FOI MEMO

Projekt/Project
NCS3-stöd till MSB:s forskningsprojekt inom ICS 2016-2020

Sidnr/Page no
1 (10)

Projektnummer/Project no
B73001

Kund/Customer
Myndigheten för Samhällsskydd och Beredskap

FoT-område
Inget FoT-område

Författare/Author
Tobias Lundberg

Datum/Date
2020-11-05

Memo nummer/Number
FOI Memo 7344

20/20 CTF

Sändlista/Distribution

Joachim Elevant	MSB
Ebba Leckström	MSB
Christian Sundberg	MSB
Erik Sundström	MSB
Gustav Söderlind	MSB
Jonas Almroth	FOI
Johan Bengtsson	FOI
Tommy Gustafsson	FOI
Jonas Hallberg	FOI
Lars Helgeson	FOI
Patrik Lif	FOI
Tobias Lundberg	FOI
Anders Norén	FOI
Teodor Sommestad	FOI
Mikael Wedlin	FOI
Lars Westerdahl	FOI

Innehåll

1 Inledning

Detta memo beskriver utvecklandet och genomförandet av *20/20 CTF*, en tävling inom IT-säkerhet som genomfördes den 26 september 2020 av FOI. 20/20 CTF finansierades av Myndigheten för Samhällsskydd och Beredskap (MSB) som del av projektet *NCS3-stöd till MSB:s forskningsprojekt inom ICS 2016-2020*[1]. Syftet med tävlingen var att bygga upp kunskap om CTF-formatet för att kunna nyttja det i framtida projekt och att undersöka om CTF:er kan anpassas för att inkludera industriella informations- och styrsystem.

En beskrivning av den tekniska infrastrukturen återfinns i kapitel 2, framtagande av uppgifter beskrivs i kapitel 3, en beskrivning av genomförande och resultat från tävlingen återfinns i kapitel 4, och kapitel 5 beskriver framtida utvecklingsområden.

1.1 Capture the Flag

20/20 CTF körde det så kallade Jeopardy-formatet av en CTF. Det går ut på att deltagarna får tävla om att lösa olika IT-säkerhetsrelaterade uppgifter. Varje uppgift går ut på att man ska hitta en så kallad ”flagga”, vilket är en mening som ligger dold eller skyddad. När man hittar en uppgifts flagga skickar man in den till CTF-plattformen och får poäng. Det lag med flest poäng när tävlingen avslutas vinner.

Utöver Jeopardy-formatet är även attack-and-defense-formatet ganska vanligt. Det går ut på att lagen istället för att lösa separata uppgifter får tillgång till en server de ska försvara, samtidigt som de attackerar servrarna som de andra lagen försvarar.

[1] FOI-2015-10, MSB 2014-4022 / 2018-12180

2 Teknisk infrastruktur

20/20 CTF nyttjade en server som köptes in inom ramen för projektet Förstudie OpenCRATE. Servern var utrustad med 40 CPU-kärnor på 2.2 GHz, 384 GB RAM och en nätverksuppkoppling på 1 Gbps. Detta bedömdes vara tillräckligt för den tänkta omfattningen på tävlingen. Operativsystemet på servern var Ubuntu 20.04. KVM[2] och WebVirtCloud[3] nyttjades för uppsättning av två virtuella maskiner. En virtuell maskin användes för att köra CTF-plattformen och en virtuell maskin användes för att köra de nätverkstjänster som tillhörde ett par av uppgifterna.

2.1 CTF-plattformen

En CTF-plattforms uppgift är bland annat att registrera användare och lag, lägga till och distribuera uppgifter, hantera registrering av svar på uppgifterna samt att beräkna och visa aktuell ställning i tävlingen.

Efter en mindre undersökning valdes CTF-plattformen CTFd[4]. Detta val gjordes bland annat baserat på en översiktsstudie av Kucek och Leitner [1], där CTFd presenteras som en av de mest mogna plattformarna. Utöver det så användes även arrangörernas tidigare erfarenheter från CTF:er, där CTFd tycks vara en av de mest välanvända plattformarna.

