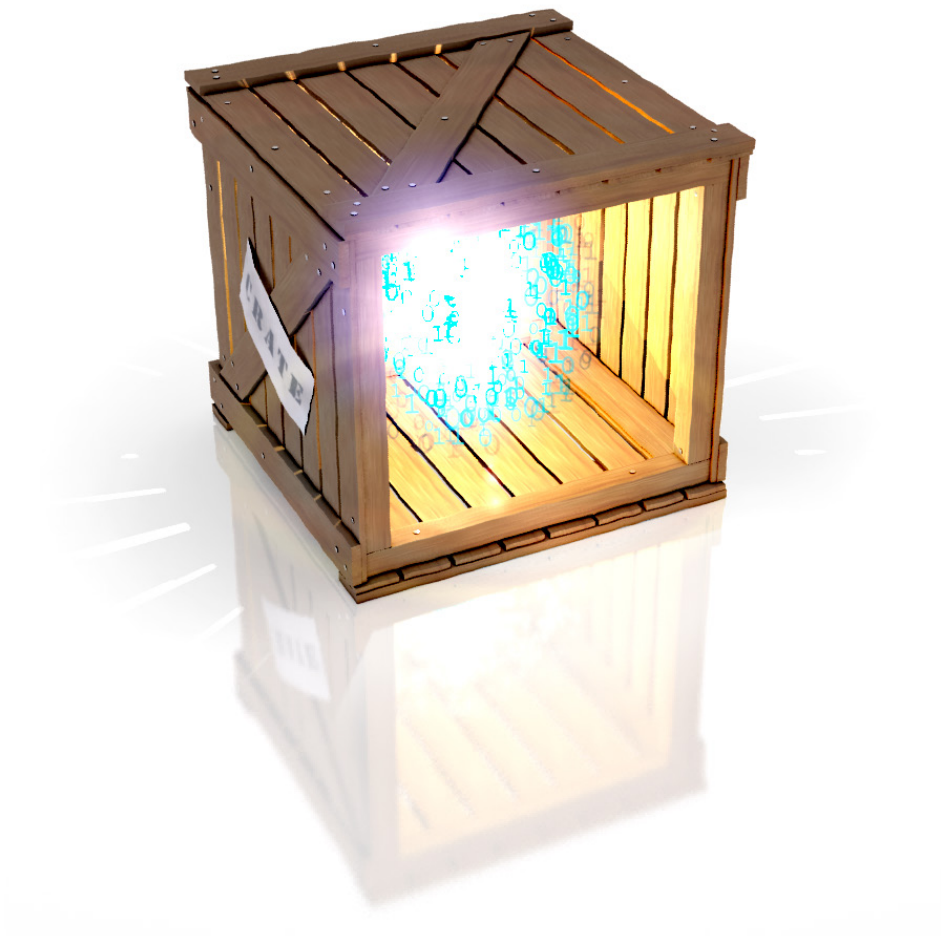
Övningsrapport: SAFE Cyber 2019

Planering, utveckling, genomförande och lärdomar av en storskalig CDX-övning

CHRISTIAN VALASSI, MIKAEL WEDLIN



FOI-R--4885--SE
ISSN 1650-1942 December 2019

Christian Valassi, Mikael Wedlin

Övningsrapport: SAFE Cyber 2019

Planering, utveckling, genomförande och lärdomar av en storskalig CDX-övning.

Titel	Övningsrapport: SAFE Cyber 2019 – Planering, utveckling, genomförande och lärdomar av en storskalig CDX-övning.
Title	Exercise report: SAFE Cyber 2019 – Planning, development, implementation and, teachings from a large-scale CDX.
Rapportnr/Report no	FOI-R--4885--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	66
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E72787
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Denna rapport beskriver hur cyberförsvarsövningar planeras och genomföra ur ett allmänt perspektiv och från FOI:s perspektiv. Vidare beskriver rapporten planering, utveckling, genomförande samt utvärdering och erfarenheter från övningen SAFE Cyber 2019.

SAFE Cyber är en årlig försvarsmaktensövning som 2019 genomfördes med stöd av FOI. Övningen riktade sig till myndigheter och företag med anknytning till Försvarsmakten. SAFE Cyber 2019 syftade till att öva hantering av incidenter i händelse av dator- och nätverksoperationer riktade mot Sverige. Övningen innefattade två olika delar: en teknisk cyberförsvarsövning (CDX) och en diskussionsövning (TTX). Totalt övades 60 individer från 21 olika organisationer med anknytning till Försvarsmakten.

Rapporten visar att det är komplext att planera och genomföra övningar innehållande två olika interagerande övningstyper. SAFE Cyber 2019 visar dock att det är möjligt att kombinera en teknisk simuleringsövning med en diskussionsbaserad övning och att det går att göra på ett sätt som skapar värde för deltagare såväl som beställare och övningsledning. Samtidigt visar resultaten att det finns potential för förbättringar i interaktionen mellan övningstyperna i syfte att skapa ett större värde för alla inblandade.

Baserat på de lärdomar som identifieras i rapporten bedöms de viktigaste aspekterna för att kunna planera och genomföra framgångsrika övningar av kombinerad CDX- och TTX-typ i framtiden vara planering av mål och syfte för övningen, en erfaren planeringsgrupp, samt flexibilitet att hantera problem när de uppkommer.

Nyckelord: Cyberförsvarsövning, Cybersäkerhetsövning, Diskussionsövning, CDX, TTX,

Summary

This report describes how cyber defence exercises are planned and conducted both from a general perspective and from the perspective of FOI. Furthermore, the report describes planning, development, execution, evaluation and experience from the SAFE Cyber 2019 exercise.

SAFE Cyber 2019 was an exercise conducted by the Swedish Armed Forces in conjunction with FOI. The exercise was aimed at Swedish authorities with responsibility for cyber security, as well as authorities and companies with a connection to the Swedish Armed Forces. The purpose of the exercise was to give incident management practice to the participants in the event of computer and network operations against Sweden. The exercise was comprised of two different parts: a technical cyber defence exercise (CDX) and a discussion-based exercise (TTX). In total, 60 individuals from 21 different organisations related to the Swedish Armed Forces participated in the exercise.

The report shows that planning and conducting exercises comprised of two different interacting exercise types is a complex process. However, SAFE Cyber 2019 does show that it is possible to combine a technical simulation exercise with a discussion-based exercise in a way that creates value for participants, as well as customers and the exercise management team. At the same time, the results show that there is potential for improvement regarding the interaction between the exercise types in order to create even greater value for everyone involved in future exercises.

Based on the knowledge gained in this report the most important aspects for planning and conducting successful joint CDX and TTX exercises in the future are planning the aims and goals of the exercise, an experienced planning team and flexibility to handle issues as they arise.

Keywords: Cyber defence exercise, Cyber security exercise, Discussion-based exercise, CDX, TTX,

Innehållsförteckning

1 Inledning

Övning och träning syftar i regel till att försörja och vidareutveckla den förmåga (kompetens och rutiner) som krävs för att hantera incidenter och situationer som kan inträffa i verkligheten. Det finns ett stort värde i att öva på incidenter då det inte finns några fundamentala skillnader mellan en simulerad övning och en verklig händelse (Paul och Roth 2016). Detta innebär att den förmåga som erhålls genom övningar får en verklig effekt i organisationers sätt att hantera incidenter. Utöver detta bidrar övningar bland annat till möjligheten att validera policyer, rutiner, hanteringsplaner och verktyg. Övningar ger även möjlighet att identifiera brister i organisationers sätt att hantera händelser, vilket utöver ovanstående exempel även bland annat inkluderar resursplanering och kommunikation (Dewar 2018).

I och med samhällets ökande IT-beroende blir det allt viktigare att upprätthålla förmåga gällande hantering av IT-relaterade incidenter. Ett sätt att öva och träna sådan förmåga är genom cybersäkerhetsövningar, eller cyberförsvarsövningar (CDX[1]), vars förekomst ökat exponentiellt de senaste tjugo åren (Dewar 2018).

CDX-övningar kan planeras och genomföras på flera olika sätt, med en varierande grad av komplexitet och storlek (Dewar 2018). Dessa övningar genomförs ofta som tekniska simuleringsövningar men kan också utformas som diskussionsbaserade övningar (TTX[2]) vars beroende till teknisk miljö i jämförelse är väldigt liten eller helt saknas.

Våra erfarenheter är att tekniska övningar ofta är komplexa att genomföra då de innefattar många olika sammanlänkade komponenter och aspekter som påverkar varandra. Detta inkluderar människor, teknisk infrastruktur, fysiska enheter (hårdvara), mjukvara, lokaler, logistik, säkerhet med mera. Utöver detta är det även viktigt att övningen är så verklighetstrogen som möjligt, vilket i regel ökar komplexiteten i framtagandet av övningen. Detta bekräftas av Dewar (2018). Även storlek på övningen, både vad gäller antalet deltagare och omfattning på innehållet, kan addera komplexitet. Detta tillsammans med fler och större sammanlänkade aspekter ökar även kraven på resurser och sannolikheten för att oförutsedda händelser och problem inträffar (Dewar 2018; Enisa 2015).

[1] Cyber defence exercise

[2] Tabletop exercise

Sammantaget innebär detta att det ställs stora krav på övningars planering och utveckling.

Denna rapport beskriver ur ett allmänt perspektiv hur cyberförsvarsövningar kan planeras och genomföras. Rapporten bidrar även med ett perspektiv på hur Totalförsvarets forskningsinstitut (FOI) planerar och genomför cyberförsvarsövningar. Vidare beskriver rapporten planering, utveckling, genomförande samt utvärdering och erfarenheter från övningen SAFE Cyber 2019.

Den årliga försvarsmaktsövningen SAFE Cyber genomfördes år 2019 med stöd av FOI. Övningen riktade sig till myndigheter och företag med anknytning till Försvarsmakten. Övningen syftade till att öva hantering av incidenter i händelse av dator- och nätverksoperationer riktade mot Sverige. Den innefattade två olika delar: en teknisk cyberförsvarsövning (CDX) och en diskussionsövning (TTX). SAFE Cyber 2019 genomfördes under september månad år 2019, totalt övades 60 individer från 21 olika organisationer.

1.1 Mål och syfte

FOI har på uppdrag av Försvarsmakten att stött planering och genomförande av övningen SAFE Cyber 2019. Som en del i detta uppdrag inkluderades även framtagning av denna rapport.

Det finns ett stort värde i att dokumentera olika övningars utvecklingsprocess och innehåll i syfte att ta vara på erfarenheter inför framtida övningar. Rapporten har därför som mål att:

- Beskriva hur cyberförsvarsövningar kan planeras och genomföras ur ett allmänt perspektiv.
- Beskriva hur SAFE Cyber 2019 planerades, samt resultat och erfarenheter från övningen.
- Beskriva hur FOI planerar och genomför cyberförsvarsövningar, med fokus på tekniskt innehåll.

Syftet med rapporten är att beskriva SAFE Cyber 2019:s olika delmoment, samt resultat och erfarenheter därifrån. FOI har som organisation en stor och mångårig erfarenhet av att planera och genomföra storskaliga övningar. Rapporten beskriver således även på ett generellt plan hur FOI planerar och genomför tekniska övningar, samt redogör för det tekniska innehåll som förekommer i FOI:s övningsverksamhet relaterat till cyberförsvarsövningar.

1.2 Avgränsningar

Denna rapport beskriver endast en delmängd av alla strategier, metoder och begrepp som relaterar till planering och genomförande av cyberförsvarsövningar. Rapporten avgränsar sig till att övergripande beskriva alternativ för övningstyper och metoder relaterat till cyberförsvarsövningar av diskussionsbaserad och simulerad karaktär. Fokus ligger på aspekter och begrepp som kan anses vara gemensamma för planering av cyberförsvarsövningar.

Vidare beskriver rapporten endast på ett övergripande plan hur övningen SAFE Cyber 2019 genomfördes. Därför redogörs inte för några specifika händelser under övningen. Istället beskrivs utmaningar och problem som uppstod under övningens genomförande i form av återkoppling från deltagare, övningsledning och planeringsgrupp.

FOI har en bred övningsverksamhet vilket innefattar fler områden än IT- och cyberförsvar. Denna rapport beskriver dock endast den övnings-verksamhet vid FOI som relaterar till just IT- och cyberförsvar. Beskrivningarna av hur övningar planeras och genomförs av FOI är endast översiktliga, eftersom detta i hög grad är individbaserat.

Parallellt med denna rapport skrevs en artikel av FOI som fokuserar på att utvärdera användandet av den incidenthanteringsmall som användes i övningen samt resultatet av denna användning. Mallen och dess innehåll beskrivs översiktligt i denna rapport, den intresserade läsaren hänvisas istället till den kommande forskningsartikeln.

1.3 Metod

Rapporten baseras på flera olika typer av informationsinsamling. Informationsinsamling för allmänna koncept relaterade till övnings-verksamhet genomfördes genom en litteraturstudie. I den studerades material från tidigare övningar, relevanta organisationer inom cybersäkerhet samt annan litteratur relaterat till cyberförsvarsövningar.

Information relaterat till övningen SAFE Cyber 2019 grundades i observationer från övningens planering, utveckling och genomförande. Vidare gjordes ostrukturerade intervjuer samt hölls diskussioner med ett urval anställda på FOI som leder eller på annat sätt deltar i FOI:s tekniska övningsverksamhet. Fokus låg på att intervjua individer som specifikt leder eller deltar i övningsverksamhet relaterat till cyberförsvar.

Den vetenskapliga artikeln som skrevs använde en webbaserad enkät i datainsamlingssyfte. Delar av enkäten med relevans för resultatet av

denna studie inkluderas i denna rapport. Resultatet presenteras i avsnitt 5.1, enkätfrågorna återfinns i sin helhet i Bilaga B: Enkätfrågor.

Slutligen nyttjades ett *debriefing-möte* med FOI-anställda som deltog under övningen samt diskussioner med deltagare i planeringsgruppen. Detta i syfte att samla in återkopplingsrelaterad data till rapportens resultatdel. Resultatet samt vidare beskrivning av dessa insamlingar presenteras i avsnitten 5.2 respektive 5.3.

2. Bakgrund

Det här kapitlet ger en översikt av hur övningsverksamheten vid FOI inom IT-säkerhetsområdet har utvecklats genom åren. Erfarenheterna från SAFE Cyber 2019 går att tillägna sig även utan detta kapitel. Syftet med kapitlet är att ge en bakgrund till den nuvarande situationsbilden gällande CRATE[3] och beskriva vägen dit.

För att i grunden förstå och tekniskt kunna beskriva funktionen hos skadlig kod med omgivande miljö behövs en djup specialistkunskap om datorhårdvara och operativsystem. FOI byggde därför upp ett IT-försvarslabb som invigdes år 2000. Labbet nyttjades i ett inledande projekt, IT-vapen i laborativ miljö, där det som en del av projektet utvecklades en prototyp till modulärt skadlig kod som kallades *Triops*. Första gången ett *laborationsnätverk* byggdes som liknade de som används i övningar idag var till en demonstration som gjordes för en avrapporterande resultatkonferens i juni år 2001. Nätverket bestod då av tio enklare kontorsdatorer som emulerade ett nätverk med 256 Linuxdatorer i varje kontorsdator. På denna resultatkonferens visades hur en datormask själv traverserade detta nätverk. Ett annat nätverk som under dessa år byggdes upp med hjälp av dessa tio kontorsdatorer var en implementation av ett militärt ledningssystem, IS MARK.

År 2004, alldeles efter en ICRC[4]-konferens i Stockholm, byggdes ytterligare ett nätverk med målet att testa och visa hur ett digitalt Röda-Korset-märke skulle kunna implementeras. Vid det här laget hade VMWare-produkter för virtualisering börjat användas som bas för att bygga nätverken.

Idaho National Laboratory (INL) drev under ett antal år ett program för att studera säkerhet, eller snarast avsaknaden av säkerhet, i styrsystem och hade även börjat ge kurser till styrsystemsoperatörer gällande säkerhet. Myndigheten för samhällsskydd och beredskap (MSB) köpte ett kurstillfälle av INL i november 2008. Ett 20-tal tekniker från olika myndigheter i Sverige deltog i kursen som avslutades med en dags övning. I övningen delades deltagarna in i ett rött lag som stod för angreppen och ett blått lag som skulle försvara en kemisk fabrik. Denna

[3] Se kapitel 4

[4] International Committee of the Red Cross

övning har varit en av de större inspirationer som FOI haft i skapandet av egna övningar av denna typ.

