Tuomas Komulainen

Palvelujen pystyttäminen kyberturvan oppimis-ympäristöön

Tradenomi
Tietojenkäsittely (AMK)
Syksy 2024

KAMK • University of Applied Sciences

Tiivistelmä

Tekijä(t): Komulainen Tuomas

Työn nimi: Palvelujen pystyttäminen kyberturvan oppimisympäristöön

Tutkintonimike: Tradenomi (AMK), Tietojenkäsittely

Asiasanat: verkkosivupalvelin, internet, kyberturvallisuus, virtualisointi

Opinnäytetyön aiheena oli koululle rakennettavan kyberturvallisuuden oppimisympäristön verkossa sijaitsevien palveluiden asennus sekä testaaminen. Koulun vanha ympäristö oli jo tekniikaltaan vanhaa ja ei toiminut kunnolla. Tavoitteena oli luoda useita erilaisia verkkosivuja simuloimaan palveluita, joita oikeastakin internetistä löytyisi. Lopuksi testattiin luotujen palveluiden ominaisuuksia käytännön esimerkeissä. Opinnäytetyö tehtiin osana KIKKA-hanketta.

Tiedonlähteenä opinnäytetyön teoriaosuudessa käytettiin verkosta löytyvää materiaalia. Teoriaosuudessa käytiin läpi aiheeseen liittyvien standardien sekä järjestöjen lisäksi palveluiden tekniseen toteutukseen liittyviä aiheita. Ympäristöä rakennettaessa käytiin useita palavereita liittyen palveluiden sisältöön ja tekniseen toteutukseen. Päädyttiin rakentamaan palvelut osin LAMP-pinon sekä osin Dockerin avulla. Näitä kahta teknologiaa vertailtiin ympäristössä tietoturvaa ajatellen. Lisäksi palveluita varten asennettiin sertifikaattipalvelin, jotta ulkoverkosta poiskytkettyyn ympäristöön saataisiin käyttöön SSL-sertifikaatit verkkosivuille.

Työn aikana oppimisympäristöön saatiin useita helposti monistettavia verkkopalveluita, jotka sopivat hyvin osaksi ympäristössä pidettävää opetusta. Ympäristöön luodut palvelut sekä verkkorakenne yhdessä luovat hyvän simulaation organisaation sisäverkosta sekä julkiverkosta. Palveluita on helppo siirtää eri virtuaaliverkkojen välillä vaihtamalla palveluita ajavan virtuaalikoneen verkkokortti oikeaan virtuaaliverkkoon. Palveluita varten on kirjoitettu kattavasti dokumentaatiota tulevaisuuden ylläpitotoimia varten.

Opinnäytetyön kirjoitushetkellä ensimmäiset opiskelijat olivat jo päässeet tutustumaan uuteen ympäristöön. Saadun palautteen perusteella ympäristö on ollut toimiva opetuskäytössä, eikä ongelmia luotujen palvelujen kanssa ole ollut ongelmia. Opinnäytetyön aikana saatu lopputulos loi hyvän pohjan kyberturvallisuusalan koulutuksen toteutukseen sekä mahdollisuuden luoda monia eri skenaarioita ympäristön sisällä. Ympäristöön tullaan tekemään paljon jatkokehitystä tulevaisuudessa.

KAMK • University of Applied Sciences

Abstract

Author(s): Komulainen Tuomas

Title of the Publication: Setting Up Web Services in the Cyber Security Learning Environment

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: web server, internet, cybersecurity, virtualization

The subject of this thesis was the installation and testing of web services to a new cyber range being built at Kajaani University of Applied Sciences. The target was to create webpages and other services simulating those found on the real internet. Lastly, the functionality of the created services was tested using practical examples. This thesis was done as a part of the KIKKA-project.

The internet was primarily used as the source of information in the theory part of this thesis. The theory part goes through standards and organizations related to this subject and covers some of the technical aspects of this project.

Meetings were held during the development phase discussing the content and technical aspects of the web services being built. It was concluded that some of the services should be built using LAMP-stack and others using Docker. Such a solution enables students to compare the two different approaches regarding cyber security of these platforms. A certificate server was installed to enable SSL-certification to some of the webservices running inside the closed network.

During the writing of this thesis, multiple easily duplicable web services were set up. They fit perfectly as a part of the teaching in the environment. The services are easily moved to different virtual networks by configuring the network card of the virtual machines where these services are being hosted from.

Alkusanat

Tämä opinnäytetyö on tehty Kajaanin Ammattikorkeakoulu Oy:lle osana KIKKA-hanketta.

Haluan kiittää koulun henkilökuntaa ohjaamisesta opinnäytetyön aikana sekä oppimisympäristön kehittämisessä mukana olleita hyvästä yhteistyöstä.

Sisällys

Symboliluettelo

IETF: Internet Engineering Task Force, organisaatio, jonka tehtävänä on tuottaa teknistä dokumentaatiota internetin kehittäjiä varten.

ACME-verkko: Oppimisympäristön kuvitteellisen yrityksen segmentoitu sisäverkko.

CONTOSO-verkko: Oppimisympäristön kuvitteellisen yrityksen segmentoimaton sisäverkko.

Segmentointi: Verkon jakaminen pienempiin osiin organisaation sisällä.

Template: Valmis kopio virtuaalikoneesta, jota voidaan käyttää identtisten virtuaalikoneiden luontiin.

PHP: Pidemmältä nimeltään PHP: Hypertext Preprocessor, verkkosivujen kehittämiseen yleisesti käytetty skriptikieli.

MySQL: Avoimen lähdekoodin relaatiotietokantaohjelma.

VSphere: VMwaren virtualisointialusta. Alustaan lukeutuvia tuotteita ovat muun muassa ESXi-hypervisor sekä vCenter -palvelimenhallintaohjelma.

Wireshark: Avoimen lähdekoodin pakettianalysaattori. Käytetään tietoliikenteen tallentamiseen sekä analysoimiseen.

POST-pyyntö: Käytetään datan lähettämiseen palvelimille HTTP-paketeissa.

SSH: Secure Shell. Salattujen etäyhteyksien muodostamiseen käytetty protokolla.

LDAP: Lightweight Directory Access Protocol. Käyttäjätiedon palvelimelta hakemiseen tarkoitettu protokolla.

Iptables: Käytetään Linux-ytimen sisäänrakennetun Netfilter-palomuurin konfigurointiin.

1 Johdanto

Koululla on ollut tarvetta paremmalle kyberturvallisuusoppimisympäristölle. Koululla oli jo olemassa entuudestaan pienimuotoinen kyberturvallisuustehtäviä varten luotu ympäristö. Ympäristössä oli paljon erilaisia ongelmia palveluiden toiminnassa sekä laitteet itse olivat jo melko vanhaa teknologiaa. Koululta oli jäänyt rahoitusta toisesta projektista, joten projektipäällikkömme keksi hyödyntää kyseisen rahapotin uuden ympäristön kehittämiseen. Tämä opinnäytetyö on tehty osana KIKKA-hanketta.

Tavoitteena oli rakentaa ympäristö, joka tarjoaa laajat mahdollisuudet erilaisten kyberturvaan liittyvien skenaarioiden luomiseen suljetussa ympäristössä. Tärkeää oli myös mahdollisuus tuotteistaa ympäristö paikallisille yrityksille tarjottavaa koulutusta sekä muita aiheeseen liittyviä tapahtumia, kuten hackatoneja, varten.

Nyt ja tulevaisuudessa tarvitaan paljon kyberturvallisuuden osaajia, joiden kouluttamiseen tämä ympäristö on yksi vastaus. Kyberympäristön avulla koulu pystyy kouluttamaan tulevaisuuden kyberosaajia sekä pitämään koulutustilaisuuksia myös paikallisille sekä ulkopaikkakuntalaisille yrityksille.

Tehtäväni ympäristön luomisessa oli pystyttää erilaisia palveluita ympäristön eri verkkoihin. Näitä palveluita tuli olla laajasti erilaisia niin kuin julkiverkossakin on. Palveluiden tietoturvallisen tason tuli vaihdella myös, jotta voitaisiin demonstroida, miten helposti tai vaikeasti murrettavia palvelut ovat riippuen niiden tietoturvan tasosta. Osasta palveluista puuttui sertifikaatti, kun taas osassa palvelimen tietoturva ei ollut kohdillaan.

2 Internet ja WWW

Tässä kappaleessa käydään läpi järjestöjä sekä lainsäädäntöä, jotka koskevat tietoverkkoja. Näitä on monia ja ne koskevat sekä yrityksiä että kuluttajia. Käydään tässä kappaleessa läpi hieman myös TCP/IP-pinoa sekä OSI-mallia, sillä ne ovat tärkeitä tietoverkkojen ymmärtämisen kannalta.

2.1 Internet Engineering Task Force

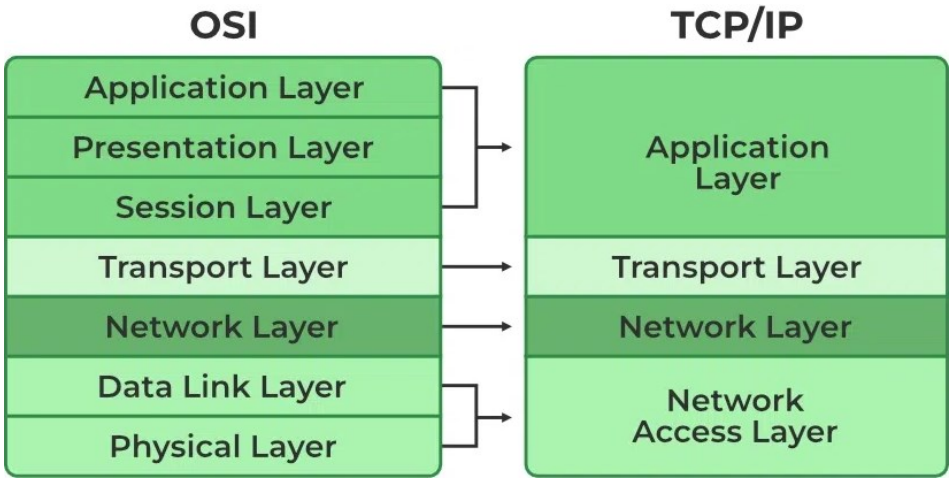
IETF eli Internet Engineering Task Force on vuonna 1986 perustettu organisaatio, jonka tehtävänä on tuottaa teknistä dokumentaatiota internetin kehittäjiä varten. IETF julkaisee RFC eli Requests for Comment -nimisiä dokumentaatioita. IETF:n dokumentaatioissa kuvataan internetin perustoiminnot, kuten osoitteistus- ja reititysteknologiat. RFC-dokumentaatiot määrittelevät myös protokollia kuten TLS ja WebRTC. Useat eri palvelut internetissä käyttävät edellä mainittuja protokollia toimiakseen. [1.]

