



FOI MEMO

Projekt/Project
Strategisk verksamhet i Crate 2022 –
Crate-CTF MSB

Sidnr/Page no
1 (9)

Projektnummer/Project no Uppdragsgivare/Client
E7161733 MSB

FoT-område
Inget FoT-område

Författare/Author
Christoffer Lauri

Datum/Date
2022-12-14

Memo nummer/Number
FOI Memo 8073

Genomförande Crate-CTF 2022

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

1 Inledning

Detta memo beskriver genomförandet av *Crate-CTF 2022*. *Crate-CTF* är en tävling inom it-säkerhet som genomförs av FOI och som under 2022 gick av stapeln den 26 november. Tävlingen finansierades i år av Myndigheten för samhällsskydd och beredskap (MSB). Årets tävling utgjorde det tredje genomförandet av *Crate-CTF*, där de tidigare två tävlingarna genomfördes år 2020¹ och år 2021². Tävlingen år 2020 benämndes dock inte *Crate-CTF*, utan som *20/20 CTF*. Till 2021 genomgick tävlingen ett namnbyte till *Crate-CTF*.

Syftet med att genomföra årets tävling var att vidareutveckla den kunskap om CTF-formatet som erhöles från de tidigare genomförandena. Tanken är att denna kunskap sedan kan användas för olika ändamål, exempelvis för att verifiera kompetens vid rekrytering eller väcka intresse för cybersäkerhet hos potentiella medarbetare som kan förstärka totalförsvaret. Målgruppen hos vilken tävlingen ska väcka intresse, inkluderar både personer som redan idag jobbar inom angränsande områden till cybersäkerhet, men framför allt gymnasieelever samt högskole- och universitetsstudenter som är på väg att välja arbetslivsinriktning. Utöver detta kan tävlingen även användas som forskningsplattform och de uppgifter som produceras har visat sig kunna återanvändas i andra projekt.

1.1 Format

Tävlingens format utgår från det som på engelska kallas för *Capture the Flag* (CTF). CTF-formatet kan delas upp i olika typer. Den typ som nyttjas för *Crate-CTF*, som även är en av de vanligast förekommande, är det så kallade *Jeopardy*-formatet. *Jeopardy*-formatet går ut på att deltagare, enskilt eller i lag, tävlar om att lösa olika säkerhetsrelaterade uppgifter. Samtidigt innehåller formatet inte någon uppgiftsrelaterad interaktion mellan olika lag. Varje uppgift går ut på att deltagare ska hitta en så kallad *flagga*. Ofta implementeras flaggor som dolda eller skyddade textfraser i de it-system som utgör uppgifterna. När deltagare har funnit en flagga rapporteras denna in till CTF-plattformen och om flaggan är korrekt tilldelas deltagaren poäng. Tävlingen pågår under en förbestämd tidsperiod, vilket innebär att alla uppgifter inte måste lösas för att utse en vinnare. Det lag med flest poäng när tävlingen avslutas vinner tävlingen. Deltagarna kan själva välja i vilken ordning de löser uppgifterna.

1.2 Teknisk infrastruktur

Crate-CTF 2022 kördes i den nationella cyberanläggningen *Crate*³ som är belägen vid FOI i Linköping. Nyttjandet av *Crate* tillgängliggjorde bland annat den hårdvara som användes för att köra tävlingens uppgifter. För *Crate-CTF 2022* nyttjades samma server som i 2021 års genomförande, *Utopia*. Denna server var utrustad med 40 CPU-kärnor på 2.2 GHz, 256 GB RAM samt ZFS RAID med SSD-hårddiskar.

Vissa uppgifter kördes som nätverkstjänster som deltagarna kopplade upp sig mot för att lösa utmaningarna. Dessa nätverkstjänster exekverade i Docker-containers⁴ för att isolera tjänsterna samt öka portabiliteten. Ett möjligt lösningssätt i en av uppgifterna i årets genomförande var att bli *root*-användare i uppgiftens Docker-container, varför den uppgiften placerades på en molntjänst för att inte riskera störa andra uppgifter. Molntjänsten har även använts under tidigare års genomföranden,

¹ Lundberg T. (2020). *20/20 CTF*. FOI Memo 7344. Totalförsvarets forskningsinstitut (FOI).

² Valassi C. (2022). *Genomförande Crate-CTF 2021*. FOI Memo 7837. Totalförsvarets forskningsinstitut (FOI).