År 2008 var första gången FOI byggde upp större nätverk i NSCs[5] avlagda superdator *Monolit* för att hålla en extern övning. Nedanstående tabell 1är ett utdrag av några av de större övningar FOI har genomfört.

Tabell 1. Tekniska övningar genomförda av FOI

År	Namn	Deltagare	Uppdragsgivare
2008	CADS	Studenter från Sverige och Estland	UD
2010	BCS	Sex lag, från SE, EE, NATO, LT, och LV.	MSB
2011	SMIA	FM CERT och FOI	FM
2012	SMIA	FM CERT och FOI	FM
2013	SAMFI	SAMFI (Svenska myndigheter)	MSB (FM)
2014	NCC	Nordiska CERT:ar	MSB (FM)
2016	-	FM	FM
2017	NTÖ	Samverkansgruppen för informationssäkerhet	MSB
2017	iPilot	Svenska kärnkraftoperatörers IT-administratörer iPilot	Polisen/SSM
2018	-	FM	FM
2019	SAFE Cyber 2019	Försvarsmaktens partners	FM

I de efterföljande avsnitten beskrivs några utvalda övningar, som kommit att bli milstolpar i utvecklingen mot den nuvarande övningsverksamheten.

[5] Nationellt Superdator Centrum, Linköpings Universitet.

2.1 2008 Cyber Adaptive Defense Strategies (CADS)

Efter turbulensen[6] runt flyttandet av en Staty i Tallinn kom Estland och Sveriges respektive försvarsministrar överens om att det borde skapas någon form av samarbete. På den estniska sidan gick uppdraget till *Sivak*, det som senare skulle bli CCDCOE[7], och på den svenska sidan gick det till CATS[8] på Försvarshögskolan (FHS). Ett möte sammankallades där det bestämdes att en simuleringsövning skulle genomföras istället för en diskussionsbaserad övning. NSC tillfrågades om deras superdator kunde användas i övningen. Det visade sig vara olämpligt, dock hade de vid tillfället precis uppgraderat sin superdator och den gamla skulle avvecklas. FOI erbjöds att ta över denna mot att den hämtades i deras datorhall. De 180 servrarna var relativt gamla, men var perfekta för FOI:s behov.

Själva övningen genomfördes i början av december 2008 som en distribuerad övning med två lag av studenter vid Linköpings universitet och två lag från Tallinns universitet. Deltagarna fick en månad på sig att bygga ett litet nätverk som de sedan skulle försvara mot DDoS-attacker. De övade fanns på respektive universitet och övningsledningen var spridd till FOI, Linköping, FHS, Stockholm samt Sivak, Tallinn.

2.2 2010 Baltic Cyber Shield (BCS)

Övningen 2008 var så pass lyckad att MSB fick inskrivet i sitt regleringsbrev att dylika övningar skulle genomföras. Sverige hade lett övningen 2008, så Sivak fick leda övningen inför 2010. Vid det här laget hade Sivak blivit ett NATO-center och det var här mycket av den terminologi uppstod som FOI fortfarande använder, exempelvis i form av färger på lagen och benämningar på planeringsmötena. Dessa är ursprungligen plockade från NATO:s övningsmetodologi. Begreppet CDX började också användas här inspirerade av den *capture the flag*-övning som konferensen DEFCON arrangerat under flera år. Det var också till denna övning FOI utvecklade de VPN-boxar som använts sedan dess.

[6] https://www.theguardian.com/world/2007/may/17/topstories3.russia

[7] NATO Cooperative Cyber Defence Centre of Excellence

[8] Centrum för asymmetriska hot- och terrorismstudier

Övningen genomfördes från svensk sida som en del av MSB:s SCADA-program vilket innebar en hel del fokus på kritisk infrastruktur. Rent praktiskt användes två ångmaskiner som genererade ström och 16 mycket enkla styrsystem vars enda funktion var att det röda laget kunde tända ett isbloss när fick tillgång till nätverket.

Det var under 2010 års övning som FOI för första gången använde verktyget FREX i en IT-säkerhetsövning för att samla in data att forska på. Den metod FREX använder går i stort sett ut på ett tidssynkroniserat sätt samla in så mycket data det går och sedan i efterhand bestämma vilka data som behövs. I denna övning genererades ett dataset på 3 terabyte (TB) som sedan resulterade i ett 10-tal olika publiceringar baserat på övningen.

MSB bestämde efter övningen med esterna att Sverige i fortsättningen skulle fokusera på det nordiska samarbetet. Esterna höll å sin sida kvar vid samma linje som tidigare, vilket ledde till utvecklingen av övningsserien *Locked Shields*.

2.3 2011 och 2012 SMIA

SMIA 2011 och 2012 var två experiment som var mer anpassade för att stödja ett forskningsprojekt än att vara pedagogiska för övnings-deltagarna. Deltagarnas uppgift var att anfalla ett nätverk som skyddades av ett intrångsdetekteringssystem och en systemadministratör. Forskningsfrågan som skulle besvaras var om detekteringen blev bättre med systemadministratör, än utan(Sommestad och Lundholm 2012).

I de gamla donerade noderna användes *VMWare server* som virtualiseringsplattform trots att denna hade slutat få support från VMWare. Det huvudsakliga skälet till detta var att VMWare var den enda produkten som kunde virtualisera utan virtualiseringsstöd i processorn, vilket de donerade servrarna inte hade. VMWares övriga produkter passade dock inte in i hur FOI byggde noder. Under hösten 2012 införskaffades nya noder, i samband med detta byttes även virtualiseringsmiljön till *VirtualBox*, vilket är den miljö som fortfarande används av FOI idag.

2.4 2013 SAMFI, 2014 NCC, 2017 NTÖ, 2017 iPilot

Övningarna SAMFI, NCC, NTÖ och iPilot genomfördes med svenska eller nordiska deltagare och med MSB som huvudman, undantaget iPilot som beställdes av Strålsäkerhetsmyndigheten. Formatet för övningar vid

FOI hade under perioden fram till 2013 hunnit stabilisera sig och övningarna mellan år 2013-2017 genomfördes med ungefär samma metod som år 2010.

3. Planering

Strukturen i detta kapitel är att varje underrubrik inleds med att beskriva en allmän aspekt av övningsplanering vilket sedan följs av ett avsnitt om hur aspekten hanterades i övningen SAFE Cyber 2019.

Planeringsfasen, som vid behov även inkluderar en utvecklingsfas, är den del av en övning som tar längst tid att genomföra. Det är väsentligt för övningens kvalitet att planering påbörjas i god tid innan genomförandet (Dewar 2018). Beroende på övningens storlek och omfattning kan detta innebära att planeringsfasen påbörjas så tidigt som flera år innan genomförandet (Enisa 2015). Viktigt är även att planeringsarbetet ständigt fortgår för att undvika att en stor del av förberedelsearbetet måste utföras de sista veckorna innan övningen ska genomföras (Wilhelmson och Svensson 2013).

3.1 Planeringsmetoder

Det har utvecklats många olika metoder för att planera övningar. Det finns tydliga skillnader mellan dessa metoder, dock finns även ett antal aspekter som kan anses vara gemensamma. Dessa aspekter kan kategoriseras på olika sätt och utföras i olika ordning beroende på vilken metod som används, dock inkluderas generellt följande aspekter (Dewar 2018; Kick 2014; Enisa 2009; NIST 2006; MSB 2012; DHS 2013):

- Identifiera mål och syfte för övningen.
- Identifiera potentiella deltagartyper för övningen.
- Identifiera lämplig övningstyp och övningsmetod för att uppfylla mål och syfte.
- Utveckla ett lämpligt scenario för att uppfylla mål och syfte som även kompletterar vald övningstyp och övningsmetod.
- Utveckla lämpligt tekniskt och diskussionsrelaterat material som kompletterar utvecklat scenario.

Det tillkommer, utöver ovannämnda punkter, ett antal aspekter som beroende på vald metod antingen ses som en separat aspekt eller inkluderas i en av de ovanstående aspekterna. Bland annat tillkommer:

- Fastställa budget för hela övningen.
- Identifiera tillgång till resurser samt vilka resurser som behövs.
- Identifiera logistiska aspekter så som transport av material och personal.
- Identifiera lämplig lokal.
- Utförande av behovsanalys.

- Utförande av risk- och sårbarhetsanalys för övningar där så är relevant.
- Upprättande av planeringsgrupp.

Utöver frågan om vilka aspekter som bör inkluderas i planeringsfasen finns det även skillnader i olika metoders tillvägagångssätt för planering. Amerikanska *Department of Homeland Security* (DHS) (2013) beskriver tre huvudplaneringsmöten för planering och framtagning av en övning: (1) initialt planeringsmöte, (2) halvtidsplaneringsmöte och (3) avslutande planeringsmöte. Andra varianter av denna metod benämner istället dessa möten som faser vilka inkluderar ett flertal planeringsmöten och fortgående arbete (Kick 2014; CCDCOE 2012; Australian Institute for Disaster Resilience (AIDR) 2012).

Andra metoder lägger inte samma vikt vid att dela upp planeringsarbetet i faser utan fokuserar istället på att ingående beskriva vilka aspekter som ska ingå i planeringsarbetet som helhet (MSB 2012; Enisa 2009; NIST 2006; Dewar 2018).

Det kan vara svårt att strikt följa en specifik planeringsmetod, vilket bland annat beror på skiftande förutsättningar mellan olika övningar. Planeringsmetoder underlättar planeringsarbetet, i synnerhet för individer och organisationer som saknar tidigare erfarenhet av att planera och genomföra övningar. Vidare underlättar planeringsmetoder framtagning och utvärdering av framtida övningar, även för erfarna individer och organisationer. Detta eftersom de skapar en övergripande struktur i planeringsarbetet som kan överföras till övningar av varierande innehåll och skala. Det är dock inget krav att följa tillvägagångssättet i etablerade planeringsmetoder för att den planerade övningen ska vara framgångsrik. Det viktiga är att de aspekter som bedöms viktiga att ta hänsyn till för den specifika övningen inarbetas på ett utförligt och korrekt sätt främst av vilka bör vara mål och syfte för övningen (Dewar 2018).

Metoderna för övningsplanering kan vidare kompletteras genom att inkludera individer med tidigare erfarenhet gällande övningsverksamhet i planeringsgruppen. Detta beror på att det inte finns någon universal-lösning för planering av cyberförsvarsövningar gällande bland annat övningstyp, resurser och deltagartyp. Resultaten av denna rapport visar också på erfarenhet som en starkt bidragande orsak till framgångsrika övningar, inte minst för övningar med tekniskt innehåll.

Vidare är det ofta viktigt att inkludera övningens beställare i övnings-planeringen för att både beställare och planeringsgrupp ska försäkras om att övningen planeras och utvecklas i enlighet med vad beställaren förväntar sig.

Planering för SAFE Cyber 2019 påbörjades i januari 2019, cirka 8 månader innan övningens genomförande. Planeringsgruppen bestod av åtta individer med olika bakgrund och erfarenhet kring övningsplanering och genomförande. I detta fall inkluderades övningens beställare i planeringsgruppen.

Den initiala planeringsfasen av övningen utgjordes till stor del av diskussioner kring syftet för övningen och vilka mål som potentiellt kan uppfyllas vid genomförandet. Vidare diskuterades hur övningens syfte potentiellt påverkar övningens möjliga utformning, det vill säga vilka övningsmetoder och övningstyper som kan tänkas vara relevanta för att syfte och mål ska kunna uppfyllas. Nästa avsnitt presenterar mål och syfte med övningen SAFE Cyber 2019 samt en kortare beskrivning ur ett allmänt perspektiv hur syfte och mål tas fram samt hur dessa bör beskrivas.

3.2 Övningens mål och syfte

Den viktigaste aspekten för planering och utveckling av en övning är att övningen har ett tydligt syfte och mål. En övnings mål och syfte påverkar utformningen av övningen, exempelvis vilken övningstyp som är relevant att nyttja (Dewar 2018).

Mål kan formuleras och kategoriseras på olika sätt, ett exempel på detta är att använda huvudmål som kan brytas ned i specifika delmål. En vanlig metod för att definiera mål är SMART, vilket är en engelsk akronym som på svenska översätts (med mindre variationer) till: specifika, mätbara, accepterade, realistiska och tidsatta. I vissa sammanhang tilläggs även en aspekt i att mål ska vara adekvata (vilket ger akronymen SMARTA)(MSB 2012; Wilhelmson och Svensson 2013).

MSB (2012) beskriver att mål ska vara specifika, vilket innebär att de ska vara tydligt avgränsade och därmed inte inkludera aspekter som övningen inte hanterar. Det är också viktigt att måluppfyllnaden är *mätbar*. Parameterns *accepterade*, innebär att målen är godkända av beställaren samt övningsledningen. Mål bör vara *realistiska* och *tidsatta* så att de går att uppnå inom ramen för övningen. Slutligen ska målen vara lämpliga (*adekvata*)i förhållande till övningens syfte.

Övningen SAFE Cyber 2019 syftade till att öva hantering av incidenter i händelse av dator- och nätverksoperationer riktade mot Sverige och innehöll två delövningar. Dessa hade olika syften:

- *Den tekniska övningens mål är att öva deltagarna i att upptäcka, rapportera och hantera incidenter.*

- *Diskussionsövningens mål är att öva deltagarna i riskhantering och beslutsfattande.*

Ett av de övergripande målen för övningen var att utvärdera Försvarsmaktens mall för incidenthantering, som därför användes skarpt under övningen. Specifikt var målet att se civila organisationers och myndigheters möjlighet att förstå och använda mallen och om de resulterande incidentrapporterna var av tillräckligt god kvalitet för att skapa ett värde i form av underlättat beslutsstöd hos mottagaren.

3.3 Övningstyper

Det finns olika övningstyper och övningsmetoder att tillgå för genomförande av cyberförsvarsövningar. Vilka av dessa som är relevanta beror i första hand på övningens mål och syfte (Dewar 2018). Valet av övningstyp och metod påverkas även av andra aspekter så som budget, planeringstid och storlek på övningen.

Cyberförsvarsövningar delas in i två breda grupper, simuleringsövningar och diskussionsbaserade övningar (Dewar 2018; MSB 2009). Där simuleringsövningar ofta genomförs som tekniska övningar och utspelar sig i fiktiv miljö som så nära som möjligt försöker efterlikna verkligheten.

Huvudmålet för simuleringsövningar är att utsätta deltagare för situationer och incidenter som de skulle kunna utsättas för i verkligheten. Diskussionsbaserade övningar kan även de ha detta mål, men utan de tekniska element som ingår i en simuleringsövning. Utöver detta kan diskussionsbaserade övningar även nyttjas i en mer avslappnad miljö utan inspel eller tidspress för att främja diskussioner kring beslutsfattande och policylösningar relaterat till ett scenario (Dewar 2018).

Övningar kan vara av lärande eller prövande karaktär, där lärande övningar ämnar förse deltagare med ny kompetens och prövande syftar till att pröva deltagares kunskap eller förmåga att hantera en situation. Prövande övningar kan även nyttjas för att exempelvis pröva ny utrustning eller en nyligen sammansatt organisation för att upptäcka styrkor och svagheter (MSB 2009). Tekniska simuleringsövningar är i Sverige idag sällan av en prövande karaktär då det sällan finns fastställda processer att öva mot.

Det finns i huvudsak tre metoder att tillgå för tekniska cyberförsvars-övningar:

- Capture-the-flag vilket är en övningsmetod där minst två lag agerar som både blått lag (BT[9]) och rött lag (RT[10]), det vill säga att de försvarar sitt egna system samtidigt som de angriper det andra lagets system. Denna övningsmetod är skalbar och finns även i andra varianter.
- Blått mot rött vilket är en uppdelning av försvarande lag och angripande lag.
- Endast ett eller flera blåa lag som individuellt eller genom samarbete ämnar försvara sina system från ett angripande lag som är en del av övningsledningen.

Diskussionsbaserade övningar innefattar just diskussioner och kan genomföras med eller utan tekniska komponenter. Fördelar med övningstypen inkluderar bland annat att det krävs få detaljkunskaper om tekniska områden vilket gör det möjligt att ta med individer som saknar ingående teknisk erfarenhet eller kunskap. Vidare kräver diskussionsbaserade övningar sällan stora resurser vilket medför att de är flexibla gällande skalbarhet och tid för genomförande (Dewar 2018).