IETF järjestää vuosittain kolme viikon mittaista, osallistujamäärältään noin 1000–1500 suuruista kokousta, joissa avustetaan työryhmiä saamaan tehtävänsä tehdyksi. Kokouksissa on myös esityksiä ja paneeleita, mutta nämä on jätetty pieneen osaan. [1.]

2.2 TCP/IP-malli

TCP/IP on tietoliikenneprotokollapino, joka koostuu useasta eri protokollasta. TCP/IP-malli on nimetty kahden yleisimmän protokollan, eli TCP:n ja IP:n mukaan. Malli määrittelee, miten ja mitä reittiä tieto kulkee verkossa laitteelta toiselle. TCP/IP koostuu neljästä kerroksesta, joita ovat sovelluskerros, kuljetuskerros, verkkokerros sekä siirtokerros. [2.] Muita malliin kuuluvia protokollia ovat muun muassa UDP, HTTP sekä TLS/SSL.

OSI-malliin verrattuna TCP/IP-malli koostuu vähemmistä kerroksista. Kuten kuvasta [Kuva 1.] havaitaan, TCP/IP-mallissa sovellus-, esitys- sekä istuntokerrokset ovat yhdessä kerroksessa. TCP/IP-mallin alin siirtokerros on OSI-mallissa jaettu kahdeksi kerrokseksi, joita ovat siirtokerros sekä fyysinen kerros.



Kuva 1. OSI- ja TCP/IP-malli [3]

2.3 World Wide Web Consortium

World Wide Web Consortium eli lyhyemmin W3C on useasta eri jäsenorganisaatiosta koostuva järjestö, jonka tehtävänä on kehittää Web-standardeja [4]. Järjestön perustaja on World Wide Webin kehittänyt Sir Tim Berners-Lee, ja hän toimii nykyisin järjestön johtajana sekä kunniajäsenenä [5].

W3C on laatinut luettelon verkkoteknologioiden standardeista, jotka sisältävät parhaat käytännöt verkkokehittäjien työhön. Näihin standardeihin lukeutuvat muun muassa HTML ja CSS. Standardit auttavat luomaan korkeatasoisia teknisiä toteutuksia verkkoon. [6.]

2.4 Tietoturvasääntely

Jokaisella verkkopalvelun tuottajalla on velvollisuus pitää tarjoamansa palvelun tietoturva ajantasalla. Näistä velvoitteista säädetään laissa ja niiden noudattamista Suomessa valvoo Kyberturvallisuuskeskus.

Sääntely velvoittaa yleisten verkkojen sekä palveluiden suunnittelussa ottamaan huomioon muun muassa sen, että sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista. Verkot on

suunniteltava niin, että ne kestävät Suomen ilmaston, sähkömagneettiset sekä muut ulkoiset häiriöt. Mahdolliset tietoturvaloukkaukset sekä uhat tulee olla havaittavissa.

Tietoturvasääntely velvoittaa myös kuluttajia. Kuluttajalla on oikeus vaatia, että teleyritysten tarjoamat verkot ovat tietoturvallisia. Samalla sääntely velvoittaa myös kuluttajaa huolehtimaan omien julkiseen verkkoon kytkettyjen laitteidensa tietoturvasta. [7.]

2.4.1 Network and Information Security Directive

NIS eli Network and Information Security Directive määrittää velvollisuuksia koskien tietojen ja verkkojen turvallisuutta. Direktiivi velvoittaa ilmoittamaan tietoturvahäiriöistä Traficomille välittömästi. NIS koskee verkkokauppoja, hakukoneita sekä pilvipalveluntarjoajia, jos yritys tai kyseisen yrityksen emoyritys työllistää yli 50 henkilöä ja liikevaihto on yli 10 miljoonaa euroa. [8.] Jos säännöstä ei noudateta, voidaan yritykselle määrätä sakkorangaistus. Jokainen jäsenvaltio määrittää sakkojen määrät erikseen.

Uusi NIS 2 -direktiivi on julkaistu vuonna 2022. Kahden vuoden siirtymäaika direktiivin käyttöönotolle päättyi 17.10.2024. Direktiivi edellyttää, että suuret palveluntarjoajat raportoivat kohtaamistaan tietoturvauhkista viranomaisille sekä varmistavat tietojärjestelmiensä tietoturvallisuuden. Yritysten on laadittava tietoturvasuunnitelma, joka täyttää kaikki NIS 2 -vaatimukset. Vaatimuksia ovat muun muassa riskianalyysi mahdollisista uhkista sekä haavoittuvuuksista, tietojärjestelmien valvonnan ja päivitysten varmistaminen sekä työntekijöiden tietoturvaan liittyvien asioiden kouluttaminen. [9.]

2.4.2 General Data Protection Regulation

General Data Protection Regulation asettaa yrityksille sekä organisaatioille vaatimuksia henkilötietojen keräämistä, säilytystä sekä hallinnointia varten. GDPR on tullut voimaan vuonna 2018, mutta se julkaistiin alun perin vuonna 2016 [10]. Kansalainen huomaa GDPR:in helpoiten verkkoa selatessa ponnahdusikkunoista, jotka pyytävät hyväksymään tietojen käsittelyn verkkosivulla. Näissä ilmoituksissa tulee ilmoittaa, kuka käsittelee, miksi, minkä takia sekä kuka vastaanottaa verkkosivulle syötettyä tietoa. [11.]

2.4.3 Kyberturvallisuuskeskus

Kyberturvallisuuskeskus on Traficomin tietoturvallisuutta valvova keskus. Kyberturvallisuuskeskuksen tehtävänä on suojella Suomen tietoverkkoa kyberuhilta sekä opastaa kansalaisia turvalliseen tietoverkkojen käyttöön. Kyberturvallisuuskeskuksen toimintaa ohjaa laki Liikenne- ja viestintävirastosta 935/2018. Kyberturvallisuuskeskus ilmoittaa verkkosivuillaan viimeisimmät rauta- sekä ohjelmistohaavoittuvuudet. Kybersää on yksi useista uutisista, joita kyberturvallisuuskeskus tuottaa. Kybersää sisältää ajankohtaiset tapahtumat kyberturvallisuuden saralla Suomessa sekä ulkomailla. Kyberturvallisuuskeskus auttaa myös kansalaisia tuottamalla koulutuksia sekä materiaalia aiheeseen liittyen.

Organisaatioiden näkökulmasta Kyberturvallisuuskeskus voi auttaa loukkauksien tapahtuessa monin tavoin. Keskus tarjoaa monia eri työkaluja sekä resursseja tietoturvaloukkauksista palautumiseen. Kyberturvallisuuskeskus tarjoaa lisäksi koulutusta sekä neuvontaa. [12.]

3 Tietoturvallinen verkkosivu

Tässä kappaleessa käyn läpi teknologioita ja periaatteita verkon palveluiden turvallisuuteen liittyen. Lisäksi kirjoitan hieman virtualisointiteknologioista, sillä verkkosivupalvelimia ei yleensä ajeta suoraan raudalla, vaan virtualisoituna.

3.1 Asiakas-palvelin-arkkitehtuuri

Yksinkertaisimmillaan asiakas-palvelin-arkkitehtuurissa asiakas pyytää palvelimelta esimerkiksi verkkosivun, jonka palvelin lähettää asiakkaalle. Asiakas voi olla esimerkiksi puhelin tai tietokone. Asiaa tarkemmin tarkasteltuna arkkitehtuuri toimii seuraavalla tavalla. Käyttäjä kirjoittaa verkkosivun URL-osoitteen selaimeen, josta pyyntö lähtee DNS-palvelimelle, joka selvittää URL-osoitetta vastaavan palvelimen IP-osoitteen. Kun IP-osoite on selvillä, selain lähettää HTTP- tai HTTPS-pyynnön kyseiseen IP-osoitteeseen. Kun palvelin on vastaanottanut pyynnön, lähettää se verkkosivun tiedostot selaimelle, joka näyttää tiedostot eli verkkosivun käyttäjälle. [13.]

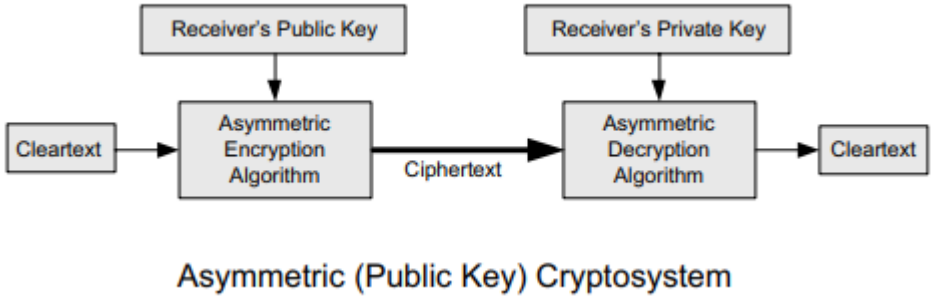
3.2 Salaus

Joissain tilanteissa voi olla tarpeellista piilottaa datan alkuperäinen sisältö ulkopuolisilta. Datan sisällön piilottamiseen auttaa salaus. Salausmenetelmiä on monia, joista tässä työssä käydään muutamia läpi. Salauksen perusperiaatteena on tiedon käsittely valitulla salaustavalla sekä salausavaimella. Salattu tieto ei ole luettavissa sellaisenaan eikä käytettyä salausmenetelmää voi päätellä tiedostosta. [14.]

Salausta varten tarvitaan avain. Avainta käytetään salauksen luomiseen sekä purkamiseen. Avaintyyppejä on monia. Salaista avainta käytetään symmetrisen salauksen purkamiseen sekä avaamiseen. Julkisen avaimen mallissa on kaksi eri avainta.