³ <https://foi.se/forskning/informationssakerhet/crate---sveriges-nationella-cyberanlaggning-for-totalforsvaret.html>

⁴ <https://www.docker.com>

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

men då endast som en möjlig reservlösning ifall tekniska problem skulle uppstå. På grund av tekniska problem under 2022 års genomförande behövde ytterligare två uppgifter flyttas ut till molntjänsten i början av tävlingen, vilket beskrivs närmare i avsnitt 2.1.

1.3 Mjukvaruplattform

Vid det första genomförandet av Crate-CTF, då kallat 20/20 CTF, valdes *CTFd* som plattform för tävlingen. Då denna plattform fungerade väl under det genomförandet valdes CTFd även som plattform för genomförandet av Crate-CTF 2021 och 2022.

Plattformens uppgift är att registrera användare och lag, hantera och distribuera uppgifter, hantera och validera deltagarnas lösningsförslag samt tilldela poäng och beräkna poängställning. Mer information om plattformen CTFd återfinns på <https://github.com/CTFd/CTFd>.

Utöver plattformen nyttjades kommunikationstjänsten *Discord* för kontakt mellan deltagare och arrangörer. På grund av kommunikationsstrukturen i Discord är det även möjligt för deltagare att öppet kommunicera med varandra, vilket kan anses som positivt då det möjliggör interaktion mellan individer från olika lag i kommunikation som inte direkt berör tävlingens uppgifter. En majoritet av kommunikationen över Discord relaterade dock till problem eller frågor kring uppgifter. En möjlighet för alla deltagare att kunna ta del av frågor och svar från andra sparar tid för både deltagare och arrangörer då frågor inte behöver ställas flera gånger.

1.4 Uppgifter

För genomförandet 2020 var målet att utveckla uppgifter som efterliknade den typ av uppgifter som vanligen förekommer i andra CTF-tävlingar. Därför gjordes eftersökningar gällande typer av uppgifter som resulterade i ett antal uppgiftskategorier. Dessa kategorier återanvändes även för Crate-CTF 2021 och 2022. Efter feedback från deltagare i 20/20 CTF samt FOI-medarbetare som utvecklade uppgifterna bestämdes att kategorin *forensik* skulle läggas till i Crate-CTF 2021. Kategorin forensik följde med även till Crate-CTF 2022, där den tillsammans med kategorin *Övriga* fick lite mer tyngd än året innan. Fördelningen av antalet uppgifter per kategori såg därför ut enligt följande för 2022 års genomförande:

- Webb: 3 uppgifter
- Kryptografi: 3 uppgifter
- Exploatering: 3 uppgifter
- Reversering: 3 uppgifter
- Övriga: 6 uppgifter
- Forensik: 5 uppgifter

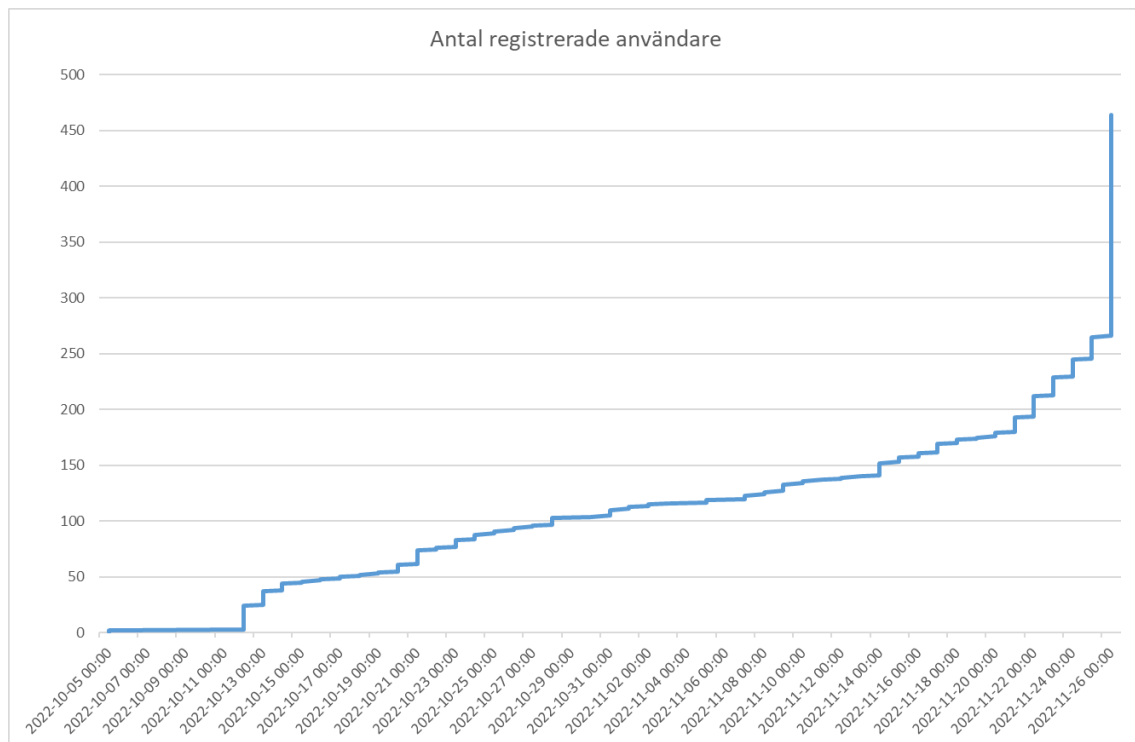
Nytt för genomförandet 2022 var att uppgifter som tagits fram för att vara enklare märktes upp med texten "uppvärmning". Detta för att hjälpa nybörjare eller de med liten CTF-vana att hitta lämpliga uppgifter att börja med.