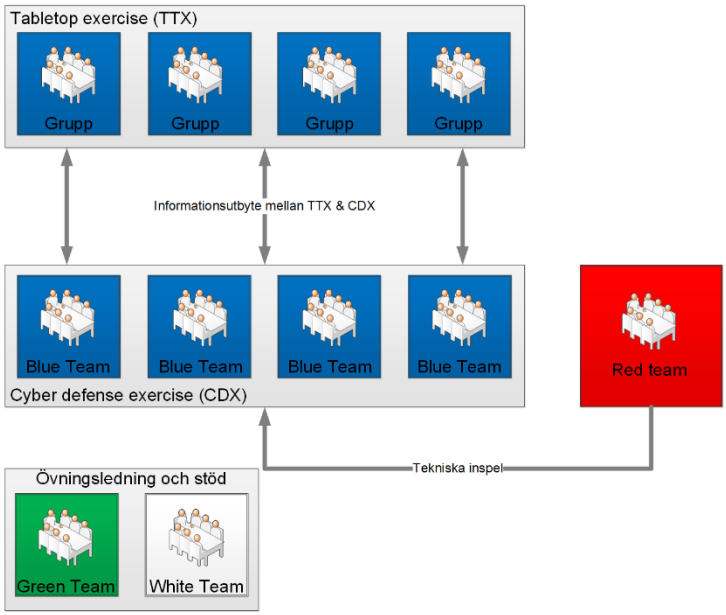
SAFE Cyber 2019 var av lärande karaktär och innehöll två olika övningsformat:

- En diskussionsbaserad övning (TTX) där olika aktiviteter och beslut diskuterades utifrån ett givet scenario med händelser över tid.
- En teknisk simuleringsövning (CDX) som genomfördes som en övning av typ 3 som beskrevs ovan. Simuleringsövningen arbetade utifrån samma givna scenario som diskussionsövningen.

Figur 1 visar en grov uppdelning av de övningslag som ingick i SAFE Cyber 2019 och visar även en uppdelning mellan övningsdelar.

[9] Eng. Blue Team, BT

[10] Eng. Red Team, RT



Figur 1. Övergripande uppdelning av övningslag och övningsdelar

CDX-övningen innehöll fyra blåa lag bestående av individer från olika organisationer som försvarade egna fiktiva system mot angrepp från det röda laget. Lagen arbetade oberoende av varandra och deltagarna uppmuntrades att inte diskutera övningen med individer från andra lag så länge övningen pågick. Eftersom alla lag löste samma uppgifter och inspel ansågs det ha en negativ effekt på övningens datainsamling om lagen kunde samarbeta.

TTX-övningen genomfördes med individer som normalt har en beslutsfattande arbetsroll. Deltagarna här delades in i fyra samtals-grupper, inte in i lag på samma sätt som i CDX, där problem och beslut diskuterades. Dessa diskussioner fortsatte sedan i gemensamma samtal med de övriga grupperna. Denna övning inkluderade också en form av inspel[11], dock inte tekniska utan istället händelser i övningsscenariots förlopp samt motspel i form av media.

[11] Se avsnitt 4.2

3.4 Övningsscenario

Ett övningsscenario är en övergripande skiss eller modell som beskriver tidslinjen för händelser och inspel i övningen. Utöver detta kan ett scenario även inkludera en bakgrundsbeskrivning av den omgivande (fiktiva) miljön för övningen. Ett scenario kan beskrivas som en berättelse eller som en tidslinje av händelser som utspelar sig i en bestämd miljö vid en bestämd tidpunkt (DHS 2013; MSB 2009). I diskussionsbaserade övningar är scenariot väldigt viktigt då det är scenariot som driver diskussionen och övningsdeltagandet.

Övningsscenarier måste vara realistiska och utmanande, samtidigt som de inte bör vara så komplicerade att deltagare blir överväldigade av svårighetsgraden (DHS 2013). Det är viktigt att övningsscenarier speglar situationer och händelser som kan inträffa i verkligheten eftersom detta påverkar deltagares lärande (Dewar 2018). Detta kan vara svårt för tekniska övningar eftersom IT-relaterade områden utvecklas så pass fort att det är svårt att hålla sig uppdaterad och veta vad som är relevant i dagsläget. Dewar (2018) påpekar att övningsscenarier och inspel ofta gynnas av tumregeln *less is more*. Det är exempelvis ofta inte relevant att deltagare ska få utstå en kaskad av tekniska inspel under en kort tidsperiod om dessa inte är troliga att inträffa i verkligheten (Dewar 2018).

Övningens utformning bör inte fixeras vid utveckling av ett scenario, istället ska scenariot utvecklas för att komplettera övningens mål och syfte. Därför bör utvecklingen av scenariot avvakta tills det att övningens syfte, mål och avgränsningar tydligt definierats och accepterats av beställare samt övningsledning (DHS 2013).

Erfarenhet från FOI:s tekniska övningsverksamhet visar att det är viktigt att de fiktiva system som används i simuleringsövningar är tillräckligt sårbara för att övningens inspel ska ha en effekt. Det vill säga att det för övningen är relevant att de system som används inte förses med samma skydd som verkliga system. Detta eftersom det är svårt att skapa tekniska inspel som påverkar ett välskyddat system. Vidare krävs att inspel är av övningskaraktär vilket innebär att om den skadliga koden läcker ut i verkligheten ska det vara uppenbart att det är skadlig kod för övnings- eller utbildningssyfte och inget som kan ha en större effekt på verkliga system. Det krävs därför rätt balans mellan realism och tillräcklig sårbarhet i systemet för att optimera utfallet av övningen.

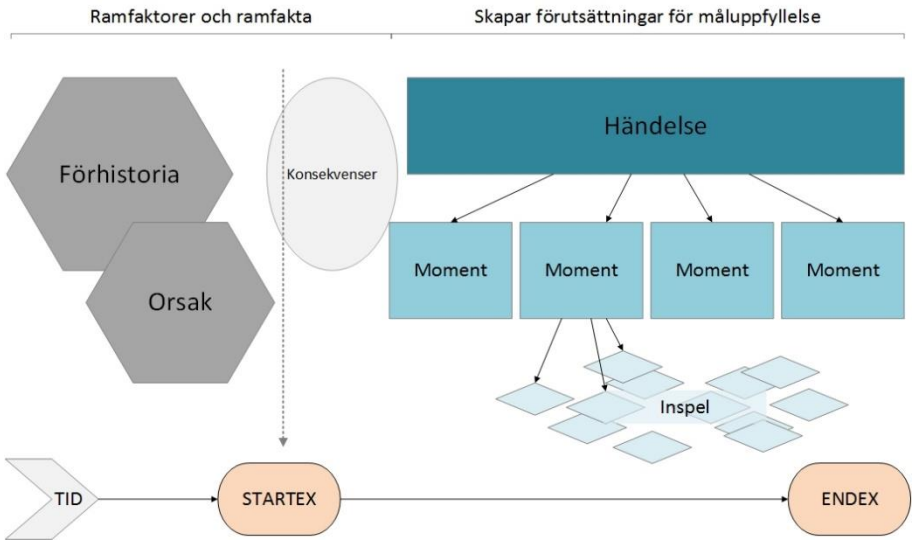
Kombinationen av de två övningstyperna påverkade utformningen av det scenario som användes i SAFE Cyber 2019. Eftersom övningarna var sammanlänkade var det nödvändigt att begränsa diskussionsövningens

möjliga scenarioutformning till att överensstämma med vad som var tekniskt rimligt att genomföra i simuleringsövningen.

Det övergripande scenariot för övningen SAFE Cyber 2019 utgjordes av en eskalerande gråzonsproblematik[12] i Sverige och närområdet, där Sverige utsätts för påverkansoperationer och nätverksattacker.

Scenariot för SAFE Cyber utspelade sig drygt ett år efter det senaste svenska riksdagsvalet. Förhistoria och de spelade incidenterna ägde rum runt Östersjön och påverkade främst Gotland och Storstockholm, men även närliggande regioner. Primärt sakområde för övningen var elförsörjning. Samtliga övade ingick i en fiktiv bolagskontext bestående av ett energibolag (*CleanFurnace*) och dess driftteam (*CleanFurnace IT*).

Figur 2 visar den övergripande tidslinjen för scenariot samt uppdelningen av förhistoria och vad som ingår i övningen.



Figur 2. Övergripande tidsflöde för scenariot i SAFE Cyber 2019

[12] Begreppet gråzon används vanligen för att beskriva en situation mellan krig och fred. En gråzonsproblematik kan orsakas av ett antal aktiviteter, exempelvis informationspåverkan, politisk påverkan, cyberangrepp och fysiskt sabotage.

3.5 Deltagare

Valet av demografi[13] för övningens deltagare påverkar övningens resultat (Dewar 2018). Resultatet för en övning gynnas ofta av att inkludera en bredare demografi av deltagare än en singulär arbetsroll. Valet ska dock grunda sig i övningens mål och syfte. En bredare demografi gynnar ofta deltagares lärande och upplevelser samtidigt som det gynnar resultatet för organisatören, viktigt är dock att individer innehar relevant kunskap och förmåga (Dewar 2018).

SAFE Cyber 2019 riktade sig till myndigheter med ansvar för cybersäkerhet i Sverige, samt till myndigheter och företag som ansvarar för system och tjänster kopplade till Försvarsmakten. Detta kan ses som en avgränsning i det demografiska urvalet för övningen.

I övningar som innehåller flera övningstyper är det viktigt att tydligt separera och klargöra skillnader i övningarnas mål och utformning. Detta för att tillfrågade organisationer ska ges tillräcklig information för att kunna anmäla rätt deltagare till rätt övning.

Deltagarna i SAFE Cyber 2019 bestod av ett antal olika aktörstyper, dels 18 olika övande organisationer med totalt 22 deltagare i fyra blåa lag, 29 deltagare i fyra diskussionsgrupper samt 9 deltagare från fyra organisationer i en expertstödsgrupp. Grupperna och lagen i TTX respektive CDX blandades med individer från olika organisationer. Alla inbjudna organisationer erbjöds att skicka representanter till båda övningstyperna.

3.6 Datainsamling

Datainsamling under övningar kan genomföras på flera olika sätt via manuell eller automatisk insamling. Tekniska övningar lämpar sig väl för att använda tekniska verktyg för insamling eftersom data kan samlas in automatiskt direkt i övningsmiljön. Exempelvis via dataloggar i systemen eller loggar av nätverkstrafiken i övningsnätverket. Manuell data-insamling utförs ofta av observatörer vilka närvarar under övningen. I vissa övningar kan det vara relevant att spela in ljud och bild av de övande för att komplettera observatörers uppfattningar under övningen (Wilhelmsson och Svensson 2013).

[13] Demografi i denna kontext avser kunskaper eller arbetsroll.

I övningens planeringsfas bör ett beslut fattas gällande hur datainsamling under övningen ska genomföras och i vilket syfte. Ett tillvägagångssätt är att samla in så mycket data som möjligt, vilket exempelvis kan vara gynnsamt i de fall där det råder oklarheter kring vilka data som kommer genereras i övningen och var i övningen de genereras. Ett annat tillvägagångssätt är att samla in data baserat på övningens mål och syfte. I dessa fall bör det vara tydligt vilka data som på förhand anses viktig samt var den genereras. En selektiv datainsamling riskerar att data som i efterhand visar sig vara viktiga inte samlas in under övningen. En fullständig insamling medför dock en risk att datamängden blir för stor och därmed ohanterlig.

Datainsamlingen för SAFE Cyber 2019 omfattade både manuell och automatisk insamling, för olika syften. Data samlades in via observationer både under planeringsfasen och under genomförandet av övningen för att stödja denna rapport, som beskrivet i avsnitt 1.3. Den automatiska datainsamlingen innefattade de incidentrapporter som samlats in i verktyget CEC[14], en webbaserad enkät samt loggar producerade av verktyget SVED[15]. Vidare samlades data även in via webbaserade enkäter samt intervjuer i syfte att utvärdera den incidentrapporteringsmall som nyttjades under övningen.

3.7 Lokaler och logistik

För övningar som utförs på plats med alla deltagare samlade på en plats spelar lokaler en viktig roll och måste bokas i god tid, i synnerhet för större övningar. Övningslokalerna måste inte bara vara av tillräcklig storlek för antalet deltagare individer med avseende på säkerhet men även bekvämlighet och funktion. Exempelvis måste det finnas tillgång till toaletter av tillräckligt antal, möbler i form av bord och stolar samt ett bekvämt inomhusklimat (DHS 2013).

För tekniska övningar påverkar tillgång till adekvat nätverksinfrastruktur valet av lokal. Exempelvis behöver övningar arrangerade av FOI tillgång till stabil internetanslutning för de VPN-boxar som används för att ansluta till infrastrukturen CRATE i Linköping. Ofta innebär detta att nätverks-anslutningen måste vara trådburen.

[14] Se avsnitt 4.1

[15] Se avsnitt 4.2

I dagarna före och under övningen är det viktigt att en lokal support-personal finns på plats som kan hjälpa övningsledning med frågor och problem relaterade till lokalen.

SAFE Cyber 2019 genomfördes i FOI:s lokaler i Kista. CDX genomfördes i lokaler på plan 8 innanför skyddsobjektet och TTX i konferenscentret som ligger utanför men i anslutning till skyddsobjektet.

3.7.1 Mat, dryck och material

Övningsledningen bör, om möjligt, förse deltagare med måltider och dryck under tiden som övningen pågår (DHS 2013). Mat och dryck påverkar deltagares energinivå vilket i sin tur påverkar deras prestation och upplevelse av övningen. Det är därför särskilt viktigt att alla aspekter kring eventuell mat och dryck är välplanerade. Exempelvis går inte en bortglömd lunch att lösa ad hoc på ett bra sätt vid större övningar.

Det är viktigt för övningsledningen att ta hänsyn till att vissa deltagare kan ha restriktioner gällande kost. Eventuella allergier eller kost-restriktioner bör meddelas till ansvarig i övningsledningen i god tid innan övningen så att rätt kost kan beställas. Utöver måltider kan det även vara relevant att erbjuda fika under förmiddag och eftermiddag för att deltagare och övningsledning ska kunna hålla en jämn energinivå under hela övningsdagen.

Utöver mat och dryck bör övningsledning även planera för att tillgodose deltagare med material som kan tänkas vara relevant för övningen. Detta kan exempelvis inkludera pennor, skrivblock och whiteboardtavlor.

Planeringen måste även ta hänsyn till transport och logi för deltagarna. Ofta kan det även vara relevant att anordna transport av deltagare till och från övningslokalen. Vidare bör man för större övningar vara ute i god tid gällande bokning av hotellrum för deltagare. Det finns en fördel i att alla deltagare bor på samma hotell då det underlättar transport till och från övningslokalen.

Övningar av större storlek som hålls innanför ett skyddat område bör ta hänsyn till den tid det tar att identifiera, registrera och förse deltagare med identifikationsbrickor. Processen för detta är normalt tidsmässigt krävande för större sällskap, planeringsgruppen bör undersöka möjligheten att påskynda processen utan att påverka säkerheten. Vidare får utomstående individer normalt inte röra sig fritt inne på ett skyddat område, vilket medför att det kan vara relevant att hyra in extra väktare för att eskortera deltagare, exempelvis för rökpauser och dylikt.

Eftersom SAFE Cyber 2019 pågick från morgon till eftermiddag över flera dagar ansågs det viktigt att förse deltagarna med mat, dryck och

fika. Antalet deltagare inklusive personal i övningsledning och stödpersonal innebar att det inte var rimligt att ta med sig alla till en restaurang för att äta. Vidare var det inte relevant att låta deltagarna hantera lunchen själva eftersom att delar av övningen genomfördes innanför skyddsobjektet. Alla luncher för övningen SAFE Cyber 2019 hanterades via ett cateringföretag som levererade färdiga luncher till övningslokalerna. Fika inhandlades från ett konditori samt från en livsmedelsbutik i närheten av övningslokalen. Vidare inhyrdes möbler för CDX-lokalerna samt whiteboardtavlor till de olika övningsdelarna.

3.8 Ekonomi

En budget för övningen bör alltid fastställas i tidigt skede. Denna ska inkludera allt som omfattar övningen (exempelvis personal, lokalhyrning, teknik och resor). Budgeten kan i sin tur bidra till etableringen av ambitionsnivå för övningen (MSB 2012; Wilhelmson och Svensson 2013).

Simuleringsövningar är generellt resurskrävande då de kräver virtuella- eller separerade nätverk där övningen ska utföras. Detta kräver hårdvara och infrastruktur som måste hanteras och underhållas av personal, vilket innebär en ekonomisk kostnad (Dewar 2018). Vidare är det för simuleringsövningar viktigt att i möjligaste mån återanvända tidigare övningars infrastruktur i syfte att spara kostnader. Diskussionsbaserade övningar är generellt inte lika resurskrävande som simuleringsövningar vilket beror på att de inte kräver varken hårdvara eller infrastruktur för att genomföras (Dewar 2018).