2.2 Nätverkstjänster till uppgifter

Under utvecklingsstadiet av uppgifterna var det ännu inte bestämt var och hur nätverkstjänsterna skulle köras, vilket gjorde det önskvärt att använda ett system med hög portabilitet. Det var även önskvärt att kunna köra flera isolerade nätverkstjänster på samma maskin. För att uppfylla dessa krav användes Docker-containers[5] för att sätta upp nätverkstjänsterna. Vid en informell sökning visar det sig att Docker används även i andra CTF:er[6].

2.3 Utvecklade verktyg

Utöver utvecklingen av själva uppgifterna behövdes verktyg för den tekniska infrastrukturen utvecklas för att göra det enkelt att sätta upp fler CTF:er i framtiden.

Ett verktyg som kompilerade uppgifterna och paketerar dem i ett format som går att importera i CTFd togs fram. Målet med detta var att det skulle vara enkelt att peka ut vilka uppgifter som ska användas i en viss CTF, för att på så sätt möjliggöra att en uppgift är enkel att återanvända i flera olika CTF:er.

Utöver detta utvecklades även diverse script för att sätta upp CTFd och installera Docker.

---

[2] https://www.linux-kvm.org/page/Main_Page

[3] https://github.com/retspen/webvirtcloud

[4] https://github.com/CTFd/CTFd

[5] https://www.docker.com/

[6] https://github.com/midnight-sun-ctf/challenges2018

3 Design av uppgifter

Då ett av målen var att arrangera en typisk CTF var det önskvärt att utveckla uppgifter som liknar den typ av uppgifter som finns i andra CTF:er. För att avgöra vilka typer av uppgifter som är vanligt förekommande gjordes en genomgång av samtliga 9467 uppgifter som fanns inlagda i ctftime.org[7] vid undersökningstillfället, där uppgifternas taggar antogs kunna vara en kategori av uppgift. En tabell med de 8 vanligaste taggarna återfinns i Tabell 1.

Tabell 1 - Vanligaste uppgiftstaggarna på ctftime.org

Tagg	Förekomst
web	1641
cryptography	1517
pwn	1449
reverse engineering	1447
forensics	896
miscellaneous	841
steganography	314

Utöver detta användes även arrangörernas tidigare erfarenheter från andra CTF:er för att ta fram kategorier. Resultatet blev att uppgifter skapades i kategorierna webb (eng. web), kryptografi (eng. cryptography), exploatering (eng. pwn), reversering (eng. reverse engineering), och övriga (eng. miscellaneous). En beskrivning av de olika kategorierna följer nedan.

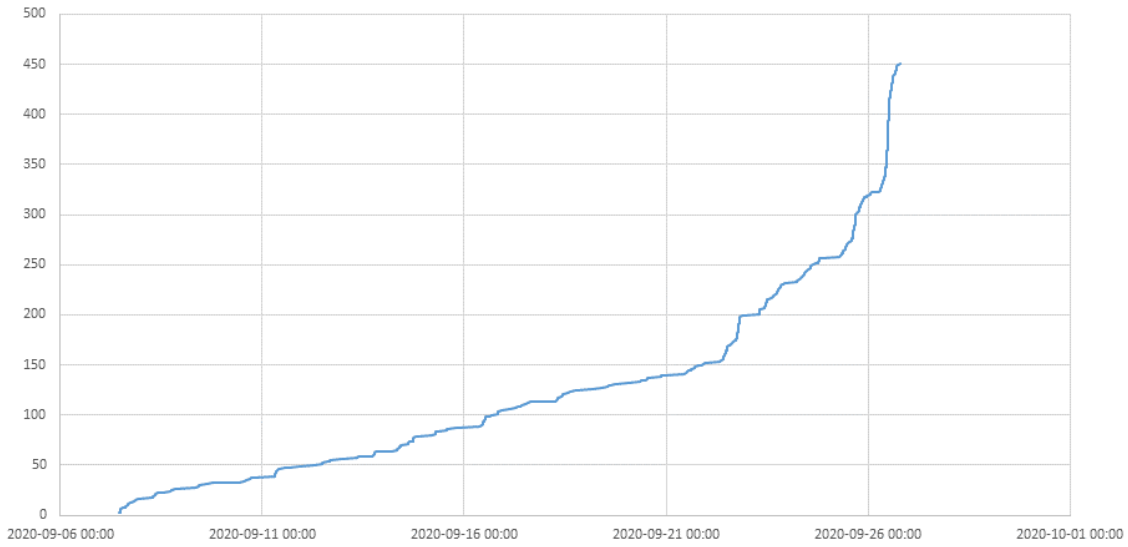
- Webbuppgifter går ut på att attackera eller undersöka en viss webbtjänst.
- Kryptografiuppgifter går ut på att hitta sårbarheter i ett visst kryptosystem för att på så sätt dekryptera en krypterad flagga.
- Exploateringsuppgifter går ut på att hitta och utnyttja en sårbarhet i en applikation. Slutmålet är att ändra applikationens flöde till sin fördel, för att på så sätt få programmet att skriva ut en flagga.
- Reverseringsuppgifter går ut på att förstå vad ett kompilerat program gör när det körs. En vanlig uppgift är att förstå hur ett lösenord kontrolleras vid en inloggning, för att sedan ta fram ett lösenord som klarar av kontrollen.
- Övriga uppgifter innehöll uppgifter som inte passade in i någon annan kategori.

