TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Mikk Oliver Kõiv 212978IAAB

Konteinertehnoloogia baasil ründesimulatsioonitarkvara loomine küberõppusele

Bakalaureusetöö

Juhendajad: Siim Vene
MSc
Jaanus Kääp
MSc

Tallinn 2025

1 Töö eesmärk

Küberõppused on tegevused, mille eesmärgiks on välja selgitada osalejate vastuvõtlikkus küberohtudele ja harjutada küberohtudele reageerimist turvalises keskkonnas. Küberõppused viiakse üldjuhul läbi õppuse tarbeks ettevalmistatud küberharjutusväljakul, mis võimaldab osalejatel teha kõiki tegevusi oma organisatsiooni toodangukeskkonda mõjutamata. Küberõppused erinevad nii läbiviimismeetodi kui ka tehnilise poole pealt. Lõputöö raames arendatud simulatsiooni kasutati tehnilisel küberõppusel, mis viidi läbi küberharjutusväljakul ning mille osalejatel tuli lahendada erinevaid realistlikke küberintsidente imiteerivaid stsenaariume. Õppusel osalejate ülesandeks oli tuvastada arendatud simulatsiooni tegevus oma võrkudes ja rakendada meetmed simulatsioonitarkvara edasise leviku tõkestamiseks ning selle eemaldamiseks.

Küberturbe õppusele on vaja luua senitundmatu ja toimiv ründesimulatsioon. Loodav simulatsioon peab imiteerima pahavara, mille eesmärk on õppuse süsteemidest välja tuua teatud märksõnadega faile. Õppusel osalejad peavad tuvastama simulatsiooni ning tegema koostööd teiste osalejatega pahavara edasise leviku tõkestamiseks ja selle eemaldamiseks. Lisatingimusena peab arendatav simulatsioon olema lahendatav päevaga, sealhulgas tuvastamine, analüüs, leviku tõkestamine ja süsteemidest eemaldamine.

2 Kasutatud metoodikad

Kuna ülesandeks on uue simulatsioon loomine, on kasutatava lahenduse metoodikaks valitud prototüüpimine. Prototüüpimisel on oodatav, et loodud lahendus on kontseptsioon. Loodud prototüübile võib leiduda mitmeid edasiarendusi, mida oleks võimalik tulevikus rakendada.

Lahenduse arendamisel tugineti peamiselt avalikest allikatest leitavale informatsioonile, mis puudutab eelkõige konteinertehnoloogia platvorme, konteinerkeskkonnast põgenemise meetodeid ja simulatsiooni mällulaadimise võimalusi. Samuti analüüsiti konteinertehnoloogiat, tuvastamaks tehnoloogias oleku erinevusi *host* süsteemiga. Loodud lahenduse jaoks loodi konteinertõmmis, mille käivitamisel simulatsioon mällu laetakse. Mälust hakkab simulatsioon teostama oma etteantud toiminguid. Simulatsioonile ligipääsuks on võimalik kasutada HTTP protokolli.

3 Lõppjäreldused

Lõputöö tulemina loodi toimiv ründesimulatsioon, mis toob õppuse süsteemidest eelnevalt määratletud otsisõnade järgi faile välja ja kuvab neid loodud HTTP proksi kasutajaliideses. Proksi kasutajaliides võimaldab käskude konteineris käivitamist. Konteinertehnoloogia valiti toimetamise viisiks demonstreerimaks, mis võib juhtuda, kui laetakse alla ja käivitatakse verifitseerimata konteinertõmmiseid. Kokku kulus simulatsiooni arendamiseks üle 40 tunni. Konkreetse simulatsiooni arendamiseks läinud aega võib tulenevalt simulatsiooni mahtu, raskusastet ning võimekust arvestades pidada mõistlikuks arendusajaks, mida on võimalik raskendada ka teiste sarnaste simulatsioonide arendamiseks.

Loodud simulatsioonil on mitmeid erinevatele küberõppustele ja infoturbe koolitustele edasiarendus- ja kohandamisvõimalusi.