En viktig kostnadsaspekt att ta hänsyn till för större övningar är personaltid i samband med själva övningen. I det ekonomiska utfallet för SAFE Cyber 2019 kan urskiljas att antalet timmar som lagts i det tidiga planeringsarbetet av FOI-personal är relativt lågt (250 timmar[16]) i jämförelse med planering och utveckling de närmsta månaderna och veckorna innan övningens genomförande (1033 timmar[17]), så väl som under själva genomförandet (500 timmar). Detta beror till stor del på att fler individer inkluderas och arbetet intensifieras när övningen närmar sig, vilket i sin tur innebär att kostnaden eventuellt ökar på grund av

[16] Mellan januari och juni

[17] Mellan juli och september

övertid. Relaterat till detta är det viktigt att kontrollera den tid som läggs på övningsrelaterat arbete innan övningen. Generellt upplevs övningsrelaterat arbete som positivt och roligt vilket ofta leder till att personal lägger ner mer tid på sådant arbete än som kanske är nödvändigt. Vidare finns det ofta mycket förbättringsarbete som kan utföras på de övningsmoduler som används. Det är därför viktigt att styra arbetet till att uppfylla väldefinierade beslutade mål och leveranser. Den tid som läggs får med andra ord inte inkludera förbättringsarbete som inte är direkt relevant för övningen.

Totalt kostade övningen cirka 2.6 miljoner SEK där arbetstimmarna (totalt 1776 timmar för FOI) stod för drygt 2 miljoner SEK, vilket inte inkluderar tiden som spenderats på utvärdering och analys efter övningen (bland annat denna rapport). Övriga kostnader inkluderar bland annat konsulttimmar från Secana på 500 000 SEK. Övriga kostnader inkluderar exempelvis catering för övningen, transport och hotell för FOI-anställda samt hyra för möbler.

En annan aspekt som driver kostnader är oförutsedda problem som uppstår under övningens planering. Ett exempel på detta ges i nästa avsnitt, gällande lokalbyte och möblering.

3.9 Utmaningar och problem

Nedan beskrivs de utmaningar och problem som uppstod i planeringsfasen för övningen SAFE Cyber 2019.

En av planeringsgruppens stora utmaningar var att kombinera en teknisk övning med en diskussionsbaserad övning. Problemet ligger inte i att utföra två övningstyper samtidigt utan att få händelser i den ena övningen att påverka händelser och beslut i den andra på ett realistiskt sätt. Ett stort problem här är att tempot i övningstyperna skiljer sig. En CDX går normalt i väldigt högt tempo jämfört med en TTX där diskussionernas omfattning påverkar hur fort övningen fortskrider. Det är därför väldigt svårt att få övningarna att agera på samma information och inspel under samma tidsperiod. Vidare har övningstyperna olika perspektiv, där diskussionsbaserade övningar ofta ser på ett helhetsperspektiv i syfte att förbättra beslutsfattandet. Tekniska övningar har i regel ett snävare perspektiv och är mer detaljorienterade relaterat till de egna systemen och hur dessa påverkas av angrepp. Tekniska övningar lägger ingen större vikt vid frågor som varför ett system angrips utan fokuserar på att minimera effekterna på de angripna systemen. De båda perspektiven kan ytligt sett se väldigt lika ut, men är övningsmässigt mycket olika.

I ett tidigt skede i planeringen bestämdes en plats för genomförande av SAFE Cyber 2019. Drygt två månader innan genomförandet visade det sig dock att de tänkta lokalerna av okänd anledning inte längre var tillgängliga under övningsdagarna. På grund av övningens storlek uppstod ett problem att på så kort varsel hitta en ny lokal i och med att det finns ett begränsat antal tänkbara lokaler av adekvat storlek och med tillräckligt god IT-infrastruktur, inom rimligt avstånd till Stockholms innerstad.

Alternativa lokaler undersöktes under sommaren och med en dryg månad kvar beslutades att övningen skulle genomföras i FOI:s lokaler i Kista. Där den tekniska övningen skulle genomföras innanför skyddsobjektet på plan 8 och diskussionsövningen samt utbildningar och föreläsningar skulle genomföras i konferenscentret i anslutning till skyddsobjektet.

Att behöva genomföra ett så pass sent påtvingat lokalbyte är inte optimalt. Detta kunde dock lösas och övningen hållas samman, genom ombokning av andra verksamheter samt genom spridning av övningsledning och övade till olika utrymmen i samma byggnad. På detta sätt kunde förutsättningarna för en lycka övning säkerställas.

4. FOI:s tekniska infrastruktur för övningar

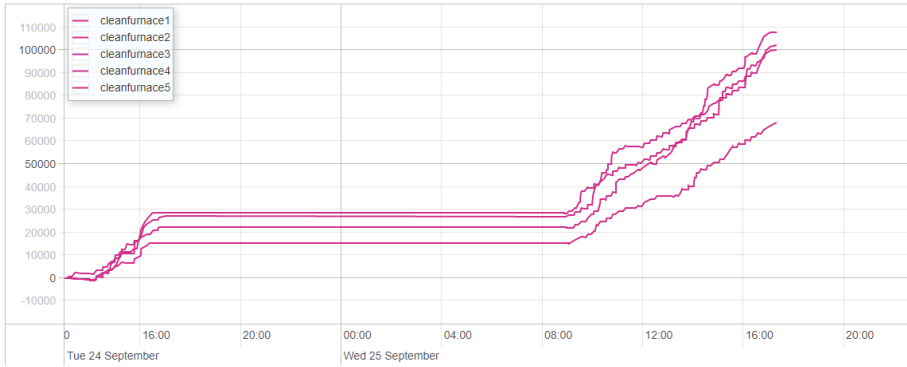
Det tekniska innehållet i en övning är ofta specifikt för övningen och vem som arrangerar övningens innehåll. Därför kommer följande avsnitt att fokusera på de tekniska aspekter gällande, verktyg, infrastruktur, mjukvara och hårdvara som inkluderas i övningar som arrangeras av FOI.

Många av FOI:s tekniska cyberförsvarsövningar utförs på liknande sätt. Oftast är det någon typ av industriell funktion som ska hållas i gång av de deltagande lagen. Funktionen i sig varierar ofta och kan bland annat utgöras av energiproduktion eller tillverkning av fysiska produkter.

De deltagande lagen ska hantera angrepp som görs mot det egna systemet samtidigt som de ansvarar för att hantera den normala driften av funktionen vilket inkluderar fiktiva inköp av material eller bränsle.

Hantering av angrepp sker genom incidentrapporter, vilka fylls i ett verktyg i övningsmiljön och skickas därefter till rättningsteamet i övningsledningen. Rättningsteamet vet vilka inspel som körts samt när de kördes och kan på så sätt avgöra riktigheten i incidentrapporten, det vill säga om laget i fråga har upptäckt ett faktiskt angrepp eller något irrelevant som de tror är ett angrepp. Utöver det ges poäng baserat på incidentrapportens kvalitet och läsbarhet.

Lagens prestation mäts genom poängräkning, vilken i huvudsak baseras på ovannämnda incidentrapporter. Lagen ges även poäng för att funktionen hålls igång där poäng ges i tidsintervall, exempelvis var femtonde minut. Poängsättningen är i första hand till för att motivera deltagare och ge en möjlighet för lagen själva att se hur de presterar genom en poänggraf (se figur 3). Det är sällan poängräkningen används för att värdera lagens prestation, eftersom övningarna ofta är av en lärande snarare än en prövande typ.



Figur 3. Poängraf SAFE Cyber 2019

CRATE är namnet på FOI:s egenutvecklade anläggning för träning, övning och simulering inom cyberrelaterade områden. Anläggningen består av cirka 500 fysiska servrar i ett kluster beläget i FOI:s lokaler i Linköping. CRATE bygger till stor del på öppen källkod och egenutvecklad mjukvara. I CRATE kan man skapa datornätverk i ett simulerat Internet (spelnät) innehållandes flera tusen virtualiserade enheter av en rad olika typer, exempelvis mailservrar, filservrar och vanliga kontorsdatorer med olika installerade applikationer. Det går även att installera fysiska enheter så som skrivare, telefoner eller PLC:s. I spelnätet kan man sedan skapa och hantera IT-angrepp genom att injicera dessa mot något av datornätverken i spelnätet.

FOI använder CRATE för att genomföra tekniska övningar. Eftersom en majoritet av storskaliga övningar genomförs på distans krävs användande av VPN-boxar[18] för att ansluta till den tekniska infrastrukturen i Linköping.

4.1 Verktyg

Utöver CRATE används ett antal verktyg och mjukvaror för övningshantering och genomförande. I de övningar som genomförs av FOI används i regel bärbara datorer som tillhandahålls av FOI. För SAFE Cyber 2019 kompletterades dock dessa datorer med datorer från Försvarsmakten i syfte att säkerställa att så många som möjligt av de övade skulle ha tillgång till en egen dator. Alla bärbara datorer kördes

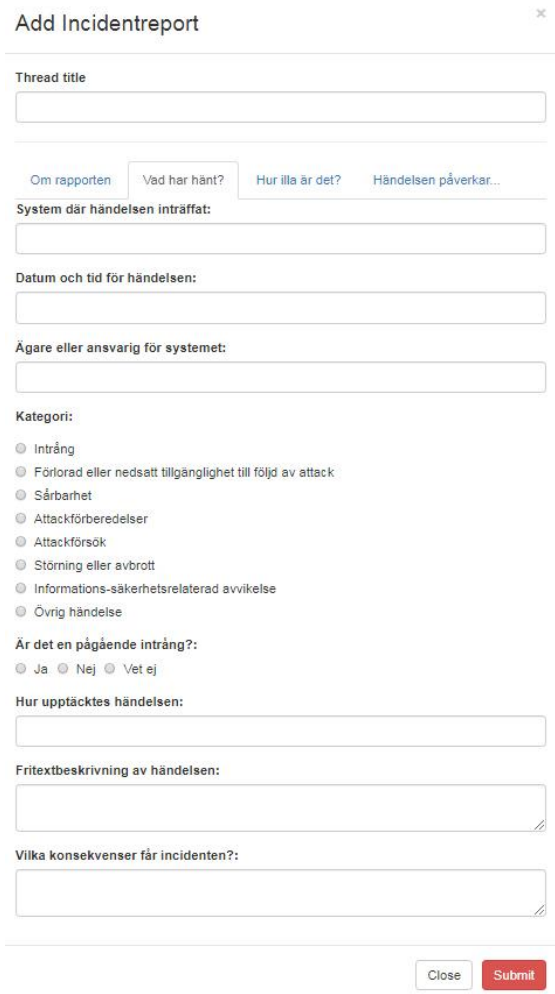
[18] Se Bilaga A: Övningsverktyg

med operativsystemet *Kali Linux* och innehöll alla de verktyg som operativsystemet har som standard, vilket bland annat inkluderar *Metasploit.*

SNART är en specialframtagen virtuell maskin som används för att lyssna på all nätverkstrafik i ett specificerat nätverkssegment. SNART innehåller ett antal verktyg vilka bland annat inkluderar *tcpdump, Snorby, snort* och *Etherape*. Threat Studies. Vällingby: FHS.

Bilaga A: Övningsverktyg innehåller en beskrivning med exempel av de verktyg som användes i SAFE Cyber 2019.

CRATE *Exercise Control* (CEC) är ett webbaserat verktyg som används för att hantera kommunikation mellan övningsledning och deltagare. Det är i CEC som deltagarna fyller i incidentrapporter, som sedan skickas till rättningsteamet i övningsledningen, som i sin tur beslutar om den inskickade rapporten ska resultera i några poäng för laget eller inte. CEC innehåller även poängräkningen som används för de flesta tekniska övningar som genomförs av FOI. Figur 4 visar ett exempel på hur den incidentrapports mall som användes i SAFE Cyber formulerades i CEC.



Figur 4. Incidentrapportsmall i CEC.

Det bör noteras att figur 4 inte visar hela incidentrapportsmallen. Flikarna med blå text i bilden innehåller formulär som bland annat rör konsekvenser av en incident. Data samlas under övningen även in automatiskt via verktygen SVED och CEC, som tidigare beskrivits.

4.2 Inspel

Tekniska inspel, eller *injects*, refererar i detta fall till strukturerade angrepp som utförs mot system som blått lag ska försvara. Inspel bör vara relevanta och jämförbara med aktuella versioner av de angrepp som används mot system vid tiden för övningen. Det är dock viktigt att de inspel som används baseras på angrepp eller angreppstyper som är välkända. Viktigt är även att inspelen är av tillräcklig variation för att deltagarintresse ska hållas på en hög nivå. Inspelen bör även relatera till varandra både logiskt och kronologiskt i syfte att stärka realismen.

Inspelen bör göras i stigande svårighetsgrad, det vill säga att det första angreppet som spelas ska vara relativt enkelt att upptäcka och åtgärda. Detta syftar till att deltagare ska komma in i övningens tankesätt och få en förståelse för hur övningen kommer se ut. För att övningsdeltagare ska ha inspel att agera emot under tiden för hela övningen är det viktigt att sprida ut inspelen så att de täcker tiden från när övningen startar tills när den slutar. Det måste samtidigt finnas en balans för hur ofta inspel sker, de får inte komma för utspritt då det riskerar att övningsdeltagare får för lite att arbeta med, de får inte heller komma för tätt då deltagarna kan bli överrumplade och riskera att inte hinna med. Det ska dock sägas att beroende på vad övningens mål och syfte är kan det vara relevant att köra inspel i en högre frekvens och försöka överrumpla deltagare, exempelvis för att öva på hur man hanterar stress i en pressad situation.

Tabell 2 visar exempel på de inspel som används i FOI:s övningar, till exempel i SAFE Cyber 2019. Tabellen visar även när poäng ska ges samt hur många poäng som tilldelas, vilket är ett stöd för rättningslaget i övningsledningen.

Tabell 2. Inspelsexempel med beskrivning och poängsättning

Namn	Beskrivning	Poängsättning
Bittorrent i nätverket	µTorrent körs av användare för att ladda ned och dela material. I detta fall laddas skadlig kod ned.	Upptäck Bittorrent-trafik med EtherApe eller Snort.

DDos mot företagets webbserver	Ett DDoS-angrepp körs mot webbservern	Upptäck angreppet med EtherApe eller annan sensor.
Hydra används för att bruteforca en FTP-server i DMZ.	Hydra är ett verktyg för att automatiskt knäcka lösenord vilket genomförs via ordboksangrepp[19]	Upptäck med EtherApe eller Snort.

Inspel och händelser hanteras via verktyget *Scanning, Vulnerabilities, Exploits and Detection* (SVED)(Holm och Sommestad 2016) vilket är ett av FOI egenutvecklat verktyg. SVED kopplar samman flera andra verktyg och erbjuder styrning av dem via ett grafiskt gränssnitt. Med hjälp av SVED går det till exempel att schemalägga inspel via Metasploit som sedan körs automatiskt. Detta innebär att inspel kan skriptas och köras samtidigt mot alla blåa lag i en övning samtidigt.

Utöver tekniska inspel kan inspel i form av media vara relevant. I FOI:s infrastruktur finns möjligheten att implementera mediainspel genom webbaserade tidningar samt en Twitter-liknande funktion, vilka båda finns implementerade i övningsnätverket. Dessa inspel nyttjades i den diskussionsbaserade övningen för SAFE Cyber 2019.

4.3 Sårbarheter

Utöver inspel finns även sårbarheter inbyggda i de system som används i FOI:s övningar. Dessa sårbarheter inkluderar bland annat gamla användarkonton från tidigare anställda i den fiktiva miljön.

Skälet till att ha inbyggda sårbarheter i övningsmiljön är dels att göra miljön tillräckligt sårbar för att vara relevant att öva i, och dels för att öka realismen i övningen. Samtidigt påverkas även övningens realism negativt av vad som kan ses som en konsekvens av dessa sårbarheter. Under övningar är det vanligt att deltagare upptäcker många av de inbyggda sårbarheter som finns i miljön. Naturligtvis vill deltagarna då åtgärda dessa sårbarheter för att säkra upp systemen, men detta kan dock inte alltid tillåtas av övningsledningen eftersom detta kan påverka möjligheten till att köra vissa inspel.

[19] Eng. Dictionary Attack

4.4 Utbildning

Det är i regel alltid relevant för en övningsledning att ge deltagare någon form av utbildning eller genomgång innan övningen påbörjas. Övningsledningen bör hålla åtminstone en allmän genomgång av övningen som bland annat diskuterar övningens utformning, mål och syfte, tidplan samt andra allmänna förutsättningar (Wilhelmson och Svensson 2013).