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

2 Genomförande och resultat

FOI:s externa hemsida uppdaterades 2022-10-06 med information om 2022 års genomförande av Crate-CTF, och en nyhet publicerades på FOI:s intranät 2022-10-12 om tävlingen. Kort tid därefter skrevs inlägg om Crate-CTF 2022 på sociala medier, så som LinkedIn, av personer som sett nyheten. Ingen betald annonsering skedde dock på sociala medier.

I figur 1 nedan visas antal registrerade användare över tid, fram till genomförandet den 26 november 2022. Totalt registrerades 464 användare, vilket var 180 fler än genomförandet 2021 och 14 fler än 2020. Uppgången i antalet registreringar kan bero på att information om tävlingen publicerades tidigare än föregående år, samt att tävlingen börjat bli mer känd eftersom den kördes för tredje året i rad. Precis som vid de tidigare två genomförandena registrerades en majoritet av deltagarna de närmsta dagarna innan tävlingen startade. Vid årets genomförande av Crate-CTF registrerades även fler lag än föregående gång, 147 stycken. Detta är en ökning med 36 lag jämfört med 2021 års genomförande.



Figur 1. Graf över antalet registrerade användare över tid.

2.1 Tekniska problem under genomförandet

I början av tävlingen upptäcktes att deltagarna inte kunde ansluta till nätverkstjänsterna för två uppgifter. Vid närmare undersökning visade det sig att de båda uppgifterna blockerades i en brandvägg. Eftersom administrationsåtkomst inte fanns till denna brandvägg fick de två uppgifterna flyttas ut till reservlösningen, alltså molntjänsten. Det innebär att totalt tre uppgifter, en planerad och två oplanerade, kördes i molntjänsten under tävlingen.