3.2.1 Epäsymmetrinen salaus

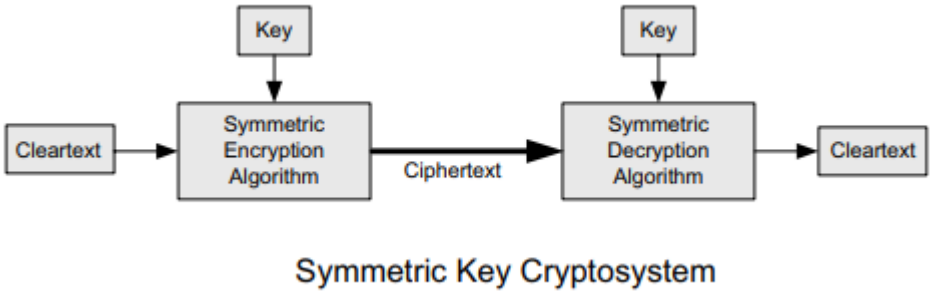
Kuten edellisessä kappaleessa mainittiin, koostuu epäsymmetrinen salaus kahdesta eri avaimesta. Epäsymmetrisessä salauksessa tiedon lähettäjällä sekä vastanottajalla on kaksi eri avainta, julkinen sekä salainen avain. Kuva 2 esittää selkeästi kahdella avaimella toimivan salauksen. Tietoa siirrettäessä data salataan vastaanottajan julkisella avaimella ja vastaanottaessaan saapuvan tiedon vastaanottaja avaa salauksen omalla salaisella avaimellaan [15].



Kuva 2. Epäsymmetrinen salaus [16, s. 810]

3.2.2 Symmetrinen salaus

Symmetrisessä salauksessa tiedon salaamiseen sekä purkuun käytetään samaa avainta. Tiedon lähettäjän sekä vastaanottajan on siis molempien tiedettävä, mitä avainta käytetään, jotta salaus saadaan purettua ja tieto luettua. Salausavaimen lähettämisessä tiedon vastaanottajalle on oltava varovainen, sillä kuka tahansa, jolla on pääsy tähän avaimeen voi lukea salatut viestit. [17.] Kuva 3 havainnollistaa symmetrisen salauksen toiminnan.

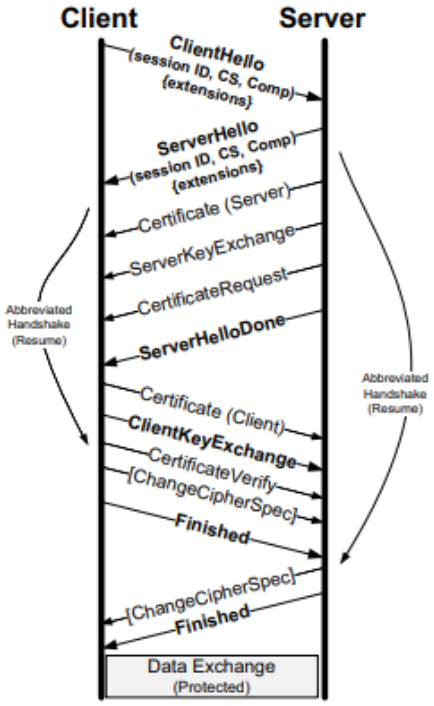


Kuva 3. Symmetrinen salaus [16, s. 810]

3.2.3 HTTP/S

Hypertext Transfer Protocol on sovellustason protokolla tiedon, kuten HTML, siirtämiseen yleisimmin selaimen ja verkkopalvelimen välillä. Oletuksena HTTP toimii portissa 80. HTTP toimii asiakas-palvelin-arkkitehtuurin mukaisesti. Asiakas lähettää palvelimelle pyynnön ja odottaa, kunnes saa siltä vastauksen. HTTP on tilaton protokolla. Palvelin ei siis säilytä istuntotietoja pyyntöjen välillä. Istuntotietojen tallentamista varten on luotu evästeet, jotta tarvittavia tietoja, kuten voidaan kirjatutumistietoja, voidaan tallentaa istuntojen välillä. [18.]

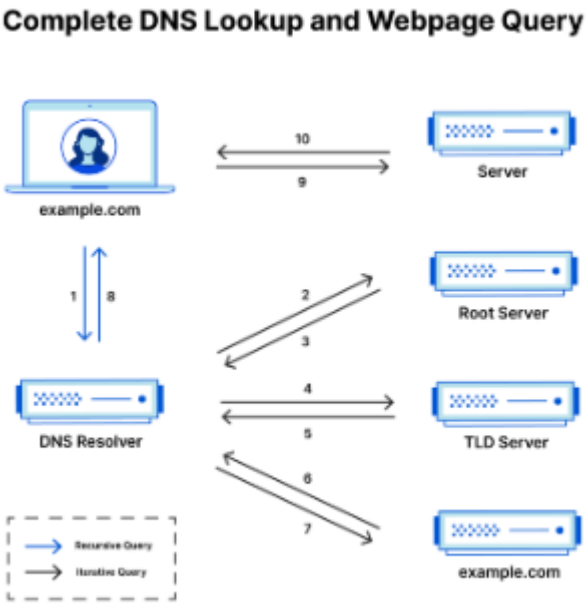
HTTPS, eli Hypertext Transfer Protocol Secure, on suojattu versio HTTP:stä ja onkin nykyajan standardi. Se toimii portissa 443. HTTPS on nykyään käytössä jokaisella verkkosivulla. HTTPS käyttää TLS eli Transport Layer Security -protokollaa. TLS on SSL:stä kehittynyt epäsymmetrinen salaustapa. Tämän protokollan avulla salataan liikenne palvelimen sekä asiakkaan välillä. Salaus on erittäin tärkeää varsinkin sivuilla, joihin syötetään käyttäjätunnuksia tai muuta sensitiivistä tietoa. Kun käyttäjä yhdistää verkkosivulle, alkaa TLS-kättely. Siinä asiakkaan laite ja verkkopalvelin keskustelevat keskenään. Ensin määritetään, mitä versiota TLS:stä käytetään. Seuraavaksi valitaan salaussarja (cipher suite), minkä jälkeen todennetaan palvelin sen TLS-sertifikaatilla. Lopuksi luodaan istuntoavaimet datan salaamiseksi yhteyden ajan. [19,20.] Kuvasta 4 nähdään kuinka asiakkaan ja palvelimen välinen keskustelu etenee.



Kuva 4. TLS-kättely [16, s. 881]

3.2.4 DNS/DNSSEC

Domain Name System muuntaa domain-osoitteen IP-osoitteeksi. DNS helpottaa verkossa selaamista, koska se poistaa tarpeen muistaa monimutkaisia IP-osoitteita. Jos halutaan vierailla esimerkiksi sanomalehti Kalevan verkkosivuilla kaleva.fi, kulkee yhteys neljän eri DNS-palvelimen kautta. Ensimmäisenä liikenne kulkee rekursiiviselle nimipalvelimelle, josta tarkistetaan, josko verkkosivun IP-osoite löytyisi sieltä. Rekursiivinen nimipalvelin on internet-palveluntarjoajan käyttämä palvelin. Jos osoitetta ei löydy, siirtyy pyyntö juuripalvelimelle. Juuripalvelin ei itsessään tiedä verkkosivun palvelimen IP-osoitetta, mutta osaa ohjata oikealle ylätason domain-palvelimelle. Ylätason domain-palvelin, toiselta nimeltään TLD-palvelin, käsittää kaleva.fi -osoitteessa .fi-osion. Viimeisenä vaiheena nimenselvityksessä on autoritäärinen nimipalvelin, josta löytyy verkkotunnus ja sitä vastaava IP-osoite. Kun osoite on selvillä, lähtee tieto takaisin rekursiiviselle nimipalvelimelle ja sieltä käyttäjän laitteelle. [21,22.] Edellä kuvatun prosessin avulla laite osaa yhdistää palvelimelle, jossa Kalevan verkkosivut ovat. Kuvasta 5 voidaan havaita sama prosessi.



Kuva 5. DNS-haku [21]

DNSSEC on turvallisempi versio DNS:stä, joka lisää kryptografisen allekirjoituksen DNS-tietueeseen. Allekirjoitus varmistaa, että pyydetty tietue tulee oikeasta paikasta, eikä tietueeseen ole hyökkääjän toimesta ujutettu väärää dataa. DNSSEC varmistaa alueiden luotettavuuden ylhäältä alaspäin. Siispä root-nimipalvelin varmistaa .fi-alueen ja .fi-alue tarkistaa siitä seuraavan. [23]

3.3 Palomuuri

Palomuuri on tärkeä osa sisäverkon suojaamista. Tässä opinnäytetyössä keskityn palomuurien osalta NGFW eli Next-Generation Firewall, suomeksi seuraavan sukupolven palomuureihin sekä WAF eli Web Application Firewall, suomeksi verkkosovelluksen palomuureihin. NGFW tarkkailee OSI-mallin verkko-, kuljetus- sekä sovelluskerrosta. Verrattuna perinteiseen palomuuriin seuraavan sukupolven palomuurit sisältävät edistyneempiä toimintoja, kuten syväpakettisuodatus, sovelluskohtainen hallinta sekä tunkeutumisen estojärjestelmä. Tavallinen palomuuri taasen tekee pääasiassa perusmuotoista paketinsuodatusta, jossa se katsoo paketin otsikon sekä mihin IP-osoitteeseen ja porttiin se on menossa. NGFW tarjoaa kattavampaa pakettien tarkistusta katsomalla koko paketin sisällön. Seuraavan sukupolven palomuurit sisältävät tunkeutumisen estojärjestelmän (IDS), joka osaa aktiivisesti estää tulevat yhteydet haitallisilta tahoilta. [24.]

Verkon palveluiden näkökulmasta palomuuri auttaa tietoturvassa monella tavalla. Yhteyksiin voidaan asettaa maarajoituksia, jotta sivulle voidaan yhdistää esimerkiksi vain Euroopan alueelta tai vaikkapa niin, että sivusto on nähtävissä vain Suomessa. Yhteyksien määrää voidaan rajoittaa, jotta palvelunestohyökkäykset tai muut suuret piikit kävijämäärässä eivät kaada verkkosivua.

Web Application Firewall (lyhyemmin WAF) tuo hyvän lisän OSI-mallin sovelluskerroksen suojaukseen. Se valvoo sovelluskerroksen liikennettä ja sääntöjen perusteella osaa esimerkiksi hyväksyä tai hylätä yhteyspyyntöjä IP-osoitteen tai HTTP-otsikon (header) perustella. WAF torjuu monia OWASP:in listaamia hyökkäyksiä, kuten cross-site script ja SQL-injektiot. [25,26.]

3.4 Virtualisointi

Tässä kappaleessa käsittelen virtualisointialustoja. Virtualisointi mahdollistaa useamman virtuaalisen tietokoneen ajamisen yhden fyysisen tietokoneen jakamilla resursseilla. Säästetään siis tilan tarpeessa sekä sähkö- ja jäähdytyskustannuksissa, koska ei tarvita useampaa fyysistä palvelinta vain tiettyä käyttöä varten.