Vidare är det i FOI:s tekniska cyberförsvarsövningar viktigt att ge deltagarna kortare föreläsningspass angående övningens tekniska aspekter, exempelvis gällande vilka verktyg som används samt hur de bör användas under övningen.

I FOI:s tekniska övningar är det även ofta nödvändigt att inkludera ett föreläsningspass angående incidentrapportering för att diskutera hur det görs och varför det är viktigt, eftersom de flesta av FOI:s tekniska övningar involverar någon form av incidentrapportering.

Inför SAFE Cyber 2019 genomfördes först en introduktion och genomgång av övningen. Under genomgången presenterades övnings-bestämmelser samt övningens metodik. Detta följdes sedan av en genomgång av scenariots förhistoria samt hur övningen utvärderades utifrån dess mål och syfte. Därefter gavs en gemensam utbildning gällande hur Försvarsmakten bedriver incidenthantering.

Diskussionsövningsdeltagare (TTX) och tekniska övningsdeltagare (CDX) delades därefter upp och gavs föreläsningar som var specifika för respektive övningstyp. CDX-deltagare gavs exempelvis en introduktion till den tekniska övningsmiljön och de verktyg som används där, samt vilket utfall som förväntades av den tekniska övningen. Totalt lades tre timmar på utbildning innan övningens start.

5. Resultat och lärdomar från SAFE Cyber 2019

Följande avsnitt beskriver upplevelser gällande övningen SAFE Cyber 2019:s planering och genomförande. Avsnitten innehåller återkoppling från övningsdeltagare, FOI:s övningsledning inklusive stödpersonal samt planeringsgruppen.

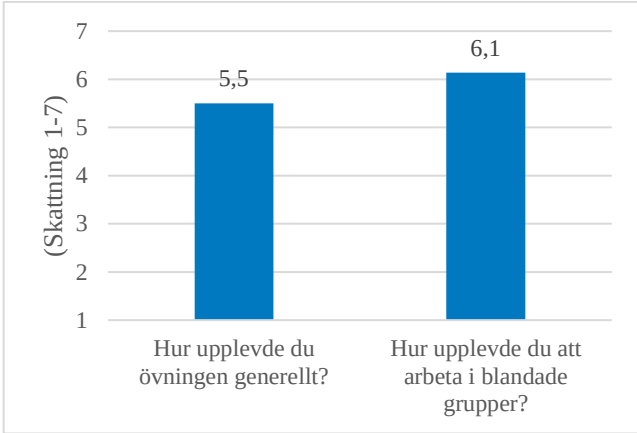
Informationen som upplevelserna baseras på är resultatet av flera olika informationsinsamlingar. Dessa beskrivs kortfattat i inledningen av respektive avsnitt.

Notera att avsnitten i detta kapitel endast beskriver återkoppling i form av kommentarer, vilka kan framstå som motsägelsefulla eller osammanhängande. Det bedömdes dock som viktigt att presentera en sammanställning av alla kommentarer som ett underlag för diskussionen i kapitel 6.

5.1 Återkoppling och upplevelser från övningsdeltagare

Återkopplingen från övningsdeltagarna baseras till största del på en enkät som deltagarna ombads genomföra i anslutning till övningens avslut. Enkäten innehöll exempelvis frågor gällande den generella upplevelsen av övningen och incidentrapporteringsmallens relevans för deltagaren. Samtliga enkätfrågor återfinns i Bilaga B: Enkätfrågor. Vidare inkluderas även deltagarkommentarer inhämtade genom observationer som utfördes under övningen och den utvärdering som genomfördes i samband med övningens slut. Nedan följer en sammanställning av deltagarnas återkoppling.

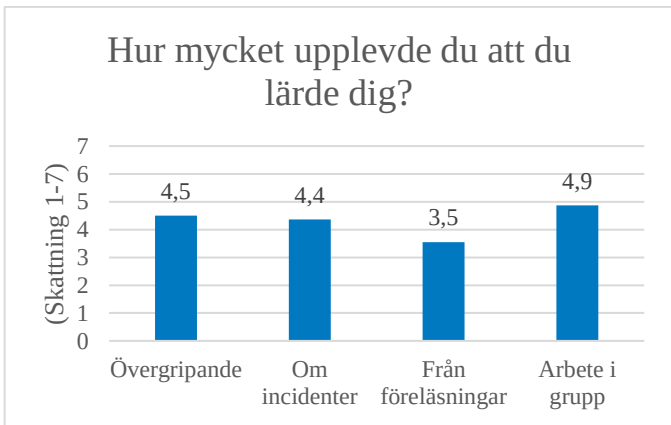
Den första frågan i enkäten behandlade deltagarnas upplevelse av övningen skattat i en skala 1-7 där 7 var det mest positiva svaret. Den andra frågan gällde deltagarnas upplevelse att arbeta i blandade grupper med individer från olika organisationer, även här på en skala 1-7. Figur 5 visar deltagarnas svar på dessa frågor.



Figur 5. Enkätsvar fråga 1 och fråga 2.

Resultaten visar att deltagare överlag upplevde övningen positivt och att det ansågs som en positiv upplevelse att arbeta med individer från andra organisationer.

Fråga 3 i enkäten innefattade fyra delfrågor om hur mycket deltagarna upplevt att de lärt sig gällande de fyra respektive aspekterna som delfrågorna berörde. Även denna fråga skattades i en skala 1-7. Figur 6 visar deltagarnas svar på dessa frågor.



Figur 6. Enkätsvar från fråga 3.

Arbete i grupp var den aspekt deltagare upplevde att de lärde sig mest av, vilket delvis kan vara ett resultat av gruppsammansättningen av individer från olika organisationer, något som upplevdes som positivt enligt fråga 2. Det uttrycktes även ett önskemål om att behålla gruppsammansättningen av lag med individer från olika organisationer inför nästa övning, eftersom det upplevdes som positivt och lärorikt att arbeta med

individer från olika organisationer och med olika befattning och erfarenheter. Vidare upplevdes det som positivt att det fanns en blandning av deltagare från privat och offentlig sektor. De olika perspektiven som detta innebar var enligt deltagare både lärorikt och intressant.

Ett önskemål som uttrycktes gällde en mer ingående utbildning eller genomgång av CEC och hur verktyget fungerar. Det uttrycktes även förbättringsförslag för CEC. För det första bör det göras möjligt att editera och komplettera rapporter efter insändning. För det andra bör CEC vara tillgängligt från alla övningsrelaterade nätverk. Utbildningsmässigt uttrycktes även önskemål om att inkludera mer bakgrundsinformation kring variabler som deltagare på förhand inte känner till, exempelvis är det svårt att veta hur en sektor fungerar om man inte har arbetat i den tidigare. Från TTX-deltagarna framfördes även önskemål om mer information gällande företaget och redan fattade beslut för att ge deltagarna en tydligare bild av var företaget beslutsmässigt befann sig i början av scenariot. En del antog exempelvis att företaget redan gått upp i krisledning medan andra grupper fattade det beslutet själva under den andra övningsdagen.

Det önskades tydligare definitioner för rapportmallens olika punkter i syfte att skapa en gemensam bild för alla deltagare. Risken är annars att punkter tolkas olika, vilket försvårar arbetet både för övningsledning (rättningslag) och för deltagarna.

Eftersom alla grupper i TTX diskuterade samma frågeställningar upplevdes det ibland som att de gemensamma diskussionerna ödslade tid då alla grupper i princip sade samma saker. I samband med detta uttrycktes önskemål om att det bör undersökas hur de gemensamma diskussionerna kan genomföras för att de ska upplevas som mer effektiva och värdefulla för de övande. Det största värdet upplevdes i denna version av övningen komma från de interna gruppdiskussionerna.

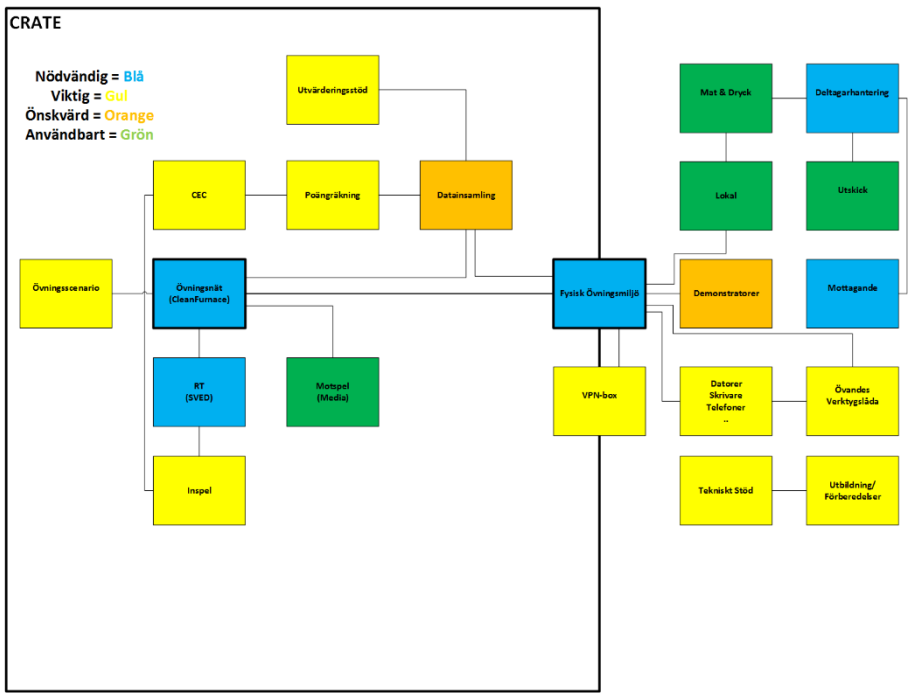
Det var oklart vilket mandat CDX-deltagare hade gällande motåtgärder och vad som var tillåtet att göra för att försvara systemen utan att riskera att förstöra spelmiljön. Vidare rådde en osäkerhet gällande önskat fokus när uppgifter ansågs olösbara av deltagare, bland annat om problem låg utanför den egna produktionsmiljön. Vissa undrade om de skulle anse problemet som olösbart och då inte vidta ytterligare åtgärder eller om det fanns något de skulle ha gjort.

Deltagare från både CDX och TTX uttryckte sitt uppskattande för kombinationen av övningstyperna, men uttryckte samtidigt ett önskemål om fler interaktiva moment mellan övningarna. Exempelvis ville deltagare i TTX erhålla fler incidentrapporter från CDX för att på så sätt kunna fatta bättre och mer välinformerade beslut. Vidare uttrycktes ett

förslag att ge CDX fler inspel från TTX och att varje TTX-grupp sammankopplas med ett CDX-lag och vice versa, vilket potentiellt skapat en bättre interaktion mellan övningstyperna.

5.2 Återkoppling och upplevelser från FOI:s övningsledning och stödpersonal

Återkoppling och upplevelser från FOI:s övningsledning och stödpersonal inhämtades från ett internt debriefing-möte som hölls efter övningens genomförande. Under mötet diskuterades och utvärderades övningen. Här användes Figur 7 som grund för skapandet av diverse kategorier som utvärderades. För varje kategori ombads varje deltagare att skriva på post-it-lappar hur saker relaterat till kategorin utfördes under övningen samt möjliga förbättringsförslag.



Figur 7 FOI:s övningskomponenter för CDX-delen av SAFE Cyber 2019

Dessa lappar sattes sedan upp på en whiteboardtavla där varje deltagare fick förklara sin ståndpunkt och andra gavs möjlighet att diskutera. En av kommentarerna gällande bilden var att den inte var komplett, då bland annat kategorin deltagare saknades. Bilden i figur 7 presenteras dock i samma format som vid mötet, i och med att det var dessa aspekter som

låg til grund för diskussionen. Nedan följer en sammanställning av de aspekter som denna utvärdering resulterade i.

Det uttrycktes här att det behövdes tydligare kommunikation till deltagare och övningsdelar när det serverades mat och fika. Detta upplevdes som otydligt under övningen, vilket ledde till att vissa missade att äta och dricka. Vidare uttrycktes önskemål om en stadigare lunch för att bättre hålla energinivån uppe, vilket kan anses viktigt eftersom övningsdagarna pågick mellan 9.00-17.00.

Förutom upplevda otydligheter kring mat och fika framkom att även informationen om var olika övningsdelar, personal och till exempel toaletter var belägna i lokalerna. Ett förslag på lösning av detta var att skapa en karta över lokalerna innehållande sådan information. Vidare upplevdes en brist på kännedom om nyckelpersoner och hur dessa kunde kontaktas.

En genomgång av övningens alla tekniska inspel utfördes av FOI på förhand innan övningen för att säkerställa att dessa fungerade korrekt och för att upptäcka eventuella problem. Det upplevdes dock finnas ett behov att testköra hela övningen, det vill säga att genomgången även borde inkluderat TTX-aspekter för att upptäcka eventuella problem.

Det uttrycktes även önskemål om att de inspel som användes under övningen skulle inkludera fler angrepp som var specifikt riktade mot industriella informations- och styrsystem, i dagsläget baseras de flesta inspel på angrepp mot vanliga IT-system. Inspelen behöver planeras bättre tidsmässigt, i övningen kördes många inspel under övnings-dagarnas första halva för att sedan avta mot dagens slut.

Övningsverktyget CEC hanterades heller inte optimalt under övningen. Exempelvis vill de som rättade inkomna incidentrapporter endast se incidentrapporter, men fick se alla möjliga typer av meddelanden. Det behövs alltså möjlighet att filtrera på meddelandetyp i CEC. Vidare inkom incidentrapporter med fält i olika ordning vilket försvårade arbetet för rättningslaget. Det uttrycktes även önskemål om att inkludera test av CEC i genomgången som gjordes av övningens tekniska inspel, i syfte att upptäcka möjliga problem.

Det var relevant för deltagarna i TTX att ta del av incidentrapporter från CDX. Däremot var all information i incidentrapporterna inte relevant för TTX, vilket ytterligare motiverar möjligheten till att kunna filtrera meddelanden i CEC. En annan ståndpunkt som uttrycktes var att CEC inte var realistiskt att använda för TTX, istället bör en lagledare för CDX-lag utses för att hantera information och frågor från TTX.

Samverkan mellan CDX och TTX fungerade, men en högre grad av samverkan önskades. Vidare borde övningsstarten förskjutas mellan CDX och TTX i framtida övningar samt att scenariot bättre kompletterar de olika övningarnas utformning. Samtidigt uttrycktes att det röda laget behöver vara mer involverat i planeringsprocessen om en ökad samverkan ska vara möjlig.

Utbildningsmässigt upplevdes det som att de blåa lagen behövde fler instruktioner om hur incidentrapporterna skulle utformas och vad de skulle innehålla, samt hur de verktyg som ingick i övningen skulle användas, exempelvis CEC. Viss information som gavs till vissa övningsdelar var även relevant för andra delar av övningen, vilka också borde fått ta del av den informationen.

Övningslokalernas utformning uppfattades inte vara optimal för CDX, ett problem som inte upplevdes för TTX. Det var inte heller optimalt att CDX-övningen genomfördes innanför FOI:s skyddsobjekt och på en annan våning än TTX. Lokalerna innanför skyddsobjektet innehöll som bekant inte några möbler, vilket innebar att dessa hyrdes in för övningen. Hantering av möbelflytt och uppsättning utfördes av FOI:s övnings-personal, vilket enligt dessa individer inte var önskvärt. Om en sådan situation uppstår i kommande övningar bör flyttpersonal anlitas för att hantera möblernas transport och uppsättning. Relaterat till detta önskades även en form av riggningsplan som specificerar vem som gör vad under de närmaste dagarna innan övningen.

Det upplevdes också att det fanns en kommunikationsbrist mellan olika delar av övningsledningen vilket resulterade i att det under övningen uppstod problem, som egentligen hade kunnat upptäckas och lösas på förhand.

5.3 Återkoppling och upplevelser från planeringsgruppen

Återkoppling från planeringsgruppen inhämtades från observationer, diskussioner med deltagare i planeringsgruppen från FOI samt från ett överlämningsmöte som genomfördes med deltagare från Secana.

En ståndpunkt var att det inte alltid går att följa en och samma planeringsmetod från övning till övning. Den valda planeringsmetoden måste passa in med den specifika övningens mål och syfte, samt övningstyp. Vidare kan organisationer (kunder) ha egna planerings-metoder som de anser ska användas. Sammantaget innebär detta att planeringsgruppen måste visa flexibilitet i planeringen av olika övningar. Vidare påpekades av medlemmar i planeringsgruppen att det sällan finns

genvägar att ta i planeringsfasen, utan att planeringen måste få ta den tid som krävs.