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

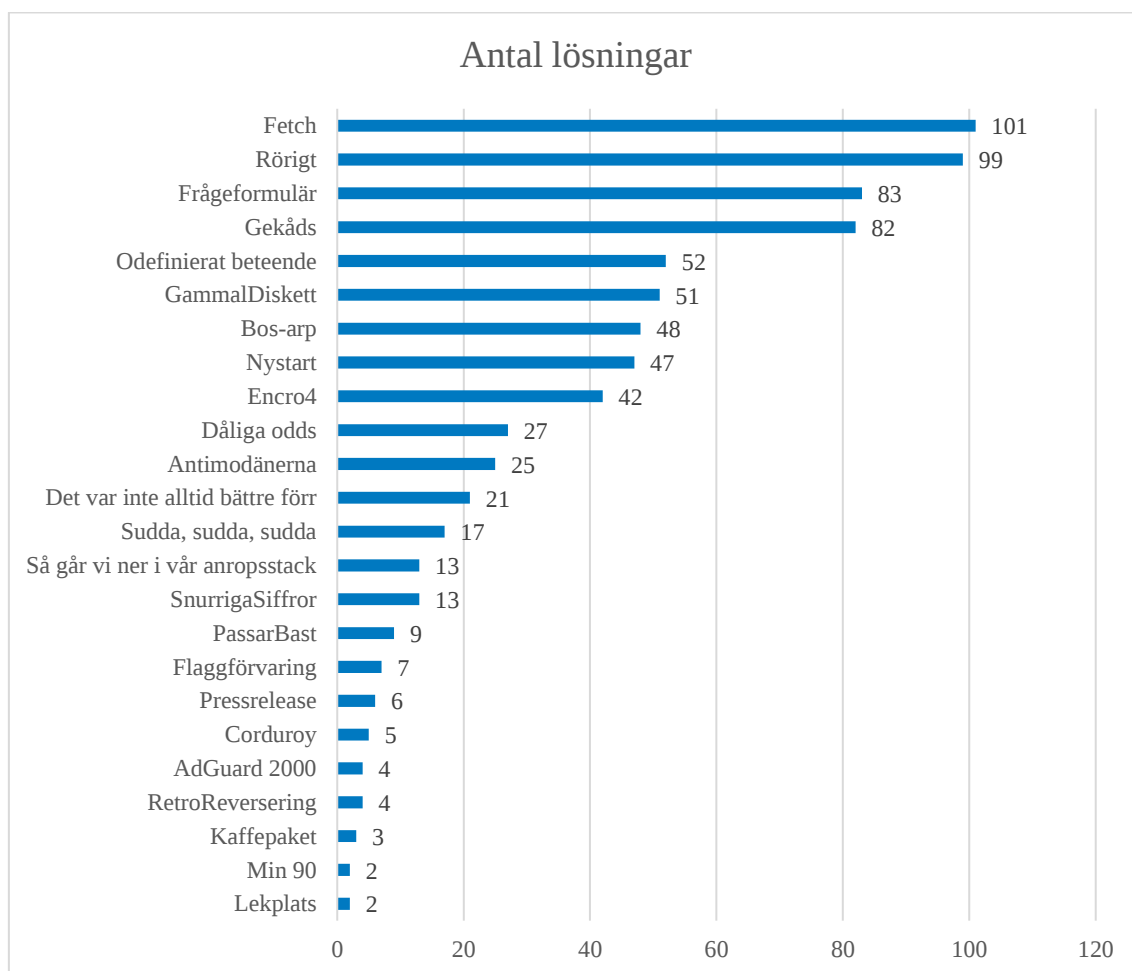
2.2 Tävlingens resultat

Till skillnad från föregående genomföranden av Crate-CTF löste ett lag alla uppgifter under årets genomförande. Detta lag löste den sista uppgiften när det återstod drygt en timme av tävlingen, så även om alla uppgifter löstes var även det bästa laget sysselsatta under nästan hela tävlingen. I tabell 1 listas den slutgiltiga poängen för de 10 bästa lagen i tävlingen. Laget *RoyalRoppers* löste alla uppgifter och fick därmed också högst poäng och förstaplatsen. Notera att poängen är dynamiska och baseras på hur många som löser dem, vilket förklarar den något udda totalsumman.

Tabell 1. De tio bästa lagen och deras poängställning.

Placering	Lag	Poäng
1	RoyalRoppers	9923
2	watevr	8925
3	5ca5dd	7924
4	ChaGU	5955
5	Omegapoint	5427
6	RIP Börje Salming	5038
7	Biljardbordet	4942
8	n00bz	4938
9	LionHack	4550
10	Hjärterhex	4473

I figur 2 nedan visas tävlingens olika uppgifter och hur många korrekta lösningar lagen lämnade in för var och en av dessa. De uppgifter som minst antal lag löste var *Min 90* och *Lekplats*, vilket förmodligen kan tolkas som tävlingens svåraste uppgifter. Uppgifterna *Fetch* och *Rörigt* löstes flest gånger, vilket var förväntat då dessa var tänkta att vara enklare uppgifter i tävlingen. Uppgiften *Frågeformulär* refererar till det frågeformulär som nyttjades för att samla in deltagarnas återkoppling. Återkopplingen presenteras i avsnitt 2.3. Frågeformuläret nyttjades som uppgift med tillhörande poäng i syfte att få så många deltagare som möjligt att lämna återkoppling om tävlingen.

