

Terminaaali

4/20



Päätoimittajan jäähhyväiset	3
Puheenjohtajan päiväkäsky	4
Talolla jutustelua	6
TOP 3 tähtikuviot	8
Pukinkonttiin sitä oikeaa RetroAutismia™	10
Kurssiarvosteluja	14
Vieraileva kolumnisti22: Joululoma	16
Esittelyssä: Capture the Flag	18

Terminaali Oulun Tietoteekkarit ry:n kiltalehti

pää-äänenkannataja jo vuodesta 1988

4-6 numeroa vuodessa

33. vuosikerta

Numero 4/2020

Painomäärä 30kpl

Painopaikka: Monisto

Osoite:

Oulun tietoteekkarit ry/Terminaali

PL4500 90014 Oulun Yliopisto

Päätoimittaja

Santeri Hyvärinen

Toimittajat

Bekim Abazi, Saku Salo,

Tomi Lehto, Niklas Riikonen,

Aleksi Tuovinen, Riina Annunen,

Jenna Onnela, Jukka Pajukangas

Kannet

Heikki Kaarlela

Päätoimittajan jäähhyväiset

Lumi on laskeutunut oulun ylle (ainakin hetkeksi). Ja vuosi alkaa lähestymään loppua, niin on tullut myös terminaalin tältä vuodelta. Samaan aikaan päättyy myös minun urani päätoimittajana, sillä siirryn toisiin tehtäviin ensi vuonna. Mutta onneksi tilalleni tulee uusi ja noheva fuksi.

Vuosi on ollut pitkä aika ja terminaalin taittaminen ja tuottaminen on ollut erittäin mieluisaa puuhaa, paljon on opittu ja paljon on opittavaa. Toivottavasti olette nauttineet laadukaan kiltalehden antimista tänäkin vuona. Vaikka urani päätoimittajana päättyy, en pystynyt luopumaan koko terminaalista, joten päädyin jatkamaan toimittajana ja toivon mukaan näin voin vaikuttaa siihen että saadaan ensi vuonakin hyvä kiltalehti.

Näillä sanoilla hyvää joulua ja onnelista uuttavuotta.
- syomasa

Puheenjohtajan päiväkäsky

Kansalaiset, Medborgare,

Kaksi asiaa ovat ikuisia Kulta ja Demokratia, ja jälleen kerran killan demokratia on tapahtunut. Vaalikokous oli ja meni, kansan tahti on tapahtunut ja uudet toimijat on valittu. Toivottavasti kaikki jotka miettivät ehdokkaaksi lähtöä, lähtivät ehdolle ja jos ei, niin toivottavasti mielenkiintoa löytyy vielä vuoden päästäkin. Hyviä hommia nämä on :D. Tietääkseni vielä on pari toimarinakkia on vapaana, jos alkoi vasta nyt kiinnostamaan.

Mutta jälleen tämäkin vuosi, olkoon se ollut kuinka eriskummallinen tahansa, on tulossa päätkseen ja ainakin minulla on ollut paikoin ihan mukavaa, toivottavasti teilläkin. Lähestyvä loma, jos sellaista aiotte viettää, tekee varmasti hyvää meille kaikille. Toivottavasti pysytte terveenä vielä tämänkin kuukauden ja laitetaan nyt kaupan päälle vielä ensi vuosikin.

Jännää miten nuo aikaisemmat 3 päiväkäskyä oli nopea ja helppo kirjoittaa, mutta nyt meinaa loppua juoni 100 sanan jälkeen. Ehkä se on hyvä että minäkin pääsen eläkkeelle ja on ehkä aikaa keskittyä muihinkin projekteihin, voisim noudattaa vaikka kiltahuoneella kuultua neuvoa, mene töihin.

Omasta puolestani kiitoksia kiltalaissille tästä vuodesta. Kiva että jaksoitte katsoa meikän pärstää näinkin pitkälle asti eikä suurempaa kapinahenkisyyttä syntynyt, tai näin minun on annettu ymmärtää. Nähdään kun nähdään ellei näkö mene.