Det upplevdes från medlemmar i planeringsgruppen att det fanns en otydlighet i vem som ägde vilka problem och uppgifter i planeringsfasen, samt vem som skulle se till att arbetet fortgick. Det uppfattades även som att de hållpunkter eller milstolpar som satts upp inte alltid följdes.

För mycket av övningsplaneringsarbetet fick utföras på kort tid innan övningens genomförande och under övningen uppstod diverse problem som behövde lösas. Det uppfattades även här som att en större del av dessa problem hade kunnat upptäckas om en ingående genomkörning av övningen hade genomförts på förhand. Den *dry-run* som genomfördes innan övningen räckte inte till för att upptäcka många av de problem som senare uppstod.

Den tekniska supportens resurser räckte inte till för att lösa alla problem tillräckligt snabbt, vilket innebar att resurser från andra övningsdelar togs för att hjälpa till med problemlösningen. Detta innebar i sin tur att dessa övningsdelar var tvungna att utföra sina uppgifter med reducerad personal.

De två övningarna hade dessutom olika behov, några av vilka inte på förhand förutsågs, vilket uppfattades bero på bristande kommunikation. Till exempel behövde TTX tillgång till teknisk utrustning, bland annat i form av datorer. Datorerna behövdes delvis för att ta del av övningens mediainspel och delvis för att ta del av de incidentrapporter som förmedlas via verktyget CEC. Detta behov tillgodosågs inte tillräckligt på förhand, vilket resulterade i att problemet istället fick lösas under övningen, något som i sin tur innebar ytterligare påfrestning på övningens tekniska support. Tydlighet i ansvarsfördelning och kommunikation noterades som en lösning på problemet.

Information mellan övningsdelar och övningsledning delades inte på ett tillförlitligt sätt. En förutbestämd och gemensam kanal för information till övningens alla delar uppfattades som en förbättringspunkt.

Avslutningsvis upplevdes samarbetet och det övergripande arbetet mellan organisationer och individer i planeringsgruppen fungera väl. Man lyckades skapa och genomföra en relevant övning som dessutom innehöll två olika övningstyper. Det påpekades dock att mer tid och resurser hade förbättrat utfallet och upplevelsen av övningen som helhet.

6. Diskussion

Detta avsnitt presenterar en diskussion kring de återkopplingsresultat som beskrevs i föregående kapitel. Liknande resultat mellan de tre återkopplande parterna sammanfattas och diskuteras i olika kategorier.

6.1 Planering

Dewar (2018) beskriver att varje övning är unik och att varje övning bör utformas för att stödja de mål och syften som är specifika för övningen i fråga. Detta kan relateras till problematiken kring planeringsmetoder som uttrycktes av planeringsgruppen. Specifikt uttrycktes att det inte alltid är möjligt att följa en och samma planeringsmetod från övning till övning. Något som även påverkas av att kunder kan ha egna planeringsmetoder de vill använda. Planeringsgruppen måste således vara flexibel i planeringen av olika övningar.

Det påpekades i inledningen till kapitel 3 att det är viktigt att planeringsarbetet påbörjas i god tid innan genomförandet av övningen och att arbetet ständigt fortgår för att undvika att en stor del av förberedelsearbetet måste utföras den sista tiden innan övningen ska genomföras. Enligt den återkoppling som gavs lyckades planerings-gruppen för SAFE Cyber 2019 inte med undvika detta, eftersom upplevelsen var att en stor del av det faktiska förberedelsearbetet utfördes de närmsta veckorna innan övningens genomförande.

Det ansågs i även som problematiskt att alla grupper i TTX diskuterade samma frågor. En möjlig förbättring gällande detta, som även uttrycktes i övningens utvärdering, skulle kunna låta grupperna hantera olika sektorer. Som exempel angavs att hälften av grupperna skulle hantera telekommunikationssektorn och andra hälften energisektorn. Detta skulle nödvändigtvis inte innebära olika frågeställningar för grupperna, men skulle potentiellt kunna ge en större spridning relaterat till hur frågeställningarna hanteras. Detta skulle i sin tur kunna innebära att de gemensamma gruppdiskussionerna skapar ett större värde. Vidare är båda sektorerna samhällsviktiga, vilket deltagarna då får möjlighet att lära sig mer om. Ett alternativ till detta är att de frågeställningar som används formuleras om för att skapa djupare och mer komplexa diskussioner, vilket potentiellt medför en större spridning i gruppernas diskussion och svar på frågeställningarna.

6.2 Kommunikation

I alla återkopplingsmoment uttrycktes någon form av kommunikationsbrist. Bland deltagare i CDX uttrycktes bland annat en fråga gällande mandat till motåtgärder. Oklarheten gällde vad som var tillåtet att göra och vem man skulle vända sig till med frågor om detta. Det fanns även utmaningar med att deltagare inte visste hur de skulle hantera problem som uppstod utanför den egna miljön. Relaterat till detta uttrycktes upplevelser av otydlighet kring var olika övningsdelar, personal, nyckelpersoner samt andra resurser var belägna och hur de skulle kontaktas. Detta kan delvis bero på att övningen var utspridd med den tekniska övningen innanför skyddsobjektet och diskussionsövningen utanför, på ett annat våningsplan.

Avsnitt 5.3 beskriver en kommunikationsbrist som främst relaterar till övningens planeringsfas gällande behov för de olika övningstyperna under övningen. Här hade kommunikationen i planeringsarbetet brustit i och med att TTX inte hade tillgång till de datorer som behövdes. Denna problematik påpekades av FOI:s personal, som uttryckte att bristande kommunikation i övningsledningen ledde till problem som annars hade kunnat upptäckas och lösas på förhand.

Ett annat område där det behövdes tydligare kommunikation gällde när det serverades mat och fika. Att missa en måltid eller fika kan upplevas som trivialt. Realiteten är dock att detta påverkar deltagares energinivå vilket i sin tur påverkar deltagares prestation och upplevelse av övningen, vilket även beskrivs i avsnitt 3.7.1. Det ska dock noteras att alla tider för mat och fika inkluderades i det schema som delades ut till deltagarna.

6.3 Verktyg

Innan övningens genomförande testades alla inspel via verktyget SVED. Det utfördes även en genomgång av övningen med planeringsgruppen. I efterhand visar det sig dock att det även borde utförts tester och genomgång av CEC samt övningsrelaterat material till TTX. Vidare ansågs det att övningen och dess tekniska komponenter borde ha testats i sin helhet, vilket skulle ha kunnat bidra till att problem som uppkom under övningen istället kunnat hanteras innan. Vikten av detta påpekas även i AIDR (2012), samt Wilhelmson och Svensson (2013). En fullskalig testning av övningen skulle även potentiellt kunna inkludera deltagarna där de under några timmar även ges möjlighet att bekanta sig med sin övningsgrupp och med övningsmiljön. Detta skulle dock innebära en logistisk utmaning i och med att alla deltagare måste samlas

innan övningen vilket kan vara problematiskt beroende på schemaläggning och resor.

Det är dessutom viktigt att inspel kommer i stigande svårighetsgrad och att de har en relevant utspridning tidsmässigt. Återkopplingen visar dock att det ansågs att övningens tekniska inspel kunnat hanteras bättre tidsmässigt, eftersom en stor del av inspelen skedde under övningsdagarnas första halva. Detta resulterade i att deltagare inte hade lika mycket att göra mot slutet av dagen. De inspelstider som bestämdes på förhand gjordes på basis av antagandet att deltagarna skulle ha en större *backlog* av uppgifter att utföra under dagens andra halva, något som visade sig vara fel. Vidare var inspelstiderna ett resultat av samspelet med TTX. Samspelet innebar i praktiken att inspelstiderna för båda övningar sammankopplades, vilket adderade en grad av komplexitet gällande schemaläggning för inspelen. Detta gav en negativ påverkan på möjligheterna att justera inspel för att bibehålla en lagom belastningsgrad för båda övningar.

6.4 Utbildning

Från figur 6 kan utrönas att deltagarna upplevde att de lärde sig minst från de föreläsningar som hölls innan övningens start. Deltagare ansåg att det hade varit nödvändigt med en mer ingående föreläsning kring verktyget CEC och hur detta skulle användas under övningen. Tydligare definitioner av incidentrapportmallens olika punkter ansågs även ha behövts i syfte att inte riskera förvirring då dessa punkter kan tolkas på olika sätt. Dessa synpunkter framkommer även i avsnitt 5.2, där det även påpekas att information som bara delades till en del av övningen även var relevant för andra delar. Avsnitt 4.4 beskriver att CDX och TTX delades upp och gavs viss information och föreläsningar separat. Återkopplingen visar dock att, mer information borde spridits till båda övningsgrupperna. Exakt vilken information som var relevant för båda övningsgrupper är oklart, men detta behöver hanteras till nästa liknande övning.

Det är ibland svårt att veta vilken teknisk kompetens som deltagare innehar. Även om kompetensen ibland kan antas vara väldigt hög inom ett specifikt område är det svårt att veta om deltagare använt samma verktyg som används i övningen. Det kan även vara relevant att inkludera en föreläsning om den tekniska infrastruktur som används, samt hur den bör interageras med i övningen, då detta inte alltid är helt uppenbart. En sådan föreläsning kan i sin tur spara tid för den tekniska supportpersonalen, eftersom de inte behöver gå runt till alla lag och besvara samma typ av frågor flera gånger. Denna typ av föreläsning borde, enligt

återkopplingen, ha inkluderats i övningen och är något som måste tas ställning till inför kommande övningar.

6.5 Genomförande

I avsnitt 5.3 påpekas att olika problem uppstod under övningen. De allra flesta problem löstes, i synnerhet de med potential att påverka hela övningen negativt. Det är i princip omöjligt att planera för och hantera alla tänkbara problem som skulle kunna uppstå under en övning redan innan övningen påbörjas. Oförutsedda problem kommer troligtvis att uppstå under övning och behöver således hanteras ad hoc. Det viktiga i problemlösningen är att minimera de potentiella effekterna ett problem kan få på en övning som helhet. För att underlätta problemlösning är det viktigt att planera för att ha tillräckliga resurser bland annat i form av stödpersonal samt att problemlösningen är flexibel. Flexibilitet avser här inte nödvändigtvis att problem löses helt men att de löses till en acceptabel nivå eller att alternativ för att ta sig runt problemet hittas.

Avslutningsvis går det från webbenkätens första fråga (se figur 5) att utröna att deltagarna överlag var nöjda med övningen. De problem som uppstod under övningen påverkade således inte deltagarnas upplevelse negativt. Kombinationen av övningstyper uppskattades, men den aspekt som upplevdes som mest positiv och lärorik var arbetet i grupp med individer från olika organisationer. Detta var ett önskemål som uttrycktes under utvärderingen av SAFE Cyber 2018 och som blev en viktig aspekt för planeringsgruppen att inkludera i år 2019 års övning. Alltså är en blandad gruppsammansättning en viktig aspekt att inkludera även i nästa övning.

6.6 Att kombinera två olika övningstyper

I avsnitt 3.9 beskrivs att det är svårt att kombinera en teknisk övning med en diskussionsbaserad övning och att problemet inte ligger i att utföra två övningstyper samtidigt. Istället ligger problematiken i att få händelser i den ena övningen att påverka händelser och beslut i den andra, på ett realistiskt sätt.

Anledningen till att detta problem uppstår är att övningstyperna skiljer sig åt i olika aspekter, däribland tempo. Tempot i en CDX är ofta högt jämfört med en TTX. I diskussionsbaserade övningar är målet ofta att främja diskussion och beslutsfattande, vilket innebär att diskussionens omfattning påverkar hur fort övningen fortskrider. I en CDX fattas beslut baserat på angrepp i form av inspel, något som typiskt innebär att beslut måste fattas snabbt för att motverka effekter från ett angrepp. Det är

därför svårt att få övningarna att agera på samma information och händelser under samma tidsperiod. Detta uttrycktes även i den återkoppling som sammanfattats i föregående avsnitt.

Skillnaden i perspektiv mellan övningarna som beskrevs i avsnitt 3.9 är en annan parameter som påverkar komplexiteten när två övningstyper kombineras, eftersom perspektiven påverkar övningstypernas interaktion. Vidare hade övningsdelarna i detta fall dessutom olika tidsperspektiv.

TTX-lagen fick ta del av incidentrapporter från CDX och hade via CEC full tillgång till alla rapporter. Detta var dock inte optimalt med tanke på den skillnad som fanns mellan övningstyperna gällande tempo. Det hade varit bättre att begränsa antalet och frekvensen med vilken TTX fick ta del av dessa incidentrapporter. Risken med att ge TTX-lagen full tillgång till alla incidentrapporter är att det blir för mycket att hantera på ett sätt som passar utformningen av en diskussionsbaserad övning. Trots detta fungerade samverkan mellan övningarna bra. Dock upplevde deltagare från båda övningar att de ville ha fler interaktiva moment mellan övningarna, exempelvis att information flödade dubbelriktat mellan TTX och CDX och inte bara från CDX till TTX som nu. Det bedömdes dock som väldigt svårt att få ett dubbelriktat informationsflöde att fungera på ett värdefullt sätt, vilket innebar att det var ett aktivt val att inte ha dubbelriktad kommunikation.

TTX-deltagarna påpekade att de ville ta del av fler incidentrapporter för att kunna fatta bättre beslut. Dock hade deltagarna full tillgång till CEC och alla incidentrapporter vilket föregående stycke också beskriver. Observationer under övningen visade dock att deltagarna i TTX sällan utnyttjade CEC och istället använde de incidentrapporter som skrivits ut av övningsledningen. Detta berodde enligt observationerna delvis på att deltagarna inte hann med att läsa rapporterna eftersom de samtidigt behövde hantera mediainspel och delvis på att det inte fanns tillräckligt med datorer.

Ett annat förslag för att hantera skillnaderna i tempo var att förskjuta övningsstarten mellan övningarna, där då TTX skulle påbörjas innan CDX. Detta skulle kunna förbättra interaktionen mellan övningarna i och med att TTX-grupperna ges ett större förberedelseutrymme för att kunna hantera fler incidentrapporter. Att utse en ansvarig representant i varje blått lag för att hantera kommunikation med TTX skulle även det kunna förbättra interaktionen mellan övningarna. Exempelvis skulle denna representant kunna besvara frågor från TTX gällande oklart innehåll i incidentrapporter, vilket förbättrar deras möjlighet till beslutsfattande och troligtvis skapar en högre grad av realism. För att detta ska generera bästa resultat krävs dock en tydligare koppling mellan övningsdelarna, exempelvis att lag CDX sammankopplas med lag i TTX.

Ett problem med en tydligare sammankoppling mellan lag i de olika övningsdelarna påpekades av deltagare i expertstödgruppen under övningens utvärdering. Specifikt gällde detta att beslut som fattas i TTX har potential att negativt påverka övningsupplevelsen för CDX. Som exempel angavs att om TTX ville stänga ner produktionen och dess tillhörande system vilket skulle innebära att motsvarande lag i CDX i praktiken inte skulle få något att göra. Denna problematik uppstod även under denna övning, övningsledningen gav då avslag på denna idé från TTX. Det kan argumenteras för att denna problematik påverkade realismen för TTX då de inte fick göra något som de skulle haft möjlighet till i en verklig situation.

Sammanfattningsvis kan sägas att övningen SAFE Cyber 2019 lyckades sammanfoga två olika övningstyper och få dem att interagera på ett sätt som skapade mervärde för deltagare. Det finns dock aspekter som kan förbättras till nästa övning och en problematik i en tydligare sammankoppling mellan TTX och CDX som måste lösas.

7. Slutsatser

Övningar är en viktig del i organisationers arbete för att försörja och vidareutveckla den kompetens och de rutiner som krävs för att hantera verkliga incidenter. Det blir allt viktigare att bibehålla kompetens gällande hantering av IT-relaterade incidenter, mycket på grund av samhällets stora beroende till just IT. Ett sätt att öva på detta är genom cyberförsvarsövningar, vilka kan planeras och genomföras på flera olika sätt.

Denna rapport har beskrivit ett flertal möjliga strategier och metoder som cyberförsvarsövningar kan genomföras med. Den sammanfattar även de aspekter för planering av cyberförsvarsövningar som kan anses som de mest centrala. Av dessa aspekter identifierar både denna rapport och andra publikationer mål och syfte som de två absolut viktigaste aspekterna för en framgångsrik övningsplanering och i förlängningen ett lyckat genomförande av övningen.

