
Küberkaitse lipuvõistlus

Meie meeskond

- **projektijuht** (korraldab tööd, suhtleb kliendiga, esitleb lahendust teistele, viib läbi võistluse koos teiste abiga)
- **analüüsija** (tegeleb nõuete analüüsiga, lahenduste väljatöötamisega, küsitleb huviliste soove ja tagasiside, testib ülesanded)
- **administraator ja seadistaja** (paneb IT-süsteemid tööle, seadistab need, testib ülesandeid, viib läbi võistluse tehnilise poole)
- **sisulooja** (loob võistlusele stsenaarumi ja ülesannetele sisu)
- **kvaliteedi kontroll/vastavusnõuete testija** (loob hindamisjuhendi, kontrollib, kas nõuete analüüs, pakutud lahendus ja IT-seadistused on tehtud nagu on kokkulepe, testib ülesanded, hindab tulemust)

Ülesanded projektis

- Uurisime oma kasutajagruppi ja nende huvi. Sooviti mängida päris CTF võistlust.
- Keskkondade kasutama õppimine: Vastavalt oma eelnevatele tehnilistele oskustele ja kogemustele ning ka kasutada olevale ajale, otsustasime õppida tundma CTFd lahendust (tasulist)
- Ülesannete loomine:
  a. lõime ülesanded paberil ja testisime neid fookusgrupi peal (oma mängu hilisemad kasutajad), tegime parandused
  b. panime ülesanded digitaalselt kirja koos lisainfoga, testisime neid
  c. sisestasime ülesanded CTF keskkonda ja testisime neid
- Viisime läbi võistluse ja küsisime tagasiside

Persoonad

Persoona: õpetaja
Arvutiõpetaja, õpetab küberturvalisust ja digitaalset ohutust ning informaatikat. Ta on saanud oma oskused õppides Tallinna Ülikoolis, kuid täiendanud on ta ennast ka Tallinna Tehnikaülikooli ja Tartu Ülikooli erinevatel didaktika kui ka IT-kursustel. Eriliselt huvitab teda sotsiaalne manipulatsioon ja infosõda, et noored oleksid sellest teemast teadlikud.
Persoona: õpilane 1
Poiss, 11 klass. On osalenud varem CTF-võistlustel. Huvitub, kuidas läbi viia ise CTF lipuvõistlust ehk luua sinna häid ülesandeid. Puutub kokku erinevate IT-teemadega, sest aitab koolis IT-toega. Tema poole pöörduvad nii õppijad kui õpetajad. Eriliselt huvitab teda krüptograafia ning ta soovib minna edasi õppima küberkaitset.
Persoona: õpilane 2
Tüdruk, 9 klass. Ei ole varem CTF-võistlusega kokku puutunud, aga teda huvitavad igasugused STEAM teemadel võistlused. Ta ei ole nendes kõige parem, aga saab iseseisvalt hakkama. Vahel isegi paremini kui poisid! Teda huvitavad nutiseadmete turvalisus, isikuandmete kaitse ja kuidas internetis turvaliselt hakkama saada.
Persoona: õpilane 3
Poiss 7. klass. On arvutimängur ja on kokku puutunud erinevate viiruste ja probleemidega arvutis. Võib ennast nimetada algajaks IT-huviliseks, aga tegelikult talle meeldib ikkagi pigem mängida. Soovib teada saada, kuidas oma arvutit turvata ja kuidas mitte sattuda mängudes küberpettuste ja manipulatsiooni ohvriks.

Kasutajate vajadused

CTF-võistluse vastu huvi	õpetaja	Õpl 1	Õpl 2	Õpl 3
Paroolid ja nende hoiustamine	x	x	x	x
Nutiseadmete turvalisus	x	x	x	x
Arvuti turvalisus	x	x		x
Hea käitumine internetis	x		x	x
Krüptograafia		x		
Infosõda	x	x		
Isikuandmete kaitse	x	x	x	x
Sotsiaalne manipulatsioon	x	x	x	x
Muu	x	x	x	

Mängu stsenaarium - Aasta 2007. Pronksiöö simulatsioon - küberrünnakud Eesti vastu.

Pronksiööna tuntakse 2007 aastal peamiselt Tallinnas toimunud tänavarahutusi, mille lisandiks olid küberrünnakud. Rahutuse ajendiks olid 26. aprillil Tõnismäe haljakul pronkssõduri juures tehtud ettevalmistused sinna 1945. aastal maetud Punaarmeelaste säilmete arheoloogilise väljakaevamise ja identifitseerimise alustamiseks.