Haikein terveisin,

Saku "sandalf" Salo
Puheenjohtaja, Luiden murtaja, Urkujen aukaisija, Avaimien haltija,
Humpaan soittaja



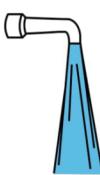
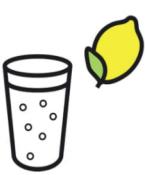
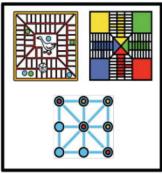
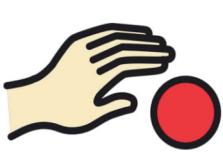
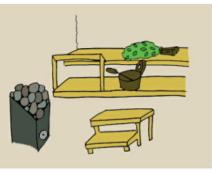
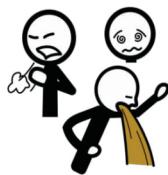
Talolla jutustelua

Oletko joskus ollut talolla nauttimassa mukavasta illasta, mutta tuntunut ettet saa sanottua kaikkea, mitä haluaisit tai tuntunut, että kaverisi on liian humalassa, eikä ymmärrä enää sinua ollenkaan? Tässä on sinulle ratkaisu!

Tässä näet kuvasarjan sanoista/ilmaisuista joita voit tarvita talolla.

Kuvia voit hyödyntää monella tavalla. Voit esimerkiksi osoittaa kuvaa puhumisen ohessa. Mikäli kaverisi on liian humalassa, voit hänelle näyttää näitä kuvia ja pyytää häntä osoittamaan kuvaa, jota hän haluaa sinulle sanoa (tai jos ei saa osoitettua kuvaa, niin kehoita lähtemään kotiin). Jos et keksi mitä tekisit talolla, niin kuvasarjasta saa hyvin vinkkiä :-)

Muistakaa juoda vastuullisesti :)

kaljaan tekis mieli 	Teekkaritalo 	juoda 	ei alkoholia 
viski?? 	lonkerou-juoma 	kaljaa 	omenasiideri 
vesi 	peltikatto 	VIINAA 	jaloviina 
örveltää 	tanssia 	jutella syvälliisiä 	pitää päästää WC 
JUOMAPELI 	Beer Pong 	Sauna 	Palju 
heikko happi 	mennä kotiin 	mitä tuli tehtyä 	liskojen yö 

TOP 3 Tähtikuviot



1. Kolmen tähdien kuvio

Tämä kolmen tähdien kuvio on mielestäni yksi kauneimmista, mitä maapallomme päällään kantaa. Tähdet ovat toisiinsa nähden kauniissa suorassa linjassa. Vaikka tätä tähtikuvioita ei voikaan välttämättä tavata sunnuntaisin (koska silläkin on lepopäivä) on se suurissa määrissä nähtävinä arkena ja lauantaisin useassa eri paikkaa.

2. Kahden tähdien kuvio

Tämä kolmen tähdien kuvion sisarkuvio on sen sijaan jo paljon harvinaisempi. Tämä kuvio koostuu kahdesta kauniisti linjassa olevasta tähdestä, jotka loistavat kirkkaimpina pimeimpinä öinä. Kuten sanottu, tämä kuvio on harvinainen. Jotkut vanhemmat tähtibongaaajat kuitenkin kertovat urbaanilegendaa, että tämän kuvion olisivat joskus päässeet livenä näkemään.





3. Yksinäinen kuvio

Tästä tähtien kuviosisarparvesta yksi joutui erilleen. Kaukana muista on hän kirkkahasti loistanut, vaikka surullisesti yksin joutuu olemaan. Seuraavan kerran, kun maljaa nostat sinä, muistele häntä mielessäsi ja skoolaa hänen kunniakseen. Harvinainen kuitenkaan hän ei ole, vaan tätä yksinäisyyttä näkee samalla tavalla kuin kolmen tähden kuviota. Mars siis bongaamaan.

