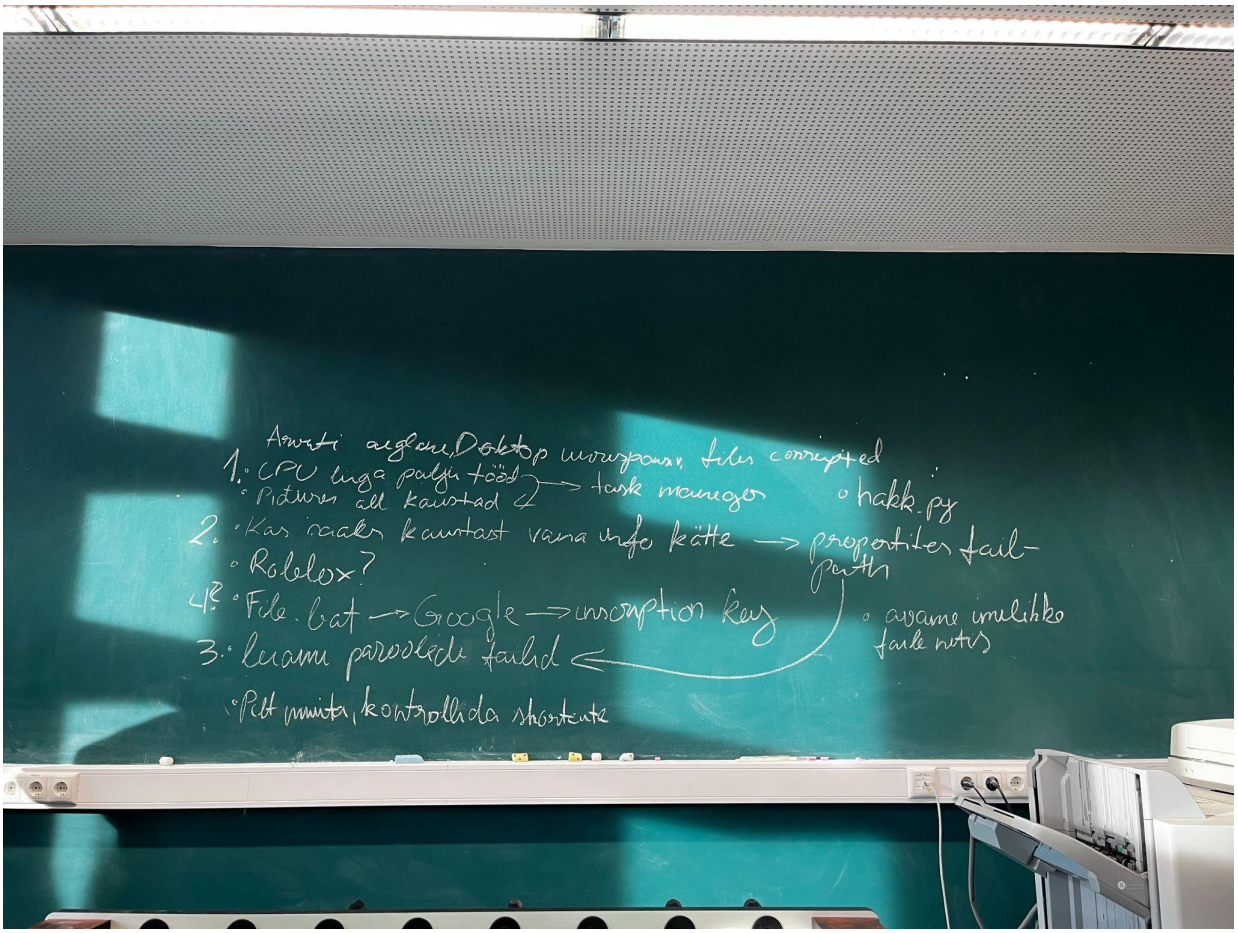
1. Töö tutvustus ja eesmärk

1.1 Olukord

Teine arvutiriistvara praktikum toimus 05.10.2023 algusega kell 08:15 füüsikumi A307 klassis. Praktikumis oli meile ette antud läpakas *HP Elitebook 840 G7 Notebook PC*, mis oli olnud nakatatud viirusega. Nimelt probleem seisnes, et arvuti oli aeglane ning fail, milles olid tähtsad paroolid, oli kaduma läinud.

1.2 Eesmärk

Töö eesmärk oli taastada kadunud failid ning korrastada arvuti võimalikult lähedale oma algseisundisse. Plaan selleks kujunes ajurünnaku ajal, mille teostasime koridoris koos 4 teise kaastudengiga. Abivahendiks kasutasime tahvlit, kuhu kaardistasime kõik oma mõtted ja ideed.



Joonis 1. *Ajurünnaku tahvel.*

Joonisel 1 on kujutatud meie mõtted, probleemid on nummerdatud ühest neljani. Esiteks tegi CPU liiga palju tööd, lahenduskäiguks mõtlesime, et peame tegumihalduriga probleemse programmi peatama. Enne ajurünnakut arvutis ringi vaadates, leidsin piltide kaustast 10 kausta nummerdatud nullist üheksani ning iga kausta sees oli sama seisukord kuni kuue korrani. See teadmine aitas anda aimu, kus võiksid paroolid peidetud olla. Plaan oli leida ja taastada parooli fail. Viimane eesmärk oli korrastada arvuti tagasi algseisundisse, see tähendab kustutada kõik, mis oli tekitatud viiruse poolt.

2. Töökäik

Klassi tagasi saabudes alustasin lihtsamast, CPU koormuse vabastamisest. Leidsin probleemse programmi ning peatasin selle. Enne eelmainitud tegevust, jätsin meelde ka programmi nime. Asukoha leidsin failides sirvides ja ebanormaalsusi otsides. Koormaja asus kaustas nimega *Program files (x69)*, mille ma kustutasin. Nüüd suurem takistus oli parooli leidmine. Kuna piltide kaustas oli rohkem, kui miljon kaustasid, siis neid ükshaaval läbi otsida oleks olnud ajakulukas. Avastasin, et kui avada kausta atribuudid, siis näen valitud kausta üldistatud sisu. Ainult ühes kaustas oli kaks faili. Tehes sama 6 korda veel, leidsid parooli ning ka kausta, mis oli krüpteeritud parooliga. Allalaadimiskaustas istus probleemi algus, fail nimega *hack.py*. Seda faili avasin *notepad* programmiga, mis võimaldas mul lugeda, kuidas terve viirus ülesehitatud on. Kõige tähtsam rida koodi oli selline, mis kirjeldas, et kausta parool on kuuekohaline number ja on analoogne kaustade teekonna numbritega. Olemas nii lukustatud kaust ja parool, oli puudu viis, kuidas parooli sisestada. Selleks kasutasin interneti abi. Otsingumootoriga leidsin veebilehe[1], kus õpetas kasutama programmi nimega *7-zip*, mille abil sain dekrüpteerida kausta. Parooli liigutasin töölauale, et oleks kiiresti kättesaadavas kohas. Veel kontrollisin, kas töötavad mängud ning kõik töölaual olevad otseteed, vahetasin taustapildi ja teostasin taaskäivituse, et kontrollida, kas arvuti on töökorras ka pärast sulgemist.

3. Viited

[1] https://nordvpn.com/blog/how-to-password-protect-a-zip-file/