Det finns ingen universallösning för planering av cyberförsvarsövningar gällande bland annat övningstyp, resurser och deltagartyp. Därför underlättar erfarenhet i planeringsgruppen processen med att planera och genomföra övningar.

Planering av större övningar är en lång process där oförutsedda problem ofta uppstår. Flexibilitet hos planeringsgruppen för att kunna hantera sådana problem utan att det får stora effekter på övningen upplevs därför som värdefullt.

SAFE Cyber 2019 var en komplex övning att planera och genomföra, vilket inte minst berodde på kombinationen av två olika övningstyper som skulle interagera med varandra. Den lyckade övningen visar dock att det är möjligt att kombinera en teknisk simuleringsövning med en diskussionsbaserad övning och att det går att göra på ett sätt som skapar värde för deltagarna, såväl som beställare och övningsledning. Samtidigt visar resultaten att det finns potential för förbättringar i interaktionen mellan övningstyperna i syfte att skapa ett större värde för alla inblandade.

Referenser

Australian Institute for Disaster Resilience (AIDR)(2012). Managing Exercises. *Australian Disaster Resilience Handbook Collection.* Melbourne: AIDR.

Cooperative Cyber Defence Centre of Excellence (CCDCOE)(2012). *Cyber Defence Exercise Locked Shields 2012 After Action Report.*

Department of Homeland Security (DHS)(2013). *Homeland Security Exercise and Evaluation Program (HSEEP).*

Dewar, R. S. (2018). *Cyber Defense Report: Cyber Security and Cyber Defense Exercises*. september 2018, Center for Security Studies (CSS), ETH Zürich.

European Union Agency for Cybersecurity (Enisa)(2009). *Good Practice Guide on National Exercises.*

European Union Agency for Cybersecurity (Enisa)(2015). *The 2015 Report on National and International Cyber Security Exercises.*

Holm, H. och Sommestad, T. (2016). SVED: Scanning, Vulnerabilities, Exploits and Detection. *IEEE*. Baltimore, MD.

Kick, J. (2014). *Cyber Exercise Playbook.* Wiesbaden: MITRE.

Myndigheten för samhällsskydd och beredskap (MSB)(2012). *Handbok: tekniska informations- och cybersäkerhetsövningar.*

Myndigheten för samhällsskydd och beredskap (MSB)(2012). *Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar.*

National Institute of Standards and Technology (NIST)(2006). *SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (SP800-84). Gaithersburg: NIST.

Sommestad, T. och Lundholm, K. (2012) *Detektering av IT-attacker – Intrångsdetekteringssystem och systemadministratörens roll* (FOI-R--3419—SE).

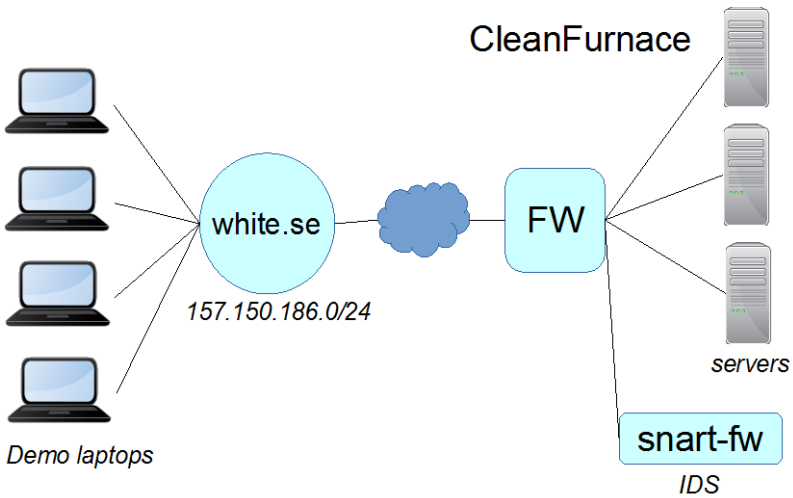
Wilhelmson, N. & Svensson, T. (2013). *Handbook for planning, running and evaluating information technology and cyber security exercises.* The Swedish National Defence College (FHS), Center for Asymmetric Threat Studies. Vällingby: FHS.

Bilaga A: Övningsverktyg

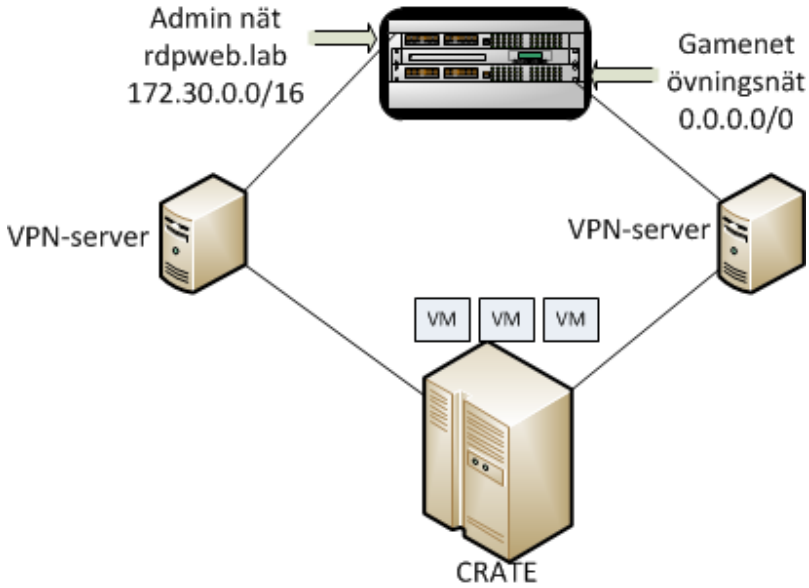
Introduction

In this document we will give an introduction and overview of useful tools for the real exercise. The picture below shows a part of the gamenet where the real exercise will run, and the small cloud is our local version of the real Internet. In this document it is assumed we are connected to a local ISP network and you are going to study the company Cleanfurnace1 external exposure to the Internet. We also have access to their internal IDS called Snart.

VPNBOX



The VPNBOX is connected to CRATE via several VPN connections. CRATE is our large cluster of servers located in Linköping. Each team have five servers, each running between 8-10 virtual machines. One of the VPNs is connected to the administrative side of CRATE, where you can connect directly to the servers. This is done on the upper switch in the box. During the exercise, you are only allowed to connect to your own virtual machines via remote desktop (rdesktop). The other VPN is connected to the gamenet, where the exercise will take place. You can connect directly into the intranet in the CleanFurnace



organization with your laptop. This is done via the lower switch. There should be a note attached that show which ports are connected where.

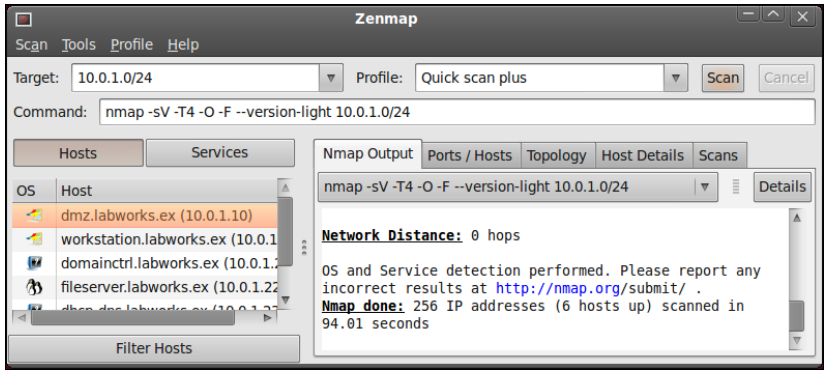
rdpweb.lab

When you connect to the admin net, you will automatically get an adress in the 172.30.105.0/24 network. Here you can go to **http://rdpweb.lab** via a web browser. This webpage contains a list of rdp connections to the machines in the CleanFurnace network.

Zenmap

Zenmap is a tool for mapping of networks. The tool can scan large networks and see what computers or equipment are connected to the net, what services they run and even try to guess what operating system they run. It can also try to determine if there is a firewall blocking traffic and which type of firewall it is. In this exercise, you will try using Zenmap for mapping your company network.

1. Start Zenmap (by desktop icon on the left side).
2. Enter **Target:** 199.206.0.0/24 (Cleanfurnace1)
3. Choose **Profile:** Quick scan plus
4. Click **Scan** and write the start time here _____
5. After about 2 minutes you will get a list of host names on the left side. On the right side of the window you will also get a list of open ports and a guess of what operating system it is running.



You can also use the command line version of Zenmap called **nmap**. It has many useful options:

- -sn do a simple ping scan and list the responding computers.
- -sV tries to probe the version of services running on the scanned ports.
- -O tries to detect operating system.
- -F tries to do a very fast scan and creates a heavy load on network traffic.
- -T0 do an extremely slow scan.

Arp-scan

SCADA systems like PLC:s and similar, can be quite sensitive about port scanning. Some might even stop working completely. Therefore, it is better to use a nicer program called **arp-scan,** but it can only scan local network segments.

6. Open a Terminal (left side icon)
7. Try running the command **arp-scan -l** and look at how many other laptops you can see in your local network.

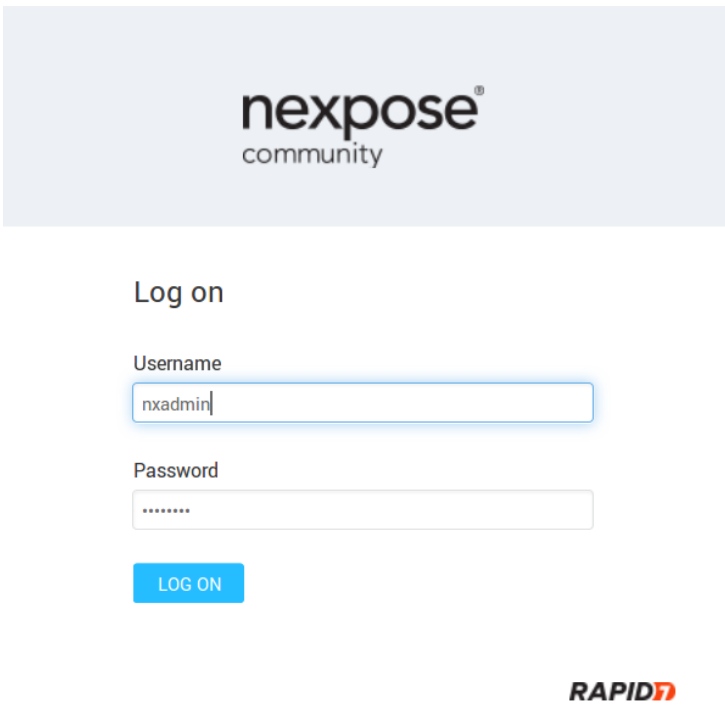
Ripe.net

If you need to know who owns a certain IP address range you can look it up at the website **http://www.ripe.net**

8. Open a web browser (left side compass icon)
9. Lookup the ip number 199.206.0.1 at http://www.ripe.net.

Nexpose

Nexpose is a tool for network vulnerability scanning. It takes over where Zenmap ended its work. Nexpose scans all open ports and services on a computer and tries different attacks and probes. It does not really perform a real attack, but instead does some simple testing if the vulnerability exists.



10. Start Nexpose by clicking on the Nexpose icon on the left side.
11. Login with user name **nxadmin** and password **rootroot.**

12. Define your target (what to scan) by clicking on **CREATE SITE** on the left side.
13. On the configuration page enter a **Name** of your choice.
14. Click on the **Assets** menu and enter your target IP number.

15. Then click on **SAVE & SCAN** at the upper right side. Time started _____
16. The scanning finishes after a few minutes.
17. To view the scanning report, click on the IP number or host name in the section **Completed Assets**. Identified vulnerabilities are listed in **Vulnerability Listing**. The most critical vulnerabilities are labeled **Severity: Critical**. Sort by the Severity column by clicking on its label. Write notes about the vulnerabilities of the computer in the list in the Zenmap section.

If you want to start or stop Nexpose, you can do this in a terminal window with the commands "**startnex**" or "**stopnex**". When changing IP-address this can be necessary.

Nexpose performs more than 60,000 tests to be able to identify more than 14,000 different vulnerabilities. Each test is written as a script, which simulates an attack. When the tests are completed, a report of the vulnerabilities found will be generated. In the report, vulnerabilities are classified on a three-step scale. The lowest classification is called Moderate. It is a note, which for example advises that a particular service should be disabled or reconfigured. The next classification is called Severe, and it implies that there is a risk that your system could be exploited. Critical is the most serious class, and means that your system has a critical security hole that an attacker most probably is able to exploit.

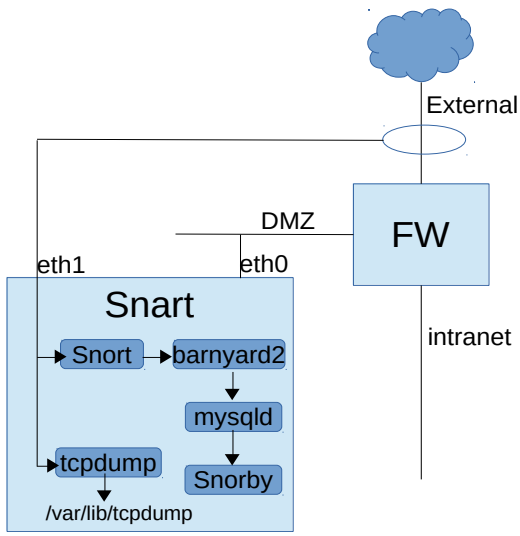
We are using a version of Nexpose called Community Edition. It is free and can be downloaded from http://www.rapid7.com. The community edition has several limitations compared to the commercial editions,

though. Nexpose and competing vulnerability scanners on the market such as Nessus, Core Impact, Saint and more, are mostly used by security departments of larger corporations and consultants to perform penetration tests. The most advanced attacks require a lot of manual work. Nexpose cannot find all types of vulnerabilities, so a deep knowledge and understanding of your systems is needed in order to protect them. Automated tools such as Nexpose will give you a very good start, though.

Sensor Snart

In order to do faster login to the Snart sensor, you can use the following commands:

18. First, run **ssh-keygen** in a terminal. Answer <return> on all questions, except answer “y” on “Overwrite (y/n)”.
19. Run **ssh-copy-id root@snart-fw.cleanfurnace1.se** to copy you ssh key. Enter the password for snart-fw. Now you can ssh without password.



There are two IDS-like network sensors named Snart placed in the company’s networks. The sensors are named snart-int and snart-ext. Both Snart sensors are connected to a monitor port in the local network. The sensor snart-int is monitoring the company’s intranet and snart-ext is monitoring the company's external interface. The sensors are running Snort/Barnyard/Snorby for network attack detection. You can also log on

to these machines with ssh and study monitor packets on the “eth1” interface.

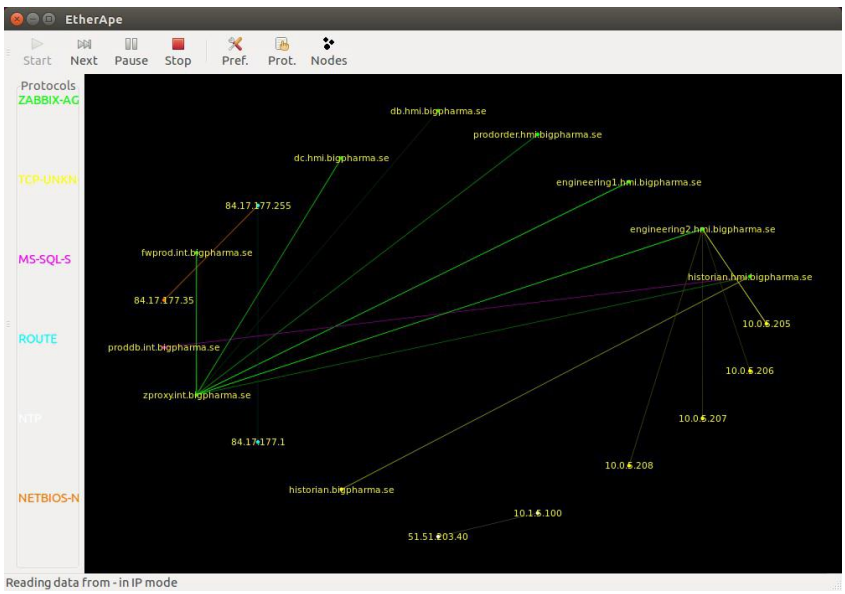
Etherape

The program **etherape** displays network activity in a graphical window. It reads network packets from an interface and displays the hosts in a star like shape. Then it draws lines between hosts and the thickness of the line indicates the amount of traffic.