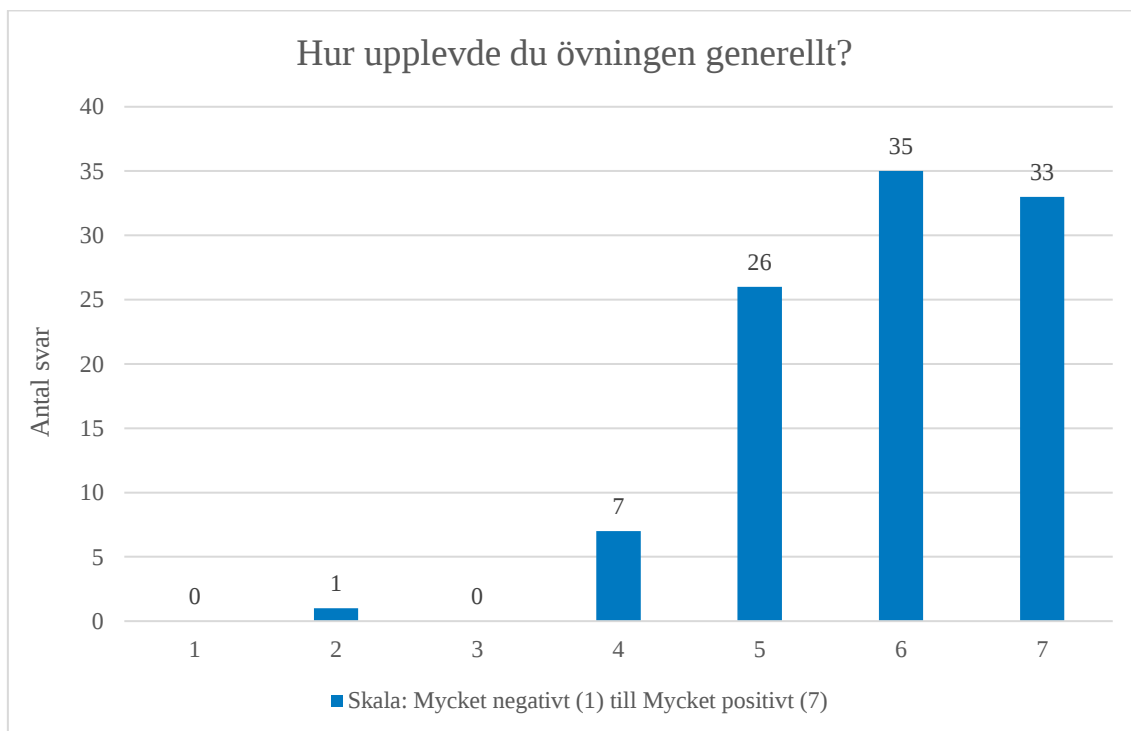
Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

Figur 2. Antalet korrekta lösningar som skickades in per uppgift.

2.3 Deltagarnas återkoppling

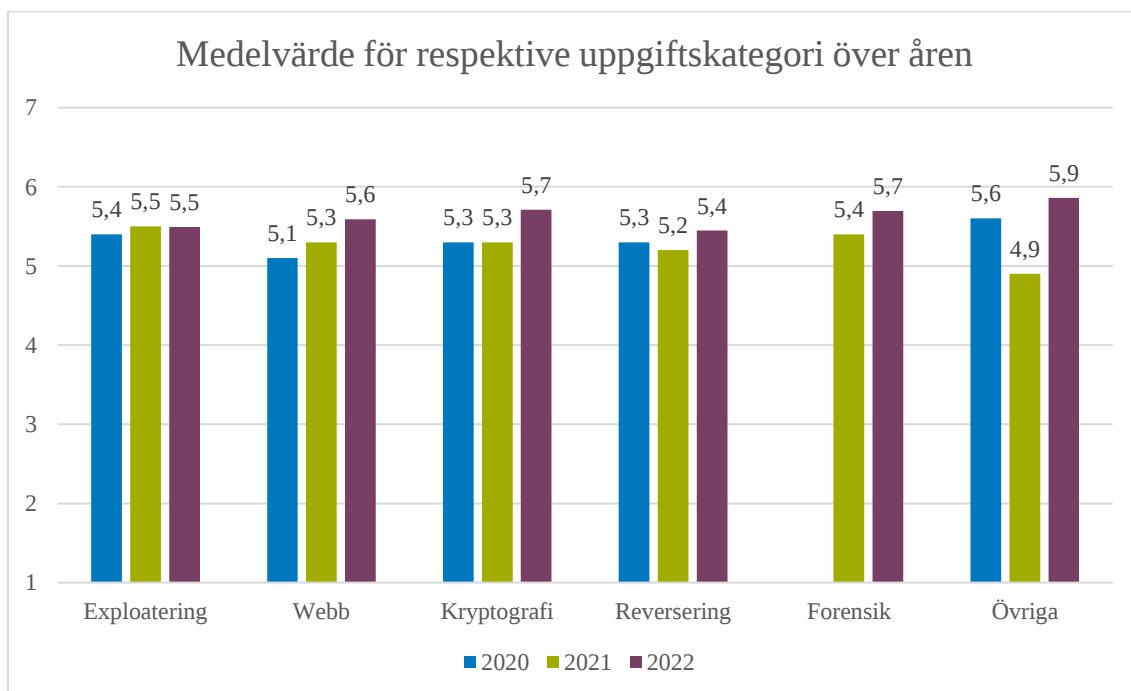
Deltagarnas återkoppling gällande tävlingen var generellt positiv. I följande tabeller visas ett urval av denna återkoppling, vilken samlades in via ett frågeformulär. För hantering och distribution av frågeformuläret nyttjades verktyget *LimeSurvey*.