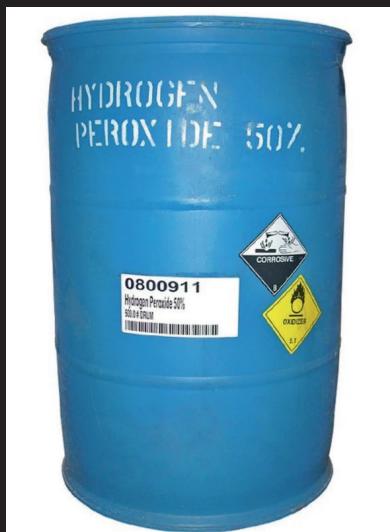
Artikkelin on kirjoittanut tähtitietäjä Jalo Viinasmus

Pukinkonttiin sitä oikeaa RetroAutismia™

Oletko huono keksimään lahjoja itsellesi tai kaverillesi? Etkö tiedä paljoa retrokonsoleista tai -peleistä? Ei häitää, me RetroAutistit™ autamme sinua keksimään mitä parhaimmat retrolahjat! Meidän vinkeillä saat zoomeritkin kiinnostumaan kivikautisista peleistä.

Capturehimmelit

Mikäli ette vielä uskalla siirtyä CRT:n ihmeelliseen maailmaan ovat capturehimmelit melkein yhtä hyviä retropelailuun. Capturehimmelit ovat myös oleellinen osa streamaussetuppiä, jos maailmanennätysten takominen speedrunnaamisella kiinnostaa. Tässä kategoriassa suosittelemme RetroTINK:iä taikka OSSC:aa, jotka molemmat ovat oikein hyviä ratkaisuja retrokonsoleiden outputin siirtämisessä nykyaan. Capturehimmelit ovat hiukan tyyriitä, mutta meillä on siihen hyvä ratkaisu: **MENE TÖIHIN!**



Vetyperoksiidi

Kellastuneen konsolin vaalentaminen, eli niin kutsuttu retrobrightaaminen on nostanut suosiotaan viime aikoina. Kyseessä on menetelmä, jossa vaalennetaan konsolin muoviosia vetyperoksidin avulla. Jokaiselle retroharrastajalle tämä ei välttämättä ole kaikista helpoin lahja, mutta kovemman luokan RetroAutistilla™ on aina käytööä kunnon purnukalle vetyperoksidia.

Projektikonsoli

Tunnetko jonkun, joka olisi kiinnostunut vanhoista retrokonsoleista? Siinä tapauksessa niin kutsuttu projektikonsoli on mitä mainioin lahja! Projektikonsolia voi käyttää retropelailuun ja modifiikaatioprojekteihin kuten RetroBrightaamiseen. Myös niin kutsuttu hajoaminen paskaan kuuluu oleellisesti retrokonsolien kunnostamisharrastukseen. Myös RGB ja HDMI modien ostaminen jo olemassa olevaan retrokonsoliin on hyvä ja suosittu vaihtoehto. Jos ennen ostoa konsolia ei pääse testaamaan tai katsomaan, voi netti-ilmoituksesta olla hankala päätellä onko konsoli mahdollista korjata tai modata. Tähän ongelmaan emme valitettavasti pysty tarjoamaan kaiken kattavaa ratkaisua, mutta muutamaan piirteeseen voi kiinnittää huomiota.



- Hajonneet muoviosat ja vahva kellaustuminen voivat olla uhka sillä ne voivat viitata haurastuneeseen muoviin.
- Hintaansa nähdyn “liian” hyväkuntoiset yksilöt saattavat olla epäonnistuneita korjausprojekteja, joita voi olla hankala itse enää ehjätä. Sen sijaan törkyiset konsolit voivat yllättää tekniikkansa kunnolla.



Retropelit

Välillä voi olla hankala miettiä, että mitä pelejä sitä hankkisi retrotoverilleen tai itselleen lahjaksi RetroAutismia™ varten. Tämän vuoksi me suosittelemme kiinalaisen flashkortin hankkimista. Miksi? No tietenkin sen takia, että flashkorteilla voi pelata lähes kaikkia retrokonsolin pelejä ikään kuin ne olisivat aitoja sillä ne pyörivät suoraan

raudalla! (Tämä tottakai koskee vain ja ainoastaan omista laillisesti hankituista pelikaseteista tehtyjä varmuuskopioita, sekä vapaasti jaossa olevia niin kutsuttuja homebrew-pelejä.) Kokemusta meillä on SNES kiinafläshkorteista, joita emme voi kun suositella. Hinnat ovat halvasta vähän kalliimpaan.