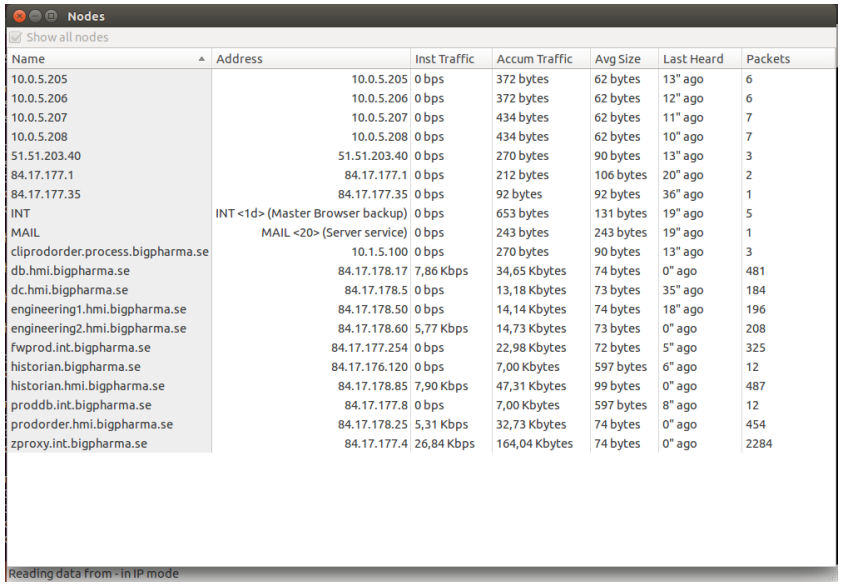
Very thick lines usually means someone is downloading a large file, or potentially doing a Denial of Service attack.

20. Start etherape with the following command: **ssh -Y root@snart-fw.cleanfurnace1.se 'etherape -i eth1 -f "not host snart-fw.cleanfurnace1.se"'**

Explanation of options: The **-Y** means that ssh should forward a X window to your local computer. The **-i eth1** indicates which interface etherape will listen on. The **-f** is followed by a filter to remove the X window session traffic from the capture.



If you want to see the actual bandwidth numbers, you can click on the **Nodes** button in the upper right menu. Below is a screenshot of a table with names, addresses and traffic amounts.



Name	Address	Inst Traffic	Accum Traffic	Avg Size	Last Heard	Packets
10.0.5.205	10.0.5.205	0 bps	372 bytes	62 bytes	13" ago	6
10.0.5.206	10.0.5.206	0 bps	372 bytes	62 bytes	12" ago	6
10.0.5.207	10.0.5.207	0 bps	434 bytes	62 bytes	11" ago	7
10.0.5.208	10.0.5.208	0 bps	434 bytes	62 bytes	10" ago	7
51.51.203.40	51.51.203.40	0 bps	270 bytes	90 bytes	13" ago	3
84.17.177.1	84.17.177.1	0 bps	212 bytes	106 bytes	20" ago	2
84.17.177.35	84.17.177.35	0 bps	92 bytes	92 bytes	36" ago	1
INT	INT <1d> (Master Browser backup)	0 bps	653 bytes	131 bytes	19" ago	5
MAIL	MAIL <20> (Server service)	0 bps	243 bytes	243 bytes	19" ago	1
cliprodorder.process.bigpharma.se	10.1.5.100	0 bps	270 bytes	90 bytes	13" ago	3
db.hmi.bigpharma.se	84.17.178.17	7,86 Kbps	34,65 Kbytes	74 bytes	0" ago	481
dc.hmi.bigpharma.se	84.17.178.5	0 bps	13,18 Kbytes	73 bytes	35" ago	184
engineering1.hmi.bigpharma.se	84.17.178.50	0 bps	14,14 Kbytes	74 bytes	18" ago	196
engineering2.hmi.bigpharma.se	84.17.178.60	5,77 Kbps	14,73 Kbytes	73 bytes	0" ago	208
fwprod.int.bigpharma.se	84.17.177.254	0 bps	22,98 Kbytes	72 bytes	5" ago	325
historian.bigpharma.se	84.17.176.120	0 bps	7,00 Kbytes	597 bytes	6" ago	12
historian.hmi.bigpharma.se	84.17.178.85	7,90 Kbps	47,31 Kbytes	99 bytes	0" ago	487
proddb.int.bigpharma.se	84.17.177.8	0 bps	7,00 Kbytes	597 bytes	8" ago	12
prodorder.hmi.bigpharma.se	84.17.178.25	5,31 Kbps	32,73 Kbytes	74 bytes	0" ago	454
zproxy.int.bigpharma.se	84.17.177.4	26,84 Kbps	164,04 Kbytes	74 bytes	0" ago	2284

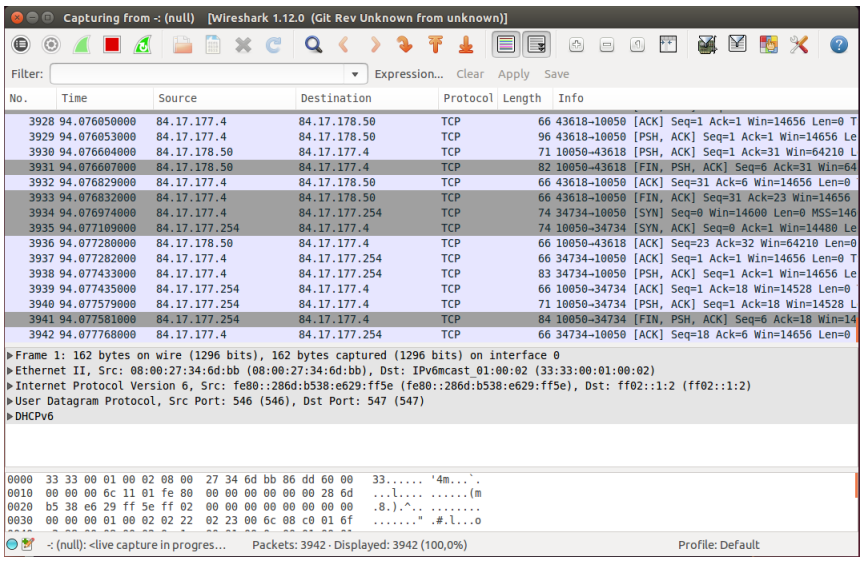
You can also set some preferences from the **Pref** menu button. The default is to update the screen every second and forget hosts after two minutes. Increase these numbers if you want a larger sample each time you look at the screen.

Wireshark and tcpdump

Wireshark is a network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file.

21. Start Wireshark with the following command:
    ssh -Y root@snart-fw.cleanfurnace1.se 'wireshark -i eth1 -f "not host snart-fw.cleanfurnace1.se"'
22. Click on the green shark fin in the button menu to start capturing traffic on interface eth1

Next picture shows the live capture of the packets in the upper window. In this window, you can click on individual packets and then see their content in the middle window. Wireshark recognizes different protocols and split them into parts, which can be seen in the middle window. Click on the small arrows on the left to open the parts of the packet. In the bottom window, you see the raw data in the packet.



Below the menu buttons, you can find the Filter Toolbar. A display filter can be entered into the filter toolbar. A filter for HTTP, HTTPS, and DNS traffic might look like this:

tcp.port == 80 || tcp.port == 443 || tcp.port == 53

Selecting the Filter: button lets you choose from a list of named filters that you can optionally save. Pressing the Return or Enter key, or selecting the Apply button, will cause the filter to be applied to the current list of packets. Selecting the Reset button clears the display filter so that all packets are displayed (again).

The Wireshark tool is good for analyzing network packets, but it has a risk of security vulnerabilities when showing live captures. Instead, the **tcpdump** program should be used for live capture. Tcpdump is a simpler network sniffer and can also save the captured packets to a file. The Snart computers has a continually running tcpdump, which saves captured packets to the directory /var/lib/tcpdump on the Snart computer.

23. List the contents of the tcpdump directory with **ssh root@snart-fw.cleanfurnace1.se "ls -l /var/lib/tcpdump"**
24. Copy the latest capture file to your laptop **scp root@snart-cleanfurnace1.se:/var/lib/tcpdump/pcap_1234_00.**

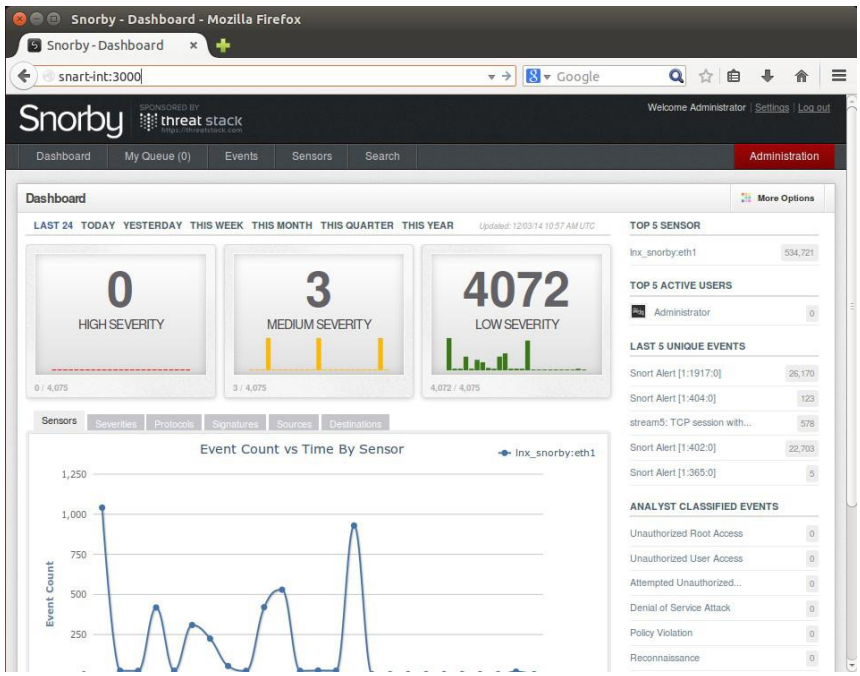
Snorby

Snort is a network intrusion detection engine. It listens to the monitor interface and tries to find network packets that contain potential network

attacks. Snort is running in the Snart sensor and collects all alarms in a local database. Snorby is a web interface to this database of snort alarms.

25. Access Snorby by pointing your web browser to **http://snart-fw.cleanfurnace1.se:3000**
26. The username is "snorby@snorby.org" and the password is "snorby".

After logging in you will see the dashboard. This is just a simple overview showing graphs over the number of alarms per hour. You can see a more useful page if you click on the Events tab, where you can see a list of alarms. You can click on each alarm and see what was attacked and the triggered snort rule. On the Search tab you can search or filter for certain event types.



The port scanning we did with Zenmap and Nexpose should be stored in the snort database.

27. Search the Snorby database for all events from your own IP number with severity 1. Check the time stamps and figure if Zenmap triggered severity 1 or not.

It is also possible to modify or add new snort rules. The current rule set is located in /etc/snort/rules/ You can modify /etc/snort/local.rules and then activate the local.rules in /etc/snort/snort.conf

Gtkpinger

This utility program sends a ping to all hosts in a preconfigured list. Then it lists them in either a command shell window or a separate GUI window.

28. Run the command: **gtkpinger Stensson.pinger &** to open the GUI interface to pinger. The argument to the command is the configuration file which is stored in the home directory on your laptop client. You can quit the pinger *with the 'q' key.*

The configuration file contains a list of hosts to scan. Edit this file if you want to add more hosts. Their definitions are located at the end of the file in the "HOSTS SECTION". You can also change timeouts for hosts. The format for each host is:

<IP or domain name>=<Description> [,arp][,[no]log], ok_delay, noreply_delay, long_delay]

The optional fields are:

arp – Indicate that host will be pinged using ARP request instead of ICMP ECHO.
Log – Indicate that host will be logged in the host log.
Nolog – Indicate that host will not be logged in the host log.
ok_delay – when ping successful, wait this time before sending next ping request.
noreply_delay – when ping failed, wait this time before sending next ping request.
long_delay – delay of reply after which the host is marked as delayed.

Syslogserver

You also have a syslog server located inside the company's network. The syslog on this server currently only show logs from the AD-server. You are free to reconfigure this server to any purpose. The syslogserver is located at syslog.int.cleanfurnace1.se

Command line tools (Windows/Linux)

There are a couple of useful command line tools when doing forensics on a computer. First we have the command "netstat" that works similarly on both Linux and Windows.

Windows:
netstat -an (show everything, listening ports, active connections)
netstat -b (which exe,dll)

Linux:
netstat -nlp (show only listening connections including pid/processname)

Sometimes it is useful to find which way a packet travels through the network. This can be discovered with the “tracert” command in Windows and “traceroute” in Linux. The “route” command can also be useful to see how the computers own routing table.

Windows:

tracert 8.8.8.8
route print
route print 150.*

Linux:

traceroute 8.8.8.8
route -n

Listing the currently running processes on a computer can be necessary if you suspect some hostile activity. In Windows, you can use the “tasklist” command and “ps” in Linux.

Windows:

tasklist	
tasklist /m	(includes dll)
tasklist /svc	(services for the processes)
tasklist /v	(domain,owner,pid,memory,cpu time)
taskmgr	(graphical tasklist)
net start	(list started services)

Linux:

ps aux	(all running processes)
top	(realtime process list)
rc-status	(list started services)
service --status-all	(alternative list started services)

Other useful Linux commands:

ifconfig	(list network interfaces)
dig	(DNS search)
nc	(generic connect to a service)

Bilaga B: Enkätfrågor

Nedan listas de frågor som användes i övningens avslutande enkät.

1. Hur upplevde du övningen generellt? [skattning 1-7]
2. Hur upplevde du att arbeta i blandade grupper (med andra organisationer)? [skattning 1-7]
3. Hur mycket upplevde du att du lärde dig? [skattning 1-7]
    a. Övergripande?
    b. Om incidenter?
    c. Från föreläsningar?
    d. Av arbetet i din grupp?
4. Hur realistisk upplevde du att övningen var? [skattning 1-7]
5. Hur upplevde du arbetet i gruppen? [skattning 1-7]
6. Hur fungerade incidentrapporteringsmallen i denna övning? [skattning 1-7]
7. Hur relevanta upplever du att följande fält under rubriken OM RAPPORTEN i incidentmallen är på din arbetsplats? [skattning 1-7]
    a. Datum
    b. Sekretessnivå
    c. Paragraf OSL
    d. Kontaktperson
8. Hur relevanta upplever du att följande fält under rubriken VAD HAR HÄNT i incidentmallen är på din arbetsplats? [skattning 1-7]
    a. System där händelsen inträffat
    b. Datum och tid för händelsen
    c. Ägare eller ansvarig för systemet
    d. Är det ett pågående intrång
    e. Fritextbeskrivning av händelsen
9. Hur relevanta upplever du att följande fält under rubriken HUR ILLA ÄR DET i incidentmallen är på din arbetsplats? [skattning 1-7]
    a. Allvarlighet
    b. Risktagning
    c. Exponering
    d. Tidskriticitet
    e. Tillförlitlighet i bedömning

10. Hur relevanta upplever du att följande fält under rubriken HÄNDELSEN PÅVERKAR i incidentmallen är på din arbetsplats? [skattning 1-7]
    a. Ledning och genomförande av nationella operationer
    b. Ledning och genomförande av internationella operationer
    c. Verksamhets- eller myndighetsledning
    d. Produktionsledning
    e. Förmåga att kommunicera med [ÖVERORDNAD ORG]
    f. Förmåga att kommunicera med [SIDOORDNAD ORG]
    g. Förmåga att kommunicera med tredje part
    h. Förmåga att kommunicera med allmänheten
    i. Trovärdighet
    j. Påverkan på extern aktör
11. Hur relevanta upplever du att följande fält under rubriken HÄNDELSEN PÅVERKAR –åtgärder i incidentmallen på din arbetsplats? [skattning 1-7]
    a. Vidtagna åtgärder
    b. Planerade fortsatta åtgärder
12. Hur relevant upplever du att följande kategorier är att använda för incidentrapportering inom din organisation? [skattning 1-7]
    a. Intrång
    b. Förlorad eller nedsatt tillgänglighet till följd av attack
    c. Sårbarhet
    d. Attackförberedelse
    e. Attackförsök
    f. Störning eller avbrott
    g. Informationssäkerhetsrelaterad avvikelse
    h. Övrig händelse
13. Inför nästa övning, vad ska vi behålla, utveckla eller eventuellt ta bort? [Fritext]

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se