Notera att alla frågeformulärets frågor inte presenteras i detta avsnitt. Alla deltagare besvarade inte enkäten och inte heller alla som påbörjade enkäten besvarade alla frågor. Detta innebär att det kan finnas relativt stora skillnader i antalet svar för olika frågor. Sammantaget begränsar detta möjligheten att dra några detaljerade slutsatser, men återkopplingen kan fortfarande ge vissa indikationer.

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

Figur 3. Deltagarnas återkoppling om hur de upplevde tävlingen generellt.

Som figur 3 visar var de svarande generellt nöjda med tävlingen. Medelvärdet för de svarandes återkoppling för denna fråga var 5,89 på den sjugradiga skalan som användes. Medelvärdet för samma fråga från genomförandet 2021 var 5,92 och för 2020 var det 5,9. Värdet var därmed marginellt lägre än tidigare år.

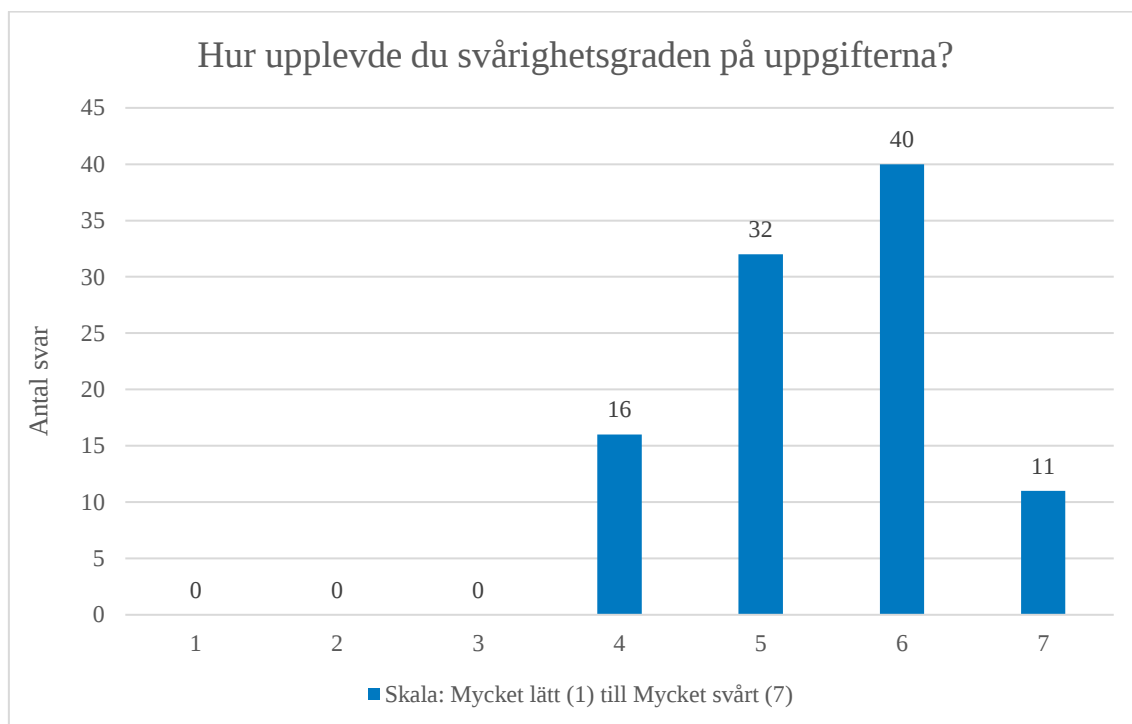


Figur 4. Medelvärden för uppgifter inom varje kategori för år 2020, 2021 och 2022.