Kategorierna webb, kryptografi, exploatering, och reversering hade 4 uppgifter vardera. Kategorin övriga hade 5 uppgifter.

[7] https://ctftime.org/

4 Genomförande och resultat

Den 7 september började tävlingen marknadsföras genom FOI:s hemsida, LinkedIn och Twitter. När tävlingen började hade 450 deltagare registrerat sig, varav 170 stycken mindre än ett dygn innan tävlingen startade. Deltagarna var indelade i 174 lag. Antalet registrerade användare över tid illustreras i Figur 1.



Figur 1 - Antal registrerade deltagare över tid

Under genomförandet av tävlingen satt två arrangörer och driftövervakade systemen och svarade på supportfrågor från deltagarna. Det hela var en ganska lugn tillställning, och någon större arbetsinsats behövde inte genomföras under tävlingen. Ett undantag var ett fåtal tekniska problem som beskrivs närmare i avsnitt 4.1.

4.1 Tekniska problem under genomförandet

En av kryptografi-uppgifterna körde en nätverkstjänst som inte avslutades rätt när deltagare kopplade bort sig och drog ganska mycket resurser som aldrig frigjordes. Detta berodde på en bugg som hittades först under slutet av tävlingen. För att hantera detta under tävlingens gång fick en arrangör starta om tjänsten ett par gånger när tjänsten började dra för mycket processorkraft. Då tjänsten startade om på mindre än en sekund och anslutningar från deltagarna var mycket sporadiska och kortlivade är det inte troligt att någon deltagare märkte av några problem.

Webbsidan som användes för uppgifterna i webb-kategorin kunde periodvis upplevas långsamt, vilket uppmärksammades av några av deltagarna. Vad dessa problem berodde på identifierades inte, och då störningen var så pass minimal behövde ingen åtgärd göras under tävlingen.

CTF-plattformen, CTFd, hade ett par stabilitetsproblem och behövde startas om fem gånger. Vad dessa stabilitetsproblem berodde på kunde inte identifieras. Totalt gjordes fem omstarter, där varje omstart gav en nertid på ungefär två minuter där deltagarna inte kunde använda plattformen. Utöver detta fick några deltagare felmeddelanden och upplevde sidan som långsam under vissa perioder.