Luomassamme oppimisympäristössä virtualisointi on tärkeässä roolissa, sillä kaikkia ympäristön verkkoon luotuja palveluja ajetaan virtuaalikoneilla sekä konteissa. Opinnäytetyön kannalta virtualisointi ei ole pääaiheena, mutta siitä on kumminkin hyvä käydä perusasioita läpi. Seuraavissa kappaleissa käyn läpi aluksi hypervisoreita sekä lopuksi konttiteknologioista Dockerin.

3.4.1 Hypervisorit

Hypervisor on ohjelma, jonka tehtävänä on luoda ja ajaa virtuaalikoneita. Hypervisorit voidaan jakaa tyypin 1 sekä tyypin 2 hypervisoreiksi riippuen, millä tasolla ne toimivat. Tyypin 1 hypervisor toimii suoraan palvelimen raudalla, kun taas tyypin 2 hypervisor toimii käyttöjärjestelmän, kuten Windows, päällä niin kuin mikä tahansa asennettava ohjelma. [27.]

Esimerkkeinä tyypin 1 hypervisoreista voidaan mainita VMwaren ESXi sekä Microsoftin Hyper-V. Tyypin 2 hypervisoreita ovat Oraclen VirtualBox sekä VMwaren VMware Workstation. [28.] Luomassamme oppimisympäristössä on käytössä VMwaren vSphere -virtualisointialusta, johon sisältyy ESXi-hypervisor sekä selaimella käytettävä keskitetty hallintaohjelmisto vCenter.

3.4.2 Docker

Docker on alusta, joka mahdollistaa palvelun nopean luonnin, ylösajon, muokkaamisen sekä poistamisen. Jokainen sovellus on omassa kontissaan, joka voidaan lyhyellä komentokehotteessa kirjoitettavalla komennolla käynnistää sekä sammuttaa. Docker toimii palvelimen käyttöjärjestelmän päällä virtualisoiden käyttöjärjestelmää, jonka päällä sovelluksia ajetaan. [29.]

Jotta palvelun saa ajettua ylös, yksinkertaisimmillaan tarvitsee vain tietää halutun palvelun imagen nimi. Docker-image on valmis kontti, joka sisältää esimerkiksi Apache-verkkopalvelimen valmiiksi asennettuna konttiin. On tärkeää ladata imaget valmistajien omilta verkkosivuilta. Näin varmistutaan imagen sisällöstä.

4 Verkkosivun tietoturvallinen käyttöönotto

Tässä kappaleessa käsittelen opinnäytetyöni käytännön osuutta. Tehtäväni projektissa oli asentaa palveluita ympäristön eri verkkoihin simuloimaan verkkokauppoja sekä muita erilaisia verkkopalveluita joita internetistä löytyy. Asensin verkkokaupan, kirjautumissivuston sekä epäilyttävän verkkosivuston kyseenalaisilla mainoksilla varustettuna. Lopuksi vahvensin joidenkin palveluiden tietoturvaa siten, että hyökkäyspinta-alaa olisi mahdollisimman vähän. Kirjautumisverkkosivun jätin tarkoituksella haavoittuvaiseksi, jotta opetuksessa voitaisiin demonstroida tätä.

4.1 KAMK Cyber Range

Kuten tämän opinnäytetyön alussa mainittiin, oli koulun olemassa oleva ympäristö päivityksen tarpeessa. Kun budjettia ympäristön päivitykseen löytyi, alkoi hankkeen toteutus. Virtualisointiympäristö koostuu kahdesta Dell-palvelimesta, joissa on kummassakin puoli teratavua muistia sekä 24 ydintä. Tallennustilaa ympäristössä on yhteensä kymmenen teratavua, joka on peilattu levyjen vikaantumisen varalta. Levypalvelimeksi valittiin Dell PowerStore 500T, koska samaa mallia käytetään koululla muuallakin.

Kyberympäristöön pääsee kolmesta luokkahuoneesta, joissa kytkimet ovat lukituissa kaapeissaan. Verkko on jaettu useampaan eri virtuaaliverkkoon. Verkon osia ovat Hallinta-, Palvelut-, ACME- sekä CONTOSO-verkko. Hallinta-verkko sisältää ESXi- sekä levypalvelimet. Palvelut-verkossa on muun muassa vCenterin käyttöliittymä sekä kuvitteellisen julkiverkon palvelut. ACME- sekä CONTOSO-verkot ovat kuvitteellisten yritysten sisäverkkoja. ACME-verkko on segmentoitu itsessään useampaan eri VLAN:iin, kun taas CONTOSO sisältää kaiken samassa IP-avaruudessa. Verkon jakamisella osiin voidaan simuloida hyvää sekä huonoa sisäverkon suunnittelua.

4.2 Webserver-virtuaalikone

Asensin Palvelut-verkkoon kaksi eri virtuaalikonetta, joista ensimmäisessä verkkopalvelut on asennettu Apache-verkkopalvelinta ajavalle virtuaalikoneelle ja toiseen konttien avulla. Apachea ajavan virtuaalikoneen nimeksi annoin Webserver. Asensin käyttöjärjestelmän vCenterin selaimeen aukeavan konsolin avulla. Kun käyttöjärjestelmä oli asennettu, otin virtuaalikoneelle SSH-

etäyhteyden Windowsin komentokehotteen avulla. SSH-yhteys tarjoaa tietoturvallisen tavan luoda etäyhteys koneelta toiselle.

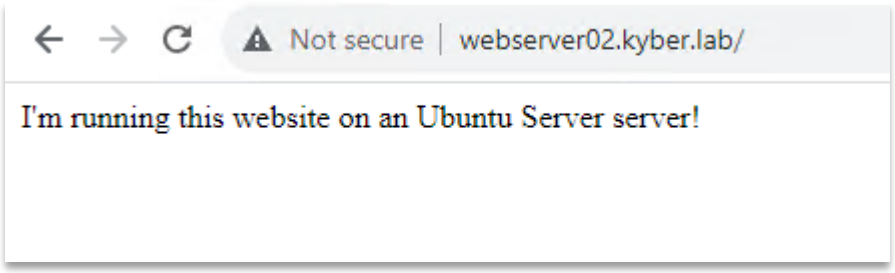
Aloitin verkkosivupalvelimen asennuksen luomalla virtuaalikoneen ympäristömme vCenter-virtualisointialustalle. Käyttöjärjestelmäksi valikoitui Ubuntu Server 20.04.6, josta teimme ympäristöön valmiin mallin eli englanniksi templaten. Loin uuden virtuaalikoneen mallista ja käynnistin virtuaalikoneen. Kun virtuaalikone oli käynnistetty, ensimmäinen tehtävä oli asettaa tietokoneelle staattinen IP-osoite. Osoitteen konfiguroimisessa auttoi mallin mukana tullut skripti, johon syötin IP-osoitelistasta vapaan osoitteen.

Jotta palvelimella voidaan näyttää verkkosivuja, tarvitaan verkkosivupalvelin. Valitsin palvelinohjelmistoksi Apachen. Apache on Apache Software Foundationin ylläpitämä projekti [30]. Asensin Apachen kirjoittamalla komentokehotteeseen sudo apt install apache2.

Kun Apache oli asennettu, loin palvelimen /var/www-hakemistoon kansiot jokaiselle verkkosivulle. Apache-palvelimelle oli tarkoitus asentaa kolme eri verkkosivua, joten tein kolme kansiota [31]. Yhdellä verkkosivuista on kirjautumis- sekä rekisteröitymislomake, joten tämä tarvitsee tietokannan asentamisen palvelimelle. Asensin tarvittavat lisäosat sekä muita tarvittavia moduuleja PHP:n ja MySQL:n käyttöön Apachen kanssa.

Kirjautumissivun tiedostot ovat .php-päätteisiä. Jotta oikeat tiedostot avautuvat, tarvitsi minun muokata Apachen apache2.conf-konfiguraatiotiedostosta AllowOverride-asetus muotoon ’All’ sekä lisätä .htaccess-konfiguraatiotiedosto verkkosivun tiedostojen kanssa samaan kansioon. Konfiguraatiotiedoston avulla Apache osaa käyttää oikeaa tiedostoa selaimessa. Kirjoitin .htaccess-tiedostoon DirectoryIndex login.php.

Jokaiselle verkkosivulle täytyy luoda oma VirtualHost-konfiguraatiotiedostonsa, jotta Apache osaa ohjata vierailijan oikealle verkkosivulle. Nämä konfiguraatiotiedostot sijaitsevat polussa /etc/apache2/sites-available/. Tiedostoon kirjoitetaan muun muassa, mitä porttia verkkosivu kuuntelee, missä polussa sivun tiedostot sijaitsevat, mitä domain-osoitetta sivusto kuuntelee sekä missä SSL-sertifikaattiavaimet sijaitsevat. Määritin sivuille alidomaineiksi webserver01, webserver02 ja kyberjynggy. Kun sain tehtyä jokaiselle verkkosivulle oman konfiguraatiotiedoston, kirjoitin komennon sudo a2ensite webserver02.conf. [32.] Käynnistin Apachen vielä uudelleen ja tämän jälkeen menin selaimella kuvassa 6 näkyvään osoitteeseen. Verkkosivu voitiin siis todeta toimivaksi.