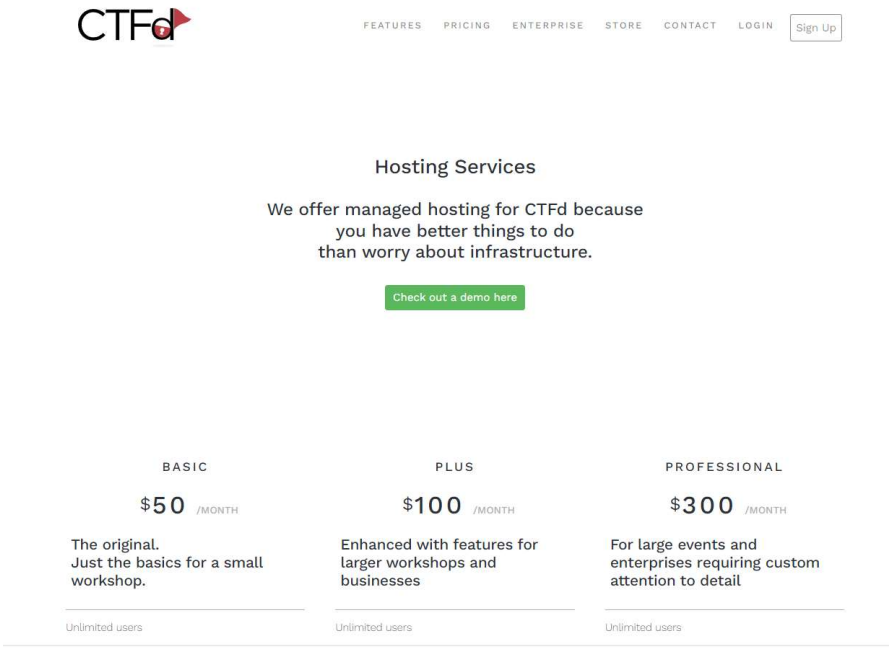
Toimunud küberrünnakud olid Eesti riigiasutusete, organisatsioonide arvutivõrkude ja nende pakutavate e-teenuste vastu (Riigikogu, presidendi, ministeeriumite, politsei, suuremate pankade ja uudisekanalite ning kommunikatsioonieттevõtted). Esialgsed rünnakud ei olnud tehniliselt keerukad, piirdudes spämmi ning kübervandalismiga, kuid toimus ka keerulisemat. 3. mail sattusid lisaks valitsusasutustele rünnaku alla eraettevõtted. Rünnakute haripunkt oli 9. mai. Monumendi teisaldamine põhjustas ägeda tüli Eesti ja Venemaa vahel.

Oled Kaitseliidu Küberkaitseüksuse salajane abiline, kes kutsutakse eksperdina appi nii riigi kui eraettevõtjatele, et hoida üleval vajalikud teenused, paigata serverid ja leida pahalased, kes on süsteemides sees. „Sinu eesmärk on aidata lahendada ära kõik mured, mida sinu lauale veeretatakse, kaitstes sellega Eesti riiki – Eesti e-riiki.“

Eelvoorus toimuvad erinevad lihtsamad tegevused 26.aprill-8.mail. Võistleja saab kasutada vihjesüsteemi, et ülesandeid lahendada, aga vihjed maksvad punkte. Põhivoorus toimuvad tegevused ühel päeval 9. mail. Võistluse ajal ära jäta tähelepanuta ka lisainfot, mida jagatakse (uudised, videod, teated).

Mängukeskkonna ülespanek

- Valisime lahenduseks baaspaketi 50 EUR kuus
- Kuna ei soovinud kogu aeg keskkonna eest maksta, siis panime üles ka omale arvutisse lahenduse, milles lõime ja testisime ülesandeid.



Ülesande näidis (harjutamiseks)

KIRJELDUS

Ülesanne lahendatatav siin: https://jouluvanake.blogspot.com

Lipp on kujul: KP22-...

KONTROLL

Sisesta lipp kontrollimiseks | Kontrolli

Näiteid ülesannete teemadest:

- Non-blind SQL injection – võistleja peab kasutama ära lihtsamat korralikult töötlemata sisendit SQL lause käitumise muutmiseks
- Android APK reverse-engineering - võistleja peab pakkima lahti Androidi rakenduse mis on .apk kujul ja leidma selle ressursidest (nt. strings.xml) vajaliku üles leidma
- OSINT – Fotol või muul sarnasel sisus olev info võimaldab paari-kolme sammuga tuvastada mingi saladuse (vms.) mis võimaldab liigset ligipääsu nt. FTP serverile
- Email forensics – Antud e-maili konto varukoopia (vms.) analüüs toimunu selgitamiseks. Lihtsam sõnaotsing/grep (nt. Outlook'i .pst fail)
- Malware forensics – Lihtsama pahavara(perekonna) tuvastamine (kuid mitte keeruline reverseengineering, keerulisem võiks olla pigem osa lõppvoorust)
- Path traversal - võistleja peab leidma veebirakenduses oleva path traversal turvaaugu ja sellega vajaliku faili välja lugema.

Riskid projektis

Lipud võistlusel on ebastandartsed. Viisime läbi eeltestimise ja parandasime vead.

Server jookseb kokku. Kuna ei lahendanud võistlust oma arvutil vaid kasutasime CTFd lahendust, siis kõik toimis hästi.

Võistlejad on ebaviisakad ja ei kuula sõna – ei realiseerund

Võistluse läbiviimine

Korraldasime 16 ülesandega 1 tunnise võistluse

Osalajaid oli 6 võistlonda (igas 3 liiget)

Panime paika reeglid:

- iga võistkond või võistleja osaleb võistlusel lubatud nimega (keskkond, abikanal), mis ei ole kellelegi solvav
- iga võistleja/võistkond lahendab ülesanded ise ilma kõrvalise abita
- võiskeskkonda ja teiste osalejate arvuteid või isikuid (suhtluses/jututoas) rünnata tehniliselt ega solvata ei või
- teiste võistkondadega koostööd ülesannete lahendamiseks teha ei või
- ülesannete lahendusi ja lahendussoovitusi teistega jagada ei või võistluse ajal ega ka peale võistlust
- vihjed maksavad võistlusel punkte, kasutage neid alles siis kui on väga häda käes

Tunnistus

- Näide

TUNNISTUS

RIIKLIKULT TUNNUSTATUD
TEADUSE POPULARISEERIJA 2022

KAITSEMINISTEERIUM

NIMI, NIMESTE

Võistluse nimi

I koht

Eesti Interneti SA

Aeg

Korraldaja

Allkiri

Hindamine

Küsisime võistlusel osalejatelt tagasiside, mis oli 90% positiivne

Soovitati:

Teha võistlus pikemalt	Luua lihtsamaid ülesandeid	Anda välja auhindu