Työkalusetit

Jokaisella RetroAutistilla™ pitäisi olla jo tarvittavat työkalut retrokonsoleidensa korjaamiseen. Aloittelevalla RetroAutistilla™ voi tosin vielä olla puutteita työkalupakissaan, ja seuraavan listan avulla voitkin auttaa häntää täydentämään sitä:

- Erikoisruuvien kärjet. Yleensä konsolin ulkokuoren ruuvit ovat epätavallisella kannalla, jotta loppukäyttäjät eivät pääsisi koskemaan konsolinsa sisuskaluihin.

Näytä erikoiskärkiä on kuitenkin onneksi helposti saatavilla kiinan verkkokaupoista.

- Lisäksi tavallinen kärkisarja, josta löytyy pieniä peruskärkiä on monesti hyödyllinen.

- Isopropyylialkoholia ja hammasharja piirien ja muiden osien puhdistukseen.

- Lämpösäädettävä kolvi pieniin korjauksiin.



Bittien täyteistä joulua toivottavat RetroAutistit,
matti_ & Sebu_

Kurssiarvosteluja

No terve terve taas meidän rakkaat lukijat. Fuksivuodesta on pyörähtänyt jo tovi niin ajattelin sitten nopeasti arvostella muutamia fuksikursseja. Katsotaanpas mitä toi weboodi näyttää.

Matematiikan peruskurssi I

Vanha klassikko, hyvä kurssi joka luo helpohkon pohjan muille matikoille.

"Jollain oli oma lusikka sopassa" - Timppa Haarukka(nimi muutettu)

Arvosana: 5/5

Sähkömittaustekniikan perusteet

Luennoitsija ei kyllä ollut parhaasta päästä, mutta kuulemma se on vaihtunut. En muista kurssista muuta kuin miten oskilloskooppi toimii ja itse saa tehdä jatkojohdon.

Arvosana: Selitää Offset/5

Matriisialgebra

Matriisi-Masan parasta tuotosta, viihdyttävä kurssi vaikka pidettiinkin salissa L3.

"Silver Fox M.P" - Jodel

Arvosana: Piirtoheitin/5

Ihminen-tietokone -vuorovaikutus

Tämän kurssin idea jäi kyllä aika vaisuksi ja toteutus oli enemmänkin käsienviljeltyä. Ehkä tää on parantunut.

Arvosana: Uulu/5

Johdatus teköälyyn

Luennoitsija oli jees, viikottaiset minikokeet oli aika aamuisia, etenkin just ennen fuksikisoja. Pienellä vaivalla helpot nopat, suosittelen.

Arvosana: A*-haku/5

Eiköhän 5 kurssia ole ihan tarpeeksi, ei tätä kuitenkaan kukaan lue loppuun asti kun ei ole kuvia. Noh nähdään taas ensi vuonna.

Moikkkeliskoikkeli ja morjenksikset sinne.

SEAGAL

VAN DAM

SNIPER

SPECIAL OPS



FSK
ab

16

freigegeben

EUROVISION

Vieraileva kolumnisti22: Joululoma

noniin hyvää huomenta ja nyt on hampaat ja parta ajettu ja kohta äkkiä laitetaan sitten aamukahvit tulille ja täs mä just yritin kattoo et miten ne koulujen ne joululomat oli vuodel sillon vuonna 1990 tai sillon 90-luvulla kun meikäläinenkin asteli kouluun ni yritin kattoo mut ei täältä mitään ei täältä mitään emmä oo mitää vie löytäny sitä ees 2000-luvulta mä yritin kattoo sitä et miten ne 2000-luvulla on noi koulu koulujen lomat koululomat on niinkun et miten ne 2000-luvulla oli ni sit mä löysin että täälläkin koulut koulujen joululomat on vasta 23.12. vasta vasta ne pääsee lomalle joululomalle ne pääsee vasta niin kuin 23. joulukuuta ja sitten heti seuraavana päivänä ku keskiviikko on joulukuun 23. päivä keskiviikko kun koulut kun joululoma alkaa niin heti seuraavana aamuna on jouluaatto torstai ni sillon ne voi viettää sitä ensimmäistä joululomapäiväänsä ja siitä ne on sitten yks kaks kolme neljä viis kuus seittemän kaheksan yheksän montako arkipäivää sitte yks kaks kolme neljä viis kuus seittemän yheksän