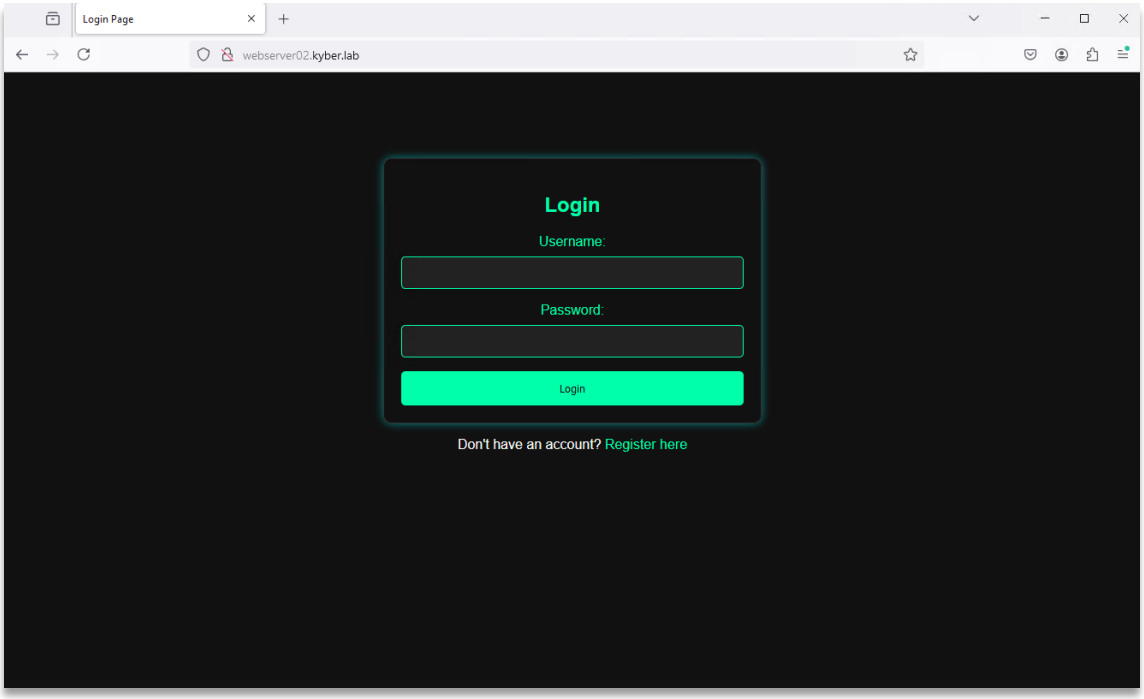
Kuva 6. Verkkosivu pystytetty

Kun perustoiminnot olivat valmiina, rupesin kirjoittamaan verkkosivuja. Koska yhdelle sivuista voidaan kirjautua, eli syöttää dataa ja saada datan perusteella vastaus, täytyi minun asentaa tietokantapalvelin ja yhdistää se verkkosivulle. Loin tietokantapalvelimeen tietokannan ja siihen taulukon, johon tuli viisi kenttää kuten alla olevassa kuvassa 7 näkyy.

```
mysql> show columns from users;
+-----------------+-------------+------+-----+---------+----------------+
| Field           | Type        | Null | Key | Default | Extra          |
+-----------------+-------------+------+-----+---------+----------------+
| id              | int         | NO   | PRI | NULL    | auto_increment |
| username        | varchar(50) | NO   |     | NULL    |                |
| email           | varchar(50) | NO   |     | NULL    |                |
| password        | varchar(50) | NO   |     | NULL    |                |
| create_datetime | datetime    | NO   |     | NULL    |                |
+-----------------+-------------+------+-----+---------+----------------+
5 rows in set (0.01 sec)
```

Kuva 7. Kirjautumisverkkosivun tietokanta

Kirjoitin verkkosivut käsin käyttäen tekoälyä ongelmien ratkaisussa sekä ulkoasua miettiessä. Eniten ongelmia tuli tietokannan yhdistämisessä verkkosivulle. Yksi helposti ratkaistu ongelma oli HTTP error 500. Ongelman sai korjattua asentamalla php-mysql-laajennuksen. PHP ei siis saanut yhteyttä tietokantaan. Kuvasta 8 nähdään valmis sivu. Kuvankaappauksessa on avattu sivu ilman sertifikaattia, mutta se toimii myös sen kanssa.



Kuva 8. Kirjautumisverkkosivu valmis

Kirjautumissivua luodessa konfiguroin sivun VirtualHost-tiedoston niin, että portit 80 sekä 443 ovat molemmat auki. Edellä mainittujen porttien avulla sivustolle pääsee siis salauksen kanssa (HTTPS) sekä ilman (HTTP). Sivuston kahta eri versiota voidaan hyödyntää ympäristössä tehtävillä testeillä. Esimerkiksi Wiresharkilla voidaan kuunnella sivustolle kirjautumista ja havaita, että ilman salausta asiakkaan kirjoittamat käyttäjätunnukset kulkevat selkokielisenä asiakkaan ja palvelimen välillä.

Ennen salattua sivua on voinut pitää luotettavana. Nykyään tosin kuka tahansa pystyy helposti asentamaan verkkosivun sertifikaatteineen sekä kopioimaan jonkin tunnetun verkkosivun ulkoasun käyttämällä esimerkiksi selainten inspect element -ominaisuutta. Siispä pelkästään verkkosivun salaus ei enää ole tae sivuston luotettavuudesta tai aitoudesta.

Apachella toimivan verkkosivun turvallisuutta voidaan vahventaa myös muilla keinoilla. Palvelimen käyttäjäoikeuksien kiristäminen sekä päivityksien ajan tasalla pitäminen ovat hyviä ideoita. Ulkoverkkoon näkyvä palvelin on hyvä segmentoida omaan verkkoonsa (DMZ) ja palomuurisäännöillä rajata, mitä liikennettä, jos mitään, päästetään paljastetulle palvelimelle. Jos verkkosivu käyttää tietokantaa, kannattaa se asentaa omalle palvelimelleen sisäverkkoon ja palomuurisäännöillä sallia vain MySQL:n tarvitsema portti 3306 verkkosivupalvelimelta tietokantapalvelimelle. [33]

4.3 Docker-kone

Tätä opinnäytetyötä varten on hyvä vertailla erilaisia ratkaisuja palveluiden pystyttämiseen verkkoon. Docker on siitä kätevä, että sen itsensä asennuksen jälkeen varsinaisten palveluiden pystyttäminen on todella helppoa ja nopeaa. Siispä vertailen kahta edellä mainittua Apachen ja Dockerin avulla luotua ratkaisua toisiinsa.

Asensin Dockeria varten oman virtuaalikoneen. Virtuaalikoneen käyttöjärjestelmäksi asensin Ubuntu Server 20.04.6. Kuten edellisenkin virtuaalikoneen kohdalla, käyttöjärjestelmän asensin vCenterin Web Consolen avulla ja loput asennukset tein SSH-yhteydellä. Niin kuin kuvasta 9 voidaan havaita, asensin virtuaalikoneelle Dockerin uusimman version.

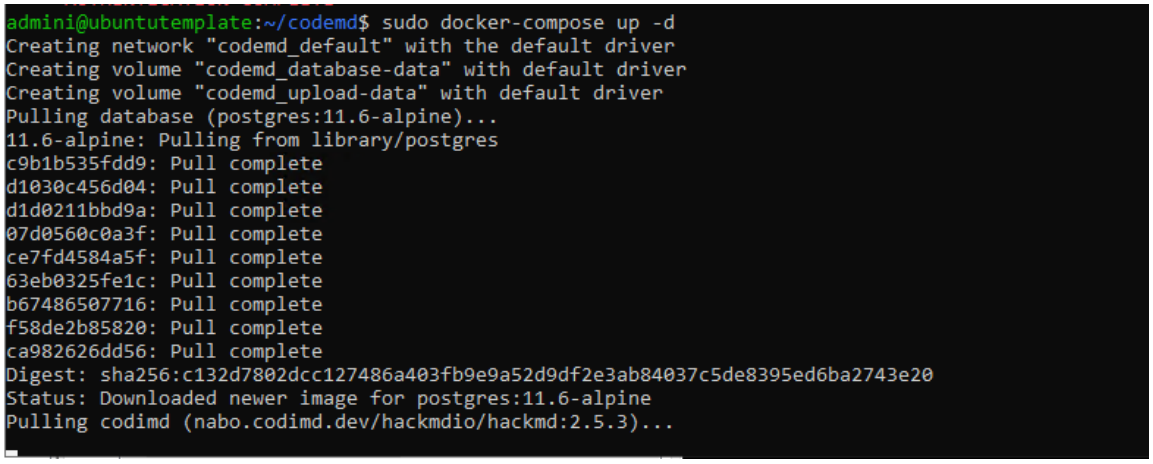
```
admini@ubuntutemplate:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-
plugin
[sudo] password for admini:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  docker-ce-rootless-extras pigz slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-buildx-plugin docker-ce docker-ce-cli docker-ce-rootless-extras docker-compose-plugin pigz
  slirp4netns
0 upgraded, 8 newly installed, 0 to remove and 95 not upgraded.
Need to get 117 MB of archives.
After this operation, 420 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://download.docker.com/linux/ubuntu focal/stable amd64 containerd.io amd64 1.6.28-1 [29.6 MB]
Get:2 http://archive.ubuntu.com/ubuntu focal/universe amd64 pigz amd64 2.4-1 [57.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/universe amd64 slirp4netns amd64 0.4.3-1 [74.3 kB]
Get:4 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-buildx-plugin amd64 0.12.1-1~ubuntu.20.04~focal
 [28.2 MB]
Get:5 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce-cli amd64 5:25.0.3-1~ubuntu.20.04~focal [13.
7 MB]
Get:6 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce amd64 5:25.0.3-1~ubuntu.20.04~focal [24.3 MB
```

Kuva 9. Dockerin asennus

Kun Dockerin asennus oli valmis, siirryin asentamaan kontteja. Asensin konttiin PrestaShop-verkkokaupan, CodiMD-markdown alustan sekä linkit jokaiseen palveluun selaimessa näyttävän Heimdallin. Kuten oheisesta kuvasta 10 nähdään, tarvitsevat CodiMD sekä PrestaShop kaksi erillistä konttia. Verkkosivupalvelin sekä tietokanta ovat omissa konteissaan ja keskustelevat keskenään omassa Docker-verkossaan.

Kuva 10. Docker-palvelimen kontit

Kuvasta 9 voidaan havaita, että asensin myös Docker Compose -lisäosan. Compose helpottaa konfigurointia varsinkin useamman kontin yhdistelmissä. Yhdellä YAML-tiedostolla määritetään mitä konttikuvia käytetään, mahdolliset määrittelyt niihin sekä mitä verkkoa käytetään. PrestaShopin Compose-tiedosto esimerkiksi sisältää asetukset verkkosivun sekä tietokannan kontteja varten, sekä millä verkolla nämä kontit yhdistetään toisiinsa. Myös myöhempi muutosten tekeminen on helppoa yhtä tiedostoa muokkaamalla. Seuraava kuva 11 havainnollistaa, kuinka Docker aloittaa määritettyjen asetusten perusteella luomaan konttia.



Kuva 11. Docker Composen avulla asennettu CodiMD

Docker-kontin turvaamiseen on monia tapoja. Kuten edellä on mainittu, kannattaa ladata imaget luotetuista lähteistä. Docker sekä isäntäkone kannattaa päivittää sekä tarkistaa päivitykset aika-ajoin. Crontabilla voidaan esimerkiksi ajoittaa viimeisimpien päivitysten lataus esimerkiksi viikoittain tai joka kuukauden alussa. Ajoituksia tehdessä kannattaa toki pitää mielessä, että päivitykset saattavat rikkoa joitain toimintoja, joten automaattinen päivitysten asennus ei välttämättä ole kannattavaa. Kuukausittainen tai viikoittainen huoltotauko on siis paikallaan. Myös lokien seuraaminen on kannattavaa. Nähdään helposti, jos jotain epäilyttävää tapahtuu kontissa.