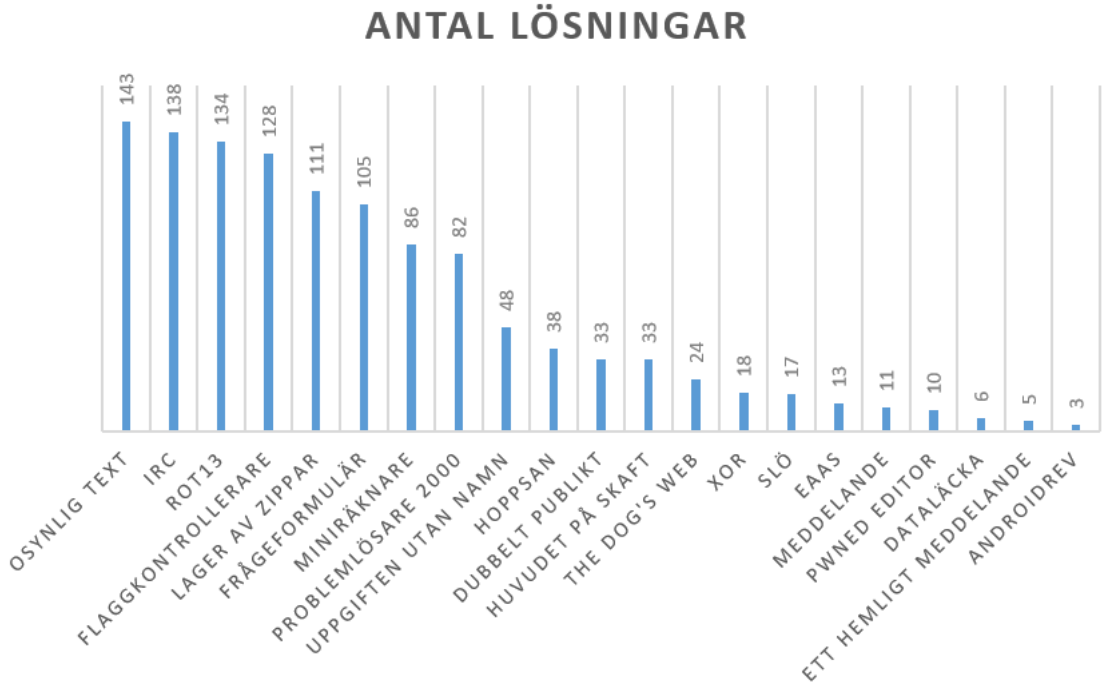
4.2 Resultat från tävlingen

Placering och resultat för de tio bästa lagen är sammanställt i Tabell 2.

Tabell 2 - Tabell över de tio bästa lagen

Placering	Lag	Poäng
1	watevr	9872
2	LionHack	9292
3	KTHCTF0x1	9022
4	MV9rwGOf08	8622
5	5ca5dd	8227
6	LarsH	8222
7	Chagu	8196
8	ZetaTwo	7646
9	OmegaPoint	7563
10	IndianTuesday	7479

Alla uppgifter blev lösta av något lag, men inget lag lyckades lösa alla uppgifter. Detta kan tolkas som att uppgifterna var tillräckligt varierande för att olika kunskaper skulle krävas, vilket är ett tecken på en bra design av uppgifterna. Vidare var fördelningen av antalet lösningar på de olika uppgifterna tillfredställande, då de enklaste uppgifterna löstes av i princip samtliga lag, medan de svåraste bara löstes av ett fåtal. Antalet lösningar på de olika uppgifterna illustreras i Figur 2.



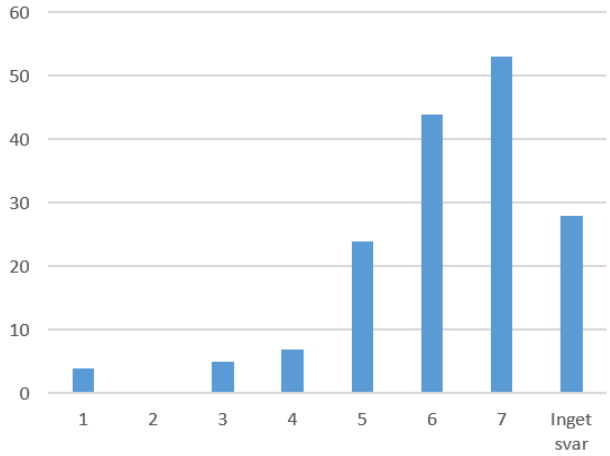
Figur 2 - Antal lösningar per uppgift

Vidare var det inte något lag som var överlägset hela vägen, utan topplaceringarna varierade under hela tävlingens gång.