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

I figur 4 presenteras ett medelvärde på en sjugradig skala för hur de svarande upplevde uppgifterna inom varje kategori, samt hur detta värde sett ut genom åren. Enligt de svarandes återkoppling upplevdes kategorin *Övriga* innehålla bäst uppgifter i årets genomförande. Detta är en kontrast mot föregående år, där denna kategori upplevdes som minst bra. Det är svårt att dra någon generell slutsats kring detta, annat än att årets uppgifter kan ha försetts med bättre beskrivningar vilket gjort målet med respektive uppgift tydligare. Ingen kategori sticker ut nämnvärt negativt i årets genomförande, vilket kan indikera att blandningen av uppgifter i respektive kategori upplevdes som bra.

Skillnaderna mellan medelvärdena för 2022 och tidigare genomföranden är relativt små, även om kategorierna i årets genomförande genomgående fått lite bättre betyg än tidigare år.



Figur 5. Den upplevda svårighetsgraden för uppgifterna.

I figur 5 visas hur de svarande upplevde svårighetsgraden på uppgifterna. Trots ett fokus på att ta fram lättare uppgifter upplevde majoriteten av de svarande att uppgifterna var svåra – förmodligen svårare än vad tävlingen haft som mål. Detta indikeras även av en del av fritextsvaren i enkäten. En förklaring kan vara att många med liten CTF-vana har deltagit i tävlingen, vilket är positivt sett till tävlingens mål. Det finns dock en risk att de med liten CTF-vana upplever att tävlingen har en annan målgrupp än de själva om uppgifter märkta som enklare fortfarande håller för hög svårighetsgrad.

Titel/Title
Genomförande Crate-CTF 2022Memo nummer/Number
FOI Memo 8073

3 Diskussion

Crate-CTF 2022 var som helhet en lyckad tävling, men det finns potentiella förbättringar att utföra till nästa genomförande. Som syntes i återkopplingen i enkäten upplevs uppgifterna fortfarande som lite för svåra för nybörjare. Att i år märka upp lättare uppgifter var sannolikt en förbättring, men nådde inte hela vägen. Därför kan det vara lämpligt för framtida CTF-projekt att lägga mer tid på att undersöka hur nybörjare ska kunna ta till sig tävlingen. En möjlighet skulle kunna vara att introducera mer interaktiva uppgifter, där deltagaren guidas igenom lösandet av uppgiften. Detta för att hjälpa deltagaren till möjliga tankesätt för att ta sig an en CTF-uppgift. Vissa deltagare kommer dock sannolikt alltid uppleva tävlingen som för svår, varför ett genomtänkt och balanserat tillvägagångssätt behövs där aspekten målgrupp också inkluderas.

Antalet deltagare som anmälde sig till tävlingen ökade markant under de närmsta dagarna innan tävlingens genomförande, vilket även observerats vid de tidigare genomförandena. Marknadsföringen kom igång tidigare detta år jämfört med exempelvis förra året, men detta verkar alltså inte ha haft någon påverkan på detta beteende. Det kan dock noteras att fler deltagare registrerats än båda tidigare år, vilket skulle kunna härröra till tidigare marknadsföring eller att Crate-CTF börjar bli känd som en återkommande händelse.

På det tekniska planet flöt tävlingen på bra, med undantag för nätverkstjänsterna för två uppgifter som av misstag blockerades i en brandvägg. Efter att problemet upptäckts kunde dock nätverkstjänsterna snabbt flyttas ut till reservlösningen och tävlingen fortsätta. Att låta uppgifterna exekvera i molntjänsten fungerade tekniskt bra, och kunde möjliggöras till en låg kostnad eftersom tiden tjänsterna behöva vara tillgängliga motsvarade tävlingens längd. Det vore därför fördelaktigt att även i framtida genomföranden ha en molntjänst tillgänglig som reservlösning.