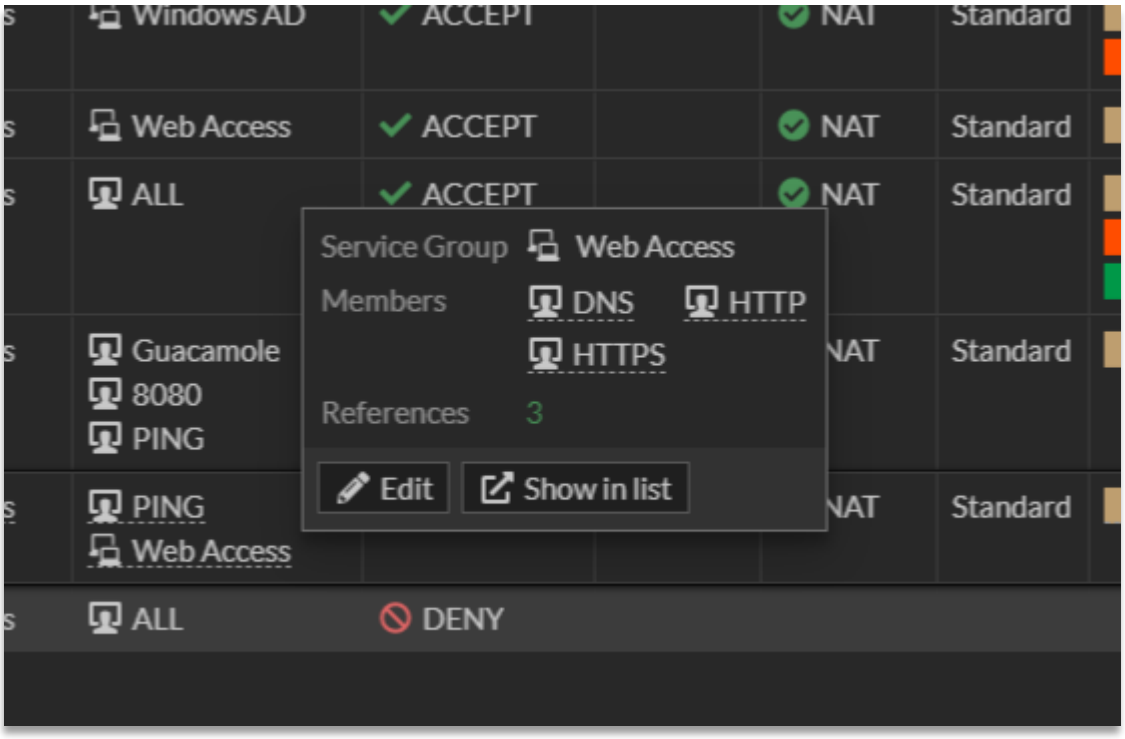
Kannattaa harkita konttien tiedostojärjestelmän muuttamista vain luku -tilaan tai ylipäänsä rajoittamaan käyttöoikeuksia. Kontin saa vain luku -tilaan lisäämällä komennon ”-read-only” Docker run -komentoon. Kontin toimiessa vain luku -tilassa mahdolliset haittaohjelmat eivät pääse helposti leviämään tai muokkaamaan tiedostoja. [34.]

Kontin hyötynä tietoturvaa ajatellen on sen eristys isäntäkäyttöjärjestelmästä. Jos hyökkääjä pääsee käsiksi verkkosivun tiedostoihin, hänellä ei ole suoraa pääsyä kontista ulos isäntäpalvelimeen. Eristys isäntäkäyttöjärjestelmästä voidaan siis luetella eduksi verratessa kontteja perinteisempään verkkosivupalvelimeen.

Docker kiertää Debianin ja Ubuntun mukana tulevan UFW (Uncomplicated Firewall) -palomuurin konfiguraatiotyökalun. Sekä Docker että UFW muokkaavat iptables-sääntöjä, mutta eri tavalla. Docker reitittää konttien liikenteen käyttäen NAT-taulua, kun taas UFW käyttää FILTER-taulun INPUT- sekä OUTPUT-ketjuja. [35.] Dockerin liikenne siis ohittaa kaikki säännöt, joita UFW on luonut. Dockerin vaikutus iptablesiin on hyvä ottaa huomioon isäntäkoneen palomuurisääntöjä tehdessä.

4.4 Palomuurin säännöt

Ympäristön palomuuriin ei ole luotu tarkempia sääntöjä koskien palveluita. Ainoat säännöt palveluihin liittyen koskevat eri verkkoja sekä mistä verkosta pääsee Palvelut-verkkoon, jossa palveluita on. Jos kumminkin tekisin tarkempia sääntöjä verkkosivupalvelinta koskien, tekisin sen näin. Palomuuriin sääntöjä luodessa katsoisin, että vain tarvittavat protokollat on listattu. Seuraavassa kuvassa 12 nähdään, kuinka esimerkissä kirjautumisverkkosivulle tulevat protokollat on rajattu PING-, DNS-, HTTP- sekä HTTPS-liikenteeseen.

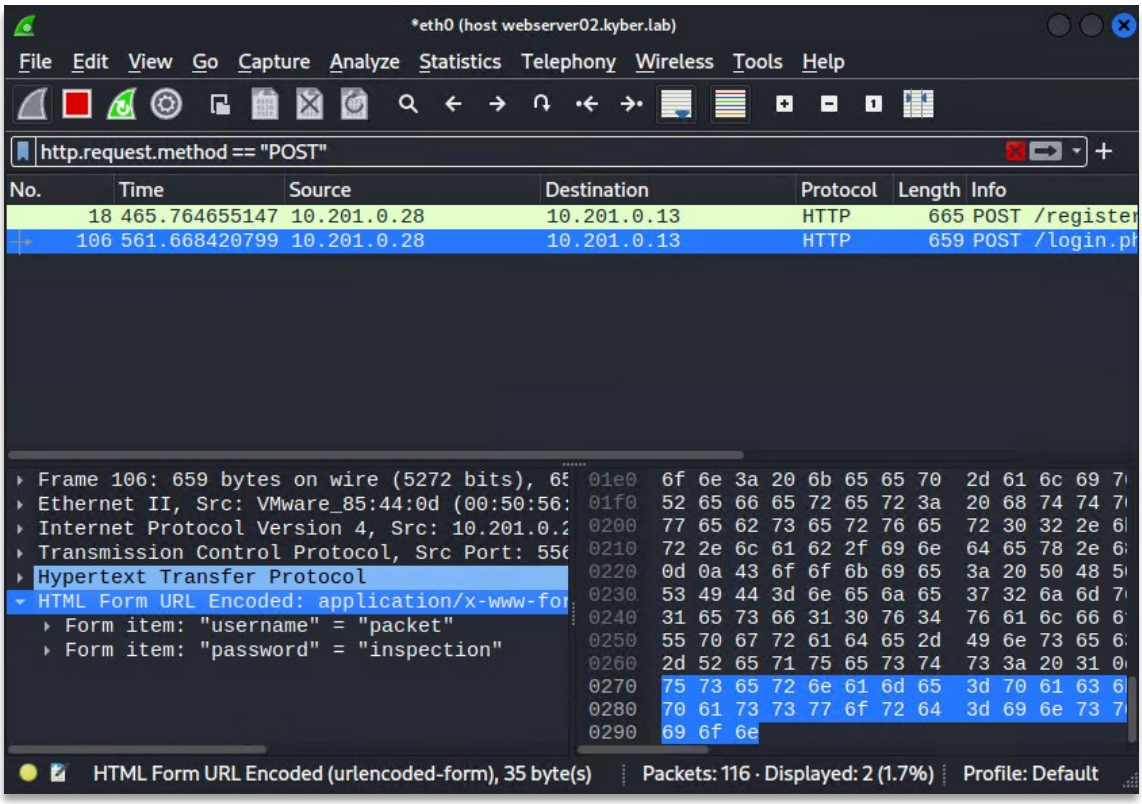


Kuva 12. Verkkosivupalvelimen sääntö FortiGate-palomuurissa

Edellä mainitulla tavalla rajataan, mitä liikennettä päästetään palvelimelle. Tuotantoympäristössä ei tosin päästettäisi HTTP-liikennettä sisälle.