yheksän arkipäivää noin viikko niillä on joulukuusta yks kaks kolme yks kaks kolme neljä viis kuus seittemän kaheksan yheksän kymmenen ykstoista ootaa nytte yks kaks kolme neljä tossa on nyt neljä yks kaks kolme neljä viis kuus seittemän kaheksan yheksän kymmenen yytoo kaatoo kootoo noin kolmetoista päivää on joululomaa sitten eiku joo-o yks kaks kolme neljä vii kuu sei kasi yheksän kymmenen ykstoista päivää joululomaa on vain yhteensä viikonloput laskien mukana kun täällä joo ykstoista tai kakstoista yks yks kakstoista noin suunnilleen ykstoista viiva kakstoista arkipäivää on vain joululomaa sitten tiedossa kun ku se on eiku hetkinen eieiei oottakaas nytte nyt mää lasken udestaan yks eiku kyllä se menee kyllä se menee yks kaks yks kakskytneljä yks kaks kolme neljä viis kuus seittemän kaheksan kaheksan yheksän kymmenen ykstoista kakstoista hetkinen nyt mä lasken ihan väärin tosta yks kaks kolme neljä viis kuus seittemän kaheksan yheksän kymmenen yytoo kaatoo kootoo kolmetoista noin kolmetoista tai

neljätoista päivää niin tota on sitten sitä sitten sitä joululomaa eiks oo hienoo että täälläkin on näin vähän joululomaa vain viikko viikko tai kaks melkein kaks viikkoo joululomaa sitten on vain mutta ei siitä nyt sitten sen enempää siitä asiasta mutta tulipahan se nyt tarkistettua sitten yhtään en muista sitä omaa omaa että oliko mulla pitempi oliko mulla paljon pitempi kuin se vain se hikiset kaks viikkoo mutta ei siitä nyt sen enempää mää rupeen nyt tässä laittaan aamukahvia tulille ja puurot tulille nyten sitten nii nyt sekä on sitte tarkistettu sekä homma sitte on tarkistettu se että on se kyllä jännä että se kiristetään noin pitkälle tarkottaakse sitä että tietyissä kun tietyissä tietyissä uskonnoissa ei joulua vietetä ollenkaan meneekö suomi siihen kans että joulua ei vietetä ollenkaan että ollaan koko joulu aika koulussa ku se kiristetään joululomakin kiristetään noin pitkälle että pidetään pitää olla koulussakin noin pitkään että joulu että ollaan melkein jouluaattoon koulussa onko se ens vuonna sitte et ollaan vielä jouluaattonakin koulussa mutta ei siitä sen enempää yhtään en tiedä miten noi lukiolaiset on mutta nyt ku on tää tämmönen

tietty tilanne ni ois ne nyt tässä tässä tietyssä tilanteessa voinut nipistää ja päästää lapset jo aikaisemmin joululomalle ku on tää tilanne on tämmönen on tää tilanne vähän tämmönen että ei viittis pitää niitää siellä siellä lomalla taiko eiku koulussa ku on tää tilanne tämmönen et tää pitää saada nyt tää tilanne nyt rauhottuun ni pääsis päästääs pääsis suomi vähän niinku pikkuhiljaa normalisoitumaan mutta jos tällanen tilanne vaan tulee ku mä oon kattonu katoin että suomessaki on taas yli 200

tapahtumaa on taas taas ollu tässä kakkosaallossa nyten yli 200 ollu tartuntaa on yli kaksisataa ollut suomessakin jo eli etteiks oo näin jos suomessaki on yli 200 tartuntaa ni on se hurja määrä hurja määrä sitte on se kyllä on se kyllä jännä että näin näinki se vaan leviää tää niin saatani sikiää sitte näin nyt otetaan tästä pillerit naamariin ja sillä sitten päästäään eteenpäin kaksi tällaista aikuisten namia naamariin...