4.3 Respons från deltagarna

Återkopplingen från tävlingsdeltagarna kom främst genom en enkät som deltagarna ombads svara på. Totalt svarade 291 olika deltagare. Nedan redovisas svaren på några representativa frågor. För att hålla memot kortfattat så redovisas inte alla frågor här, utan frågor som handlar om deltagarnas utbildning och arbetslivserfarenhet utelämnas. Även frågor som berör deltagarnas upplevda nytta med CTF:er utelämnas.

Svaren på frågan ”Hur upplevde du övningen generellt?” redovisas i Figur 3. Deltagarna uppmanades svara på skala 1 (Mycket negativt) till 7 (Mycket positivt). Genomsnittet bland svaren var 5.9, vilket kan anses som ett högt betyg för tävlingen.



Figur 3 - Enkätsvar om upplevelse av 20/20 CTF

Enkäten frågade även om upplevelse av uppgifterna inom olika kategorier. Deltagarna uppmanades svara på en skala 1 (Mycket negativt) till 7 (Mycket positivt). Samtliga kategorier hade ett genomsnittsbetyg på över fem, och ingen kategori stack ut som mycket bättre eller sämre än någon annan. Genomsnittsbetyget för varje kategori presenteras i Tabell 3.

Tabell 3 - Genomsnittsbetyg för de olika kategorierna

Kategori	**Snittbetyg**
Webb	5,15
Kryptografi	5,31
Reversering	5,34
Exploatering	5,40
Övriga	5,56

Enkäten bad deltagarna att fylla i ett fritextfält med övriga kommentarer. Totalt svarade 60 personer. En informell bedömning av dessa gjorde att 31 svar kunde anses vara positiva, 17 vara negativa och 12 vara varken positiva eller negativa. Bland de negativa svaren återfanns bland annat kommentarer om att uppgifterna var för lätta, att uppgifterna var för svåra, att CTF:en höll på för kort tid, att CTF-plattformen var för långsam och att poängen för uppgifterna inte reflekterade svårighetsgraden. Bland de positiva svaren fanns det kommentarer om att det var lärorikt, kul att delta, att uppgifterna hade lagom svårighetsgrad och att det gav mersmak på ett deltagande i fler CTF:er.

5 Framtida arbete

Responsen på tävlingen var mycket positiv från både deltagarnas och uppdragsgivarens sida. Detta gör att förutsättningarna för att kunna arrangera fler CTF:er borde ses som god. Nedan kommer några förslag på utvecklingsområden och forskningsfrågor som kan besvaras inom ramen för framtida CTF-projekt.

5.1 Forskningsfrågor

Följande forskningsfrågor kan vara intressanta att studera i samband med ett framtida CTF-arrangemang.

- Hur väl fungerar tävlingsresultat från en CTF som rekryteringsunderlag?
- Vad är det som gör att en deltagare gör bra ifrån sig i en CTF?
- Hur kan CTF:er användas som delmoment i en utbildning?
- Hur kan CTF:er användas för utvärdering och analys av system?

Några av frågorna har vi delvis fått svar på i samband med genomförandet av 20/20 CTF. Baserat på responsen från deltagarna kan vi konstatera att ett visst intresse för FOI som arbetsplats har tillkommit och att många av de deltagare som lyckades väl i tävlingen har varit aktiva inom CTF:er tidigare. Mer noggranna analyser behövs dock för att kunna besvara frågorna med säkerhet.

5.2 Utveckling

Följande punkter beskriver vissa utvecklingsområden för uppgifterna och den tekniska infrastrukturen:

- Tilldelning av portar för en nätverkstjänst behövde göras manuellt. Detta borde gå att automatisera ytterligare.
- Verktygen för att sätta upp en CTF och välja uppgifter till denne borde gå att effektivisera. En arrangör borde exempelvis kunna välja ut intressanta uppgifter för att sedan automatiskt sätta upp de maskiner och tjänster som krävs för att genomföra CTF:en.
- Påpekade brister i plattformen CTF:d skulle eventuellt behöva identifieras och åtgärdas, alternativt skulle en egen CTF-plattform kunna utvecklas.

6 Referenser

[1] M. L. Stela Kucek, ”An Empirical Survey of Functions and Configurations of Open-Source,” *Journal of Network and Computer Applications,* 2019.