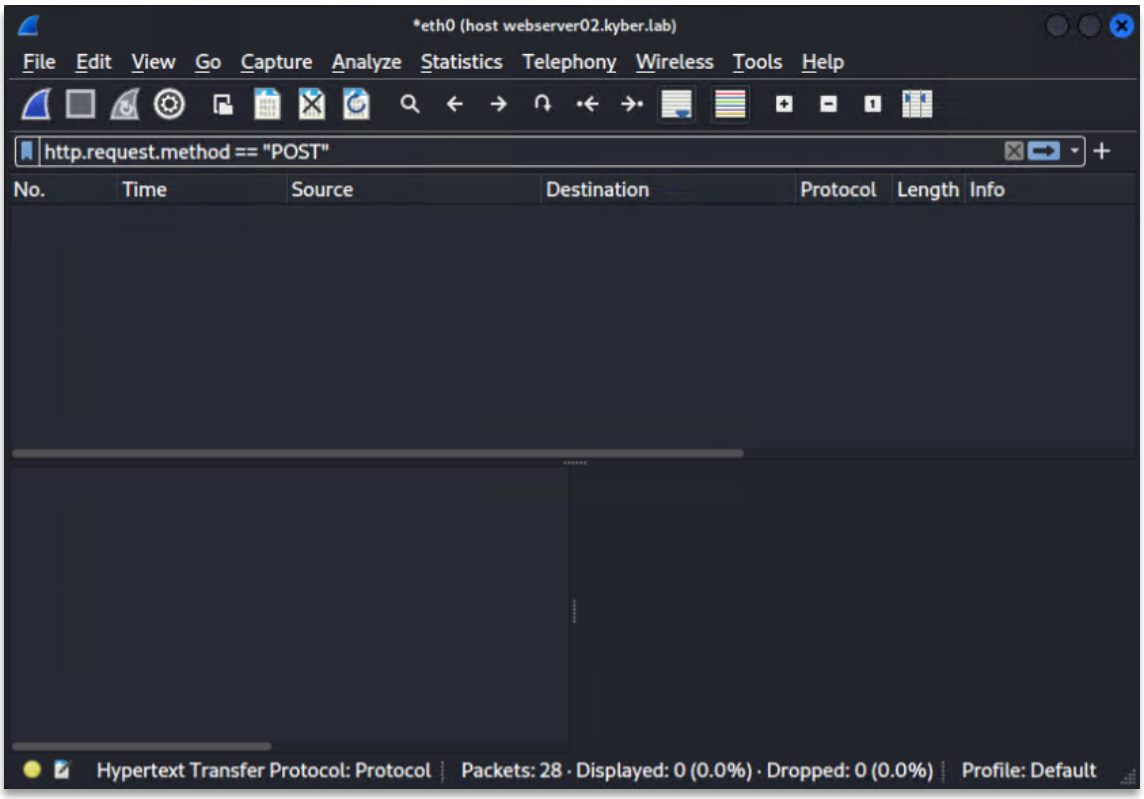
4.5 Testaaminen

Kun ympäristöön on toteutettu palveluita, on niitä aika kokeilla. Käytin kirjautumissivua pakettien tarkastelemiseen. Testaamisessa käytin Kali Linux -virtuaalikonetta. Aluksi kirjauduin sivun HTTP-versiolle, kuunnellen samalla liikennettä Wiresharkilla. Kuten alla olevasta kuvasta 13 nähdään, on Wireshark tallentanut liikennettä ja samalla saanut selville, millä käyttäjätunnuksella sekä salasanalla kirjauduin verkkosivulle. Käyttäjätunnuksena oli ”packet” sekä salasanana ”inspection”. Wireshark oli tallentanut muutakin liikennettä, mutta jotta saatiin suodatettua halutut paketit, joissa palvelimelle lähetetty data on, lisäsin suodattimeksi http.request.method == ”POST”. Lisäämäni suodatin näyttää vain POST-pyyntöihin liittyvät paketit. Edellä mainitut paketit liittyvät verkkosivujen lomakkeiden täyttämiseen sekä tiedostojen lataamiseen palvelimelle [36].



Kuva 13. Wireshark on tallentanut paketteja

Seuraavaksi kokeilin, mitä Wireshark saa tallennettua, kun kirjaudun luomalleni sivulle HTTPS-protokollaa käyttäen. Huomasin, että kirjoittamaani käyttäjätunnus-salasana-yhdistelmää ei näkynyt Wiresharkin tallennuksessa. Seuraava kuva 14 näyttää, kuinka rajaamalla vain POST-pyyntöihin ei tuo tuloksia. Tekemäni koe siis havainnollistaa salauksen tärkeyden varsinkin sivuilla, jonne käyttäjä itse antaa tietoa.



Kuva 14. Ei POST-pyyntöjä

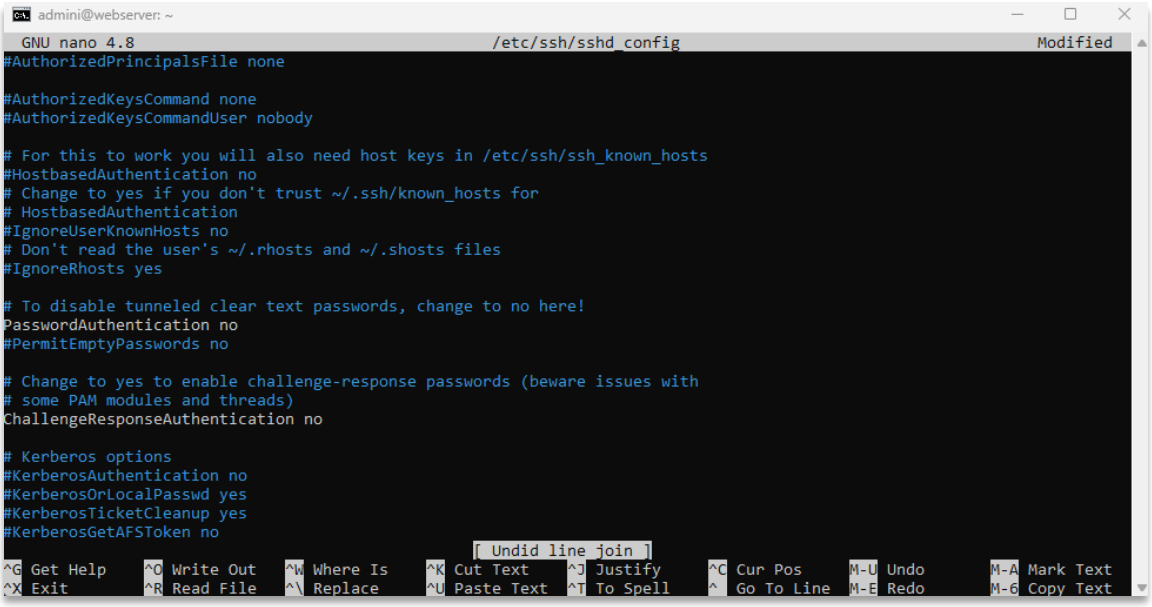
Virtuaalikoneella ajettavaa verkkosivupalvelinta voidaan konfiguroida ottamalla yhteys virtualisointialustan kautta. Tämä tosin vaatii ensin kirjautumista kyseiseen alustaan, joten se on turhan monimutkainen tapa. Suoraviivaisempaa on ottaa yhteys suoraan verkkosivupalvelimeen SSH:n avulla. SSH-yhteys kannattaa ottaa käyttöön niin, että vain SSH-avaimella päästään palvelimelle eikä salasanalla kirjautuminen ole käytössä. Avainta käyttämällä ehkäistään luvattomien yhteyksien muodostaminen, jos salasana on päätynyt vääriin käsiin. Otin verkkosivupalvelimelle SSH-avaimen käyttöön sekä kokeilin ottaa SSH-yhteyden kahdella eri koneella.

Aloitin luomalla SSH-avaimen paikallisella tietokoneella. Kuten seuraavasta kuvasta 15 voidaan nähdä, loin paikallisella Windows-tietokoneella avainparin. Avainpari tallentui käyttäjätunnukseni piilotettuun .ssh-kansioon. Avainparin julkinen avain siirrettiin seuraavaksi verkkosivupalvelimelle. Siirsin julkisen avaimen virtuaalikoneelle PowerShell-komennon avulla [37].

```
C:\Users\tuomas>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\tuomas/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\tuomas/.ssh/id_rsa
Your public key has been saved in C:\Users\tuomas/.ssh/id_rsa.pub
The key fingerprint is:
```

Kuva 15. Avainparin luonti Windowsissa

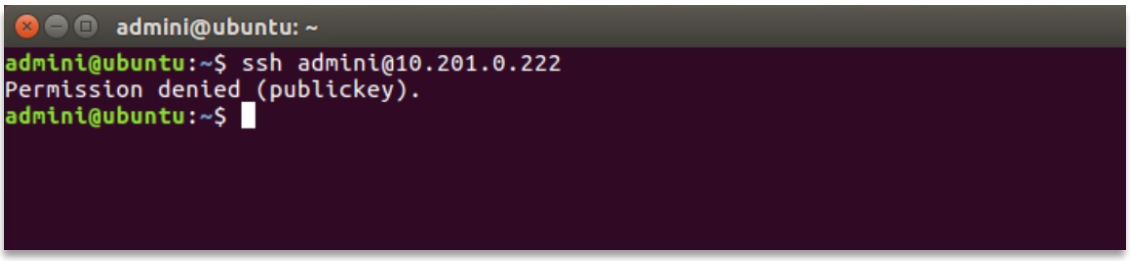
Kun avain oli siirretty verkkosivupalvelimella olevan käyttäjätunnuksen .ssh-kansion authorized_keys-tiedostoon, aloitin konfiguroimaan SSH-palvelinta avaimen käyttöön. Sshd_config-tiedosto näyttää komentoituna kaikki oletusasetukset. Siispä minun täytyi muokata alkuperäinen ’PasswordAuthentication yes’ -asetus muotoon ’PasswordAuthentication no’, sekä ottaa kommentointi pois käytöstä. Kuva 16 näyttää, miltä asetustiedosto näytti muutosten jälkeen. [38.]



Kuva 16. Sshd-konfiguraatiotiedosto

Aluksi muutos ei estänyt salasanan käyttöä kirjautumiseen, mutta huomasin, että polun /etc/ssh/sshd_config.d 50-cloud-init.conf -tiedosto yliajoi sshd_config-tiedostossa määritetyt asetukset. Tein siis tarvittavat muutokset edellä mainittuun tiedostoon.

Varmistin muutosteni toimivuuden ensiksi kirjautumalla paikallisella koneellani verkkosivupalvelimelle. Pääsin kirjautumaan palvelimelle ilman tarvetta syöttää salasanaa. Seuraavaksi kokeilin kirjautua toiselta koneelta, jolla ei ole tarvittavaa avainta. Seuraava kuva 17 näyttää, kuinka komentokehote palauttaa Permission denied (publickey) estäen pääsyn palvelimelle.



Kuva 17. Pääsy evätty

5 Yhteenveto

Ympäristöön on luotu useita palveluita, joita voidaan hyödyntää kursseilla erilaisissa tehtävissä. Tämä palvelujen sekä verkkojen kokonaisuus tarjoaa mahdollisuuden luoda monia erilaisia skenaarioita. Osissa palveluista on sertifikaatti, kun taas osasta se on jätetty pois harjoitteita varten. Tärkeimpiin palveluihin, kuten palomuurin, levypalvelimen, ePDU sekä virtualisointiympäristön hallintapaneeleihin on lisätty sertifikaatti myös.

Palveluiden luominen onnistui hyvin. Verkkosivujen luomiseen auttoi internetin laaja valikoima ohjeita sekä tekoäly antoi hyviä vinkkejä, jos hakusanoilla ei meinannut löytyä. Valmiiden palveluiden, kuten GitLabin asennuksessa valmistajan oma dokumentaatio oli arvokasta apua esimerkiksi LDAP-kirjautumisen käyttöönotossa.

Haasteita projektiin toi sertifikaattien käyttöönotto. Prosessin ymmärtämisessä meni oma aikansa sekä toimivien ohjeiden löytäminen oli hankalaa. Lopulta kumminkin saatiin sertifikaatit toimimaan sekä ymmärrystä asiasta. Asensinkin omaan kotilabraanikin ADCS-sertifikaattipalvelimen sekä sertifikaatit omiin TrueNAS- sekä ProxMox-hallintapaneeleihini. On siis tullut hyödynnettyä opittuja taitoja projektin ulkopuolellakin.