Esittelyssä: Capture the Flag

Erikoishaastattelussa CTF-pro Jari Jääskelä

Mikä on hauskempaa kuin istua yksin kämpillä 24/7? No istua yksin kämpillä 24/7 koneen ääressä haxaamassa CTF! Kaiken ihmiskontaktin välttäminen on nyt vieläpä sosiaalisesti hyväksyttyä. Mutta mitä on tämä mystinen CTF? Se selviää juuri nyt



CTF eli "Capture the Flag" ei ole pelkästään tietokonepeleissä tai pihaleikeissä käytettävä pelimuoto, vaan sillä voidaan tarkoittaa myös tietokoneilla ratkaistavien "hakkerointihäasteiden" selvittämistä. Häasteissa on tavoitteena löytää jokin tietty kohde, yleensä tekstinpätkä (eli "flagi"), joka toimii merkinä haasteen suorittamisesta. Perusidea on siis todella yksinkertainen, mutta kaikki muu siinä ympärillä tekee asiat

kiinnostavaksi. Minkälainen on sitten tyypillinen CTF-haaste? Suoraa vastausta ei ole, koska haasteet voivat olla todella toisistaan poikkeavia. Muutamia yleisimpiä kategorioita häasteille kuitenkin voidaan katsoa olevan olemassa. Huomaa kuitenkin, että haasteiden ei ole pakko noudattaa mitään kategoriarajoja tai mitään luokitteluja ollenkaan (eikä tämäkään listaus ole kattava).

- * **Steganografiaan**
liittyvissä tehtävissä etsitään esimerkiksi kuviin tai äänitiedostoihin erilaisilla tekniikoilla piilotettua informaatiota.
- * **Reversauskseen**
liittyvissä haasteissa pyritään jollakin tavalla takaisinkääntämään tai muutoin analysoimaan kohteena olevan binäärikoodin toimintaa flagin löytämiseksi.
- * **OSINT (Open Source Intelligence) -haasteet**
on tarkoitettu ratkaistavaksi julkisesti saatavilla olevan tiedon pohjalta, esimerkiksi sosiaalista mediaa, hakukoneita tai julkisia tietokantoja hyödyntämällä.
- * **“Binary exploiting”** (käytetään myös termiä pwn)
-tehtävätyypissä pyritään löytämään haavoittuvuus ohjelmasta (esim. pinon ylivuoto) ja ”hakkerointamaan” ohjelma sopivalla sytteellä (googleta vaikka ”shellcoding and ROP”).
- * **Kryptologiahaasteissa**
tarkoituksena on purkaa salattu materiaali. Purkaminen voi onnistua esimerkiksi käytetyn salausalgoritmin puutteellisen implementaation vuoksi.
- * **Forensiikkaan**
liittyvissä haasteissa tutkitaan esimerkiksi muistidumppien tai verkkoliikennelogien avulla mitä järjestelmässä on tapahtunut aikaisemmin. Myös kadonneen/ rikkinäisen datan palauttamiseen liittyvät tehtävät ovat mahdollisia.
- * **Web-haasteet** liittyvät jollakin tapaa verkkoturvallisuuteen, kuten esimerkiksi XSS-, CSRF-, Path traversal- tai SQL-haavoittuvuuksiin.

Miksi tätä sitten kannattaa harrastaa?

Ensisijaisesti tämä on hauskaa*, mutta niin on moni muukin asia.

Harrastuksissa ei ole tietenkään pakko olla mitään järkeää, mutta hauskan lisäksi tämä on myös opettavaista.

Haasteilla on useimmiten jonkinlainen liittymäkohta oikean maailman ongelmiin (vaikka välillä tiettyä keinotekoisuutta ei voi välittää), tai sitten ne toimivat muutoin vain hyödyllisenä aivojen venyttelynä.

**Tai siis... riippuu vähän mikä on käsitelyksesi hauskuudesta. Jatka lukemista niin ongelma selvinnee.*



Mikä sitten on ikävää?

Jumiin jääminen haasteissa on yleistä ja erittäin turhauttavaa. Oikeaan suuntaan löytäminen saattaa olla todella vaikeaa jos ei ole mitään hajua suunnasta johon pitäisi lähteä.

Joissakin haasteissa oppimiskynnys saattaa olla hyvin korkea (eikä haasteessa tietenkään etukäteen paljasteta mitä pitäisi oppia ennen kuin asia aukeaisi). Yksi jokaisen harrastajan jossain vaiheessa kohtama ongelma on myös oikean flagin tunnistaminen. Välillä flagin onnistuu löytämään huomaamattaan, jolloin tulee hakkaamaan päättääni umpikujan

seinään niin kauan kunnes tajuaa katsoa taakseen. Tämä harrastus vaatii siis sietokykyä epävarmuudelle, turhautumiselle ja toistuville epäonnistumisille.

Capture the flag experience



Mitenkäs sitten alkuun? Ensin on tietenkin löydetvä CTF-haasteita jostakin. Jokin sopiva palvelu, josta löytyy eritasoisia haasteita tarpeeksi ja mahdollisesti pistelasku oman "rankin" seuraamiseksi (mikä motivoi mukavasti) lienee hyvä valinta.

Entäs välineistö? Tietokoneen tarvitset tottakai, eikä sen tarvitse edes olla himo turbo nörtin eeppinen numeron murskaaja mylly. Erelaisia työkaluja sen sijaan tarvitsee paljon. Oikean työkalun löytäminen/tietäminen on usein tärkeä osa haasteiden ratkaisua. Ottamalla itselleen esimerkiksi Kali Linuxin virtuaalikoneeksi saadaan ihan asiallinen pohja työkalupakille.

Google auttaa todennäköisesti paremmin alkuun pääsemisessä kuin minä tällä tekstillä. Eiköhän sieltä löydy etsijöille avuliaat listaukset palveluista, työkaluista ja foorumeista.

Tässäpä perusjutut, seuraavaksi haastatellaan CTF-pro **Jari Jääskelää**.



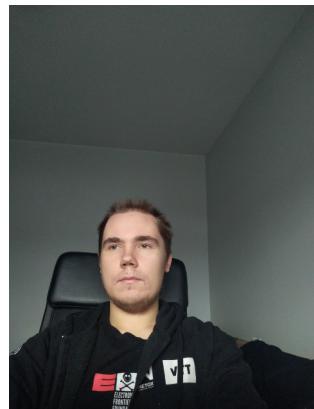
Jari Jääskelän haastattelu

Kuka?

Jari Jääskelä

Opiskelin tietotekniikkaa 2017 - 2020 Oulun yliopistossa, valmistuin alkuvuodesta. Ennen sitä opiskelin sähkötekniikkaa Ylivieskassa (2013-2017).

Parhaiten minut tavoittaa Discordista:
jaras#4730



Mitä hommailet?

Nykyään työskentelen osa-aikaisena OUSPG:llä lähinnä tietoturva-asioiden parissa ja siinä sivussa teen kaiken maailman sovelluskehitystä.

Vapaa-ajalla tulee myös nykyään tehtyä jonkin verran bug bounteja, eli haavojen löytöä ja niiden raportointia palkkiota vastaan. Yleensä tämä on hyvin turhauttavaa, mutta mahtava fiilis jos löytää jotain :)

Mikä "ränkki"?

"Virallinen" ranking on ctftime.org-sivulla. Ranking täällä on tiimi kohtaisesti. Salty Cabbages -tiimin kanssa ollaan osallistuttu vain yhteen CTF:ään, jolla päästiin 4. sijalle Suomen rankingissa, mikä ei paljoa vaatinut :). HackTheBox:ssa on tullut nyt 2 vuoden aikana ~50 konetta korkattua, paras rankkini taisi olla ~150. kansainvälisesti ja 1. Suomessa noin 1,5 v sitten. [1]

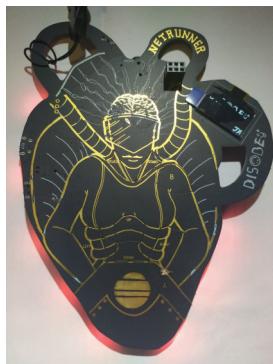
Mikä oli eka CTF/harrastuksen alku?

Tästä on jo muutama vuosi, oisikohan ollut joskus 2012-2014 root-me.org-sivulla, missä on hyvin paljon erilaisia haasteita. Joskus on tullut myös crackme-haasteita (reversaus) tehtyä cracmes.de and tuts4you.com -sivuilla. Ensimmäinen varsinaisen CTF, mihin panostin taitaa olla 2017 pico ctf, mikä on aloittelijoille suunnattu.

Mitä CTF-juttuja tällä hetkellä?

Nyt ei ole ollut paljon aikaa CTF-juttuille. Seuraavaksi pitäisi löytää motivaatio tämän vuoden Disobeyn puzzlea varten :).

Disobey on vuosittainen Helsingissä järjestetty tietoturvatapahtuma. 50 ensimmäistä puzzlen suorittajaa, jotka lunastavat palkkion saavat hienon hacker badgen ja pääsyliipun alennettuun hintaan. Disobeyssä järjestetään myös CTF, missä on hienoja tunkkeja palkintona . Viime Disobeyssä (helmikuu, 2020) lähdin tähän CTF:ään mukaan muutaman muun kanssa Netoxelta ja VTT:ltä. Päästiin kolmossijalle.



Millainen on ollut vaikein kohtaamasi tehtävä?

Vaikeita haasteita on hyvin, hyvin paljon ja suurin osa näistä on jänyt ratkaisematta :). Muutamia haasteita mitä on mieleen jänyt, niin on viime vuoden OverTheWiren joulukalenteri CTF:ssä.

Yhdessä haasteessa täytyi huijata pelissä manipuloimalla verkkoliikennettä. Tämä käytti jonosalusta (stream cipher) ja IV (initialization vector) lähetettiin langan yli ennen salausta, niin tästä manipuloimalla ja korreloimalla useita viestejä pystyi purkamaan salauksen ja väärentämään liikennettä. Pelin lähdekoodia tai binääriä ei tietenkään ollut saatavissa, niin tämä vähän hankaloitti

tätä haastetta. Yksi toinen mielenkiintoinen oli viime vuoden Disobey puzzlen reversaus osuus. Tässä täytyi kaivaa lippu bootloaderista. Suoritin tämän emuloimalla bootloaderin käyttäen Unicornia. Vaihtoehtoisesti tässä olisi voinut käyttää qemua tai bochsia. Tässä writeup tästä: <https://jarijaas.github.io/posts/disobey-2020..>

Tiukat vinkit aiheesta kiinnostuneelle opiskelijalle:

Ensimmäisenä täytyy tietenkin mainita, että suorittamalla Oulun yliopiston CompSec-kurssin saa tosi hyvän CTF-pohjan :). Kannattaa tietenkin harjoitella perustaitoja eri osa-alueilta. Parhaiten tietenkin oppii tekemällä, niin kannattaa aloittaa haasteista, joista löytyy writeup, niin turhautuessa voi luntata. Näitä haasteita löytyy hyvin paljon netistä. Esimerkkinä hacker101 aina avoin CTF [2], joka keskittyy web-sovelluksiin.

ctftime.org:sta näkee tulevat CTF-kilpailut ja writeuppeja vanhojen kilpailujen haasteista, niin tähän sivustoon kannattaa tutustua. Tällä on myös paljon aloittelijoille suunnattuja CTF:iä, mistä pääsee hyvin CTF:iien makuun.

Taitoja voi myös harjoitella HackTheBox:ssa ja TryHackMe:ssa. Täältä siis löytyy myös vähän sitä perinteistä CTF:ää realistisempaa tavaraa. TryHackMe [3] ja SANS [4] järjestää nyt haasteita joulun aikaan, niin kannattaa myös tutustua näihin.

Jos haluat keskustella aiheesta, niin tuki voi ottaa yhteyttä jaras#4730

[1] <https://www.hackthebox.eu/profile/116576>

[2] <https://www.hacker101.com>

[3] <https://tryhackme.com/room/adventofcyber2>

[4] <https://holidayhackchallenge.com/2020/>

Kiitoksia Jarille, onnea matkaan ja hyvää joulua minunkin puolestani.
- Paju