Kehitettävääkin ympäristössä on paljon. Verkkosivuille voisi kehittää enemmänkin sisältöä sekä kehittää palveluiden teknistä toteutusta. Esimerkkinä tästä voitaisiin mainita tarkkojen palomuurisääntöjen lisääminen, kuten vain tietyiltä ACME-ympäristön koneilta pääsy tietylle verkkosivulle.

Opinnäytetyötä kirjoittaessa ovat jo ensimmäiset opiskelijat käyttäneet ympäristöä. Opettajalta kuultuna ympäristö toimi hyvin sekä luomani palvelut eivät tuottaneet ongelmia. Ainoa vastoinkäyminen kuuleman mukaan oli ympäristön Kali-Linux-koneiden kaatumiset, mutta tämä ratkaistiin lisäämällä virtuaalikoneisiin lisää suoritinytimiä sekä muistia.

6 Pohdinta

Mielestäni tämän ympäristön rakennusprojekti on sujunut hyvin. Kaikki tavoitteet on saatu täytettyä. Olen saanut projektin aikana todella paljon käytännön kokemusta tietoverkkojen suunnittelusta ja käyttöönotosta. Sertifikaattien käyttöönotto, kuten edellisessä kappaleessa mainittiinkin, oli aluksi hankalaa mutta tehdessä oppii.

Palomuuria olisi voinut hyödyntää enemmänkin palveluita koskien. Nykyiset palomuurisäännöt koskevat yleisesti liikennettä eri verkkojen välillä. Palomuurin Web Application Firewall -ominaisuutta olisi voinut hyödyntää, mutta tämä jääköön tulevaisuudessa toteutettavaksi.

Aiheena palveluiden luominen verkkoon on todella mielenkiintoista ja siksi valitsinkin tämän opinnäytetyöni aiheeksi. Pidän luovasta työstä ja sivuja suunnitellessa kädenjälki näkyy hyvin. Verkkosivujen suunnittelu voisi ehkä olla jotain, mitä tulisi tehtyä myöhemminkin.

Aika on kulunut nopeasti ympäristöä kehitellessä. Ympäristön kehittäminen aloitettiin vuoden 2023 elokuussa ja meni noin vuosi, että saimme ympäristön siihen pisteeseen, missä se on nyt. Alun perin ympäristön valmistuminen oli suunniteltu saman vuoden loppuun, mutta projektin skaala oli niin iso sekä tarvittavien tavaroiden saapuminen pidensivät aikataulua.

Projektin loppuvaiheilla teimme Hands-on-tyyppisiä tehtäviä opiskelijoille ympäristöön tutustumista varten. Tehtäviä saimme tehtyä muutamia eri aihealueisiin liittyen. Tehtäviä tehdessä tuli hyödynnettyä paljon käytännön osaamista.

Tulen varmasti hyödyntämään oppimiani taitoja tulevaisuuden työelämässä. Tuntuu että olen oppinut tämän projektin aikana ehkä jopa enemmänkin kuin kurssien aikana. Tosin kursseilla ei olisi ehtinyt käydäkään yhtä laajasti asioita läpi. Tekemällä siis oppii todella paljon.

Lähteet

1. IETF. Introduction to the IETF [Internet]. [viitattu 7.10.2024]. Saatavilla: https://www.ietf.org/about/introduction

2. Klusaitė L. NordVPN. TCP IP -mikä se on, mihin sitä tarvitaan ja mitä se tekee? [Internet] 9.3.2022 [viitattu 5.9.2024]. Saatavilla: https://nordvpn.com/fi/blog/tcp-ip-protokolla/?srsltid=AfmBOor2j0Xl3tItjCSJqOKQmXQiMYbwdPkW2zHGDCmtlv-Z3r7V5pf_

3. GeeksforGeeks. TCP/IP Model. 5.8.2024. [viitattu 14.10.2024]. Saatavilla: https://www.geeksforgeeks.org/tcp-ip-model/

4. W3C. About us. [Internet]. [viitattu 8.10.2024]. Saatavilla: https://www.w3.org/about/

5. W3C. Staff. [Internet]. [viitattu 8.10.2024]. Saatavilla: https://www.w3.org/staff/

6. RDFox. What is w3c? What are the w3c standards? Why do they matter? [Internet]. [viitattu 8.10.2024]. Saatavilla: https://www.oxfordsemantic.tech/faqs/what-is-w3c-what-are-the-w3c-standards-why-do-they-matter

7. Kyberturvallisuuskeskus. Tietoturvasäätely. [Internet]. [viitattu 9.10.2024]. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturvasaantely

8. Kyberturvallisuuskeskus. Digitaaliset palvelut ja infrastruktuuri. [Internet]. [viitattu 9.10.2024]. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaaliset-palvelut-ja-infrastruktuuri

9. Tietosuojakeskus. Uusia velvoitteita tietojen ja verkkojen turvallisuuteen – Mikä on NIS 2 direktiivi? [Internet]. [viitattu 20.11.2024]. Saatavilla: https://tietosuojakeskus.fi/mika-on-nis-2-direktiivi/

10. InfoLawGroup. GDPR: Getting Ready for the New EU General Data Protection Regulation. [Internet]. 5.5.2016 [viitattu 15.10.2024] Saatavilla: https://www.infolawgroup.com/insights/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation

11. Your Europe. Yleinen tietosuoja-asetus. [Internet]. [viitattu 9.10.2024] Saatavilla: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm#inline-nav-11

12. Jurvanen L. Mitä kyberturvallisuuskeskus tekee? [Internet]. 27.10.2023 [viitattu 10.10.2024]. Saatavilla: https://www.savelan.fi/mita-kyberturvallisuuskeskus-tekee/

13. Nishtha. What is Client-Server Architecture? [Internet]. [viitattu 21.10.2024]. Saatavilla: https://intellipaat.com/blog/what-is-client-server-architecture/

14. IT-Helpdesk. Yleistä salausmenetelmistä. [Internet]. [viitattu 22.10.2024]. Saatavilla: https://helpdesk.it.helsinki.fi/help/3253

15. Cloudflare. How does public key cryptography work? [Internet]. [viitattu 22.10.2024]. Saatavilla: https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/

16. Fall Kevin R., Stevens R. TCP/IP Illustrated, Volume 1. The Protocols. Toinen painos. Addison-Wesley; 2012. Saatavilla: https://ia803003.us.archive.org/20/items/RichardStevensTCPIPIllustratedEN/Richard_Stevens-TCP-IP_Illustrated-EN.pdf

17. Heinonen P. Tiedonsalaaminen. [Internet]. [viitattu 8.11.2024]. Saatavilla: https://appro.mit.jyu.fi/doc/tiedonsalaus/

18. MDN. HTTP. [Internet]. 2.10.2024 [viitattu 8.11.2024]. Saatavilla: https://developer.mozilla.org/en-US/docs/Web/HTTP

19. Cloudflare. What is HTTPS? [Internet]. [viitattu 8.11.2024]. Saatavilla: https://www.cloudflare.com/learning/ssl/what-is-https/

20. Cloudflare. What is TLS (Transport Layer Security)? [Internet]. [viitattu 8.11.2024]. Saatavilla: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

21. Cloudflare. What is DNS? | How DNS works. [Internet]. [viitattu 10.11.2024]. Saatavilla: https://www.cloudflare.com/learning/dns/what-is-dns/

22. Šimonėlytė M. DNS: aloittelijan opas internetin nimipalvelinjärjestelmään. [Internet]. 4.4.2023 [viitattu 10.11.2024]. Saatavilla: https://nordvpn.com/fi/blog/mika-on-dns/

23. Cloudflare. How does DNSSEC work? [Internet]. [viitattu 5.12.2024]. Saatavilla: https://www.cloudflare.com/learning/dns/dnssec/how-dnssec-works/

24. Houghton S. Next-Generation Firewall (NGFW) vs Traditional Firewall. [Internet]. 25.9.2024 [viitattu 12.11.2024]. Saatavilla: https://www.aztechit.co.uk/blog/next-generation-firewall-ngfw-vs-traditional-firewall

25. Palo Alto Networks. What is the Difference Between Web Application Firewall (WAF) and Next-Generation Firewall (NGFW)? [Internet]. [viitattu 12.11.2024]. Saatavilla: https://www.paloaltonetworks.com/cyberpedia/difference-between-wafs-and-ngfws

26. Cloudflare. What is a WAF? | Web Application Firewall explained. [Internet]. [viitattu 12.11.2024]. Saatavilla: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

27. VMware. What is a hypervisor? [Internet]. [viitattu 8.9.2024]. Saatavilla: https://www.vmware.com/topics/hypervisor

28. AWS. What's the Difference Between Type 1 and Type 2 Hypervisors? [Internet]. [viitattu 8.9.2024]. Saatavilla: https://aws.amazon.com/compare/the-difference-between-type-1-and-type-2-hypervisors/

29. AWS. What is Docker? [Internet]. [viitattu 4.9.2024]. Saatavilla: https://aws.amazon.com/docker/

30. The Apache Software Foundation. The Number One HTTP Server On The Internet. [Internet] [viitattu 31.10.2024]. Saatavilla: https://httpd.apache.org/

31. Both D. How to configure multiple websites with Apache web server. [Internet] 29.3.2018 [viitattu 6.11.2024]. Saatavilla: https://opensource.com/article/18/3/configuring-multiple-web-sites-apache

32. Padilla A. Install and Configure Apache. [Internet] 26.8.2021 [viitattu 7.11.2024]. Saatavilla: https://ubuntu.com/tutorials/install-and-configure-apache#4-setting-up-the-virtualhost-configuration-file

33. Schandl B. Protecting your Application Database on the Network Level. [Internet] 3.11.2017 [viitattu 3.12.2024]. Saatavilla: https://medium.com/monsterculture/protecting-your-application-database-on-the-network-level-6393749c9c3c

34. RunCloud Blog. Docker Security – Best Practises to Secure a Docker Container. [Internet] 30.10.2023 [viitattu 6.11.2024]. Saatavilla: https://runcloud.io/blog/docker-security#5-set-volumes-and-file-system-permissions-to-readonly

35. Docker Docs. Packet filtering and firewalls. [Internet]. [viitattu 17.11.2024]. Saatavilla: https://docs.docker.com/engine/network/packet-filtering-firewalls/

36. Girnus P. Wireshark: Filter HTTP GET & POST Request Packets. [Internet] 6.3.2024 [viitattu 20.11.2024]. Saatavilla: https://www.petergirnus.com/blog/wireshark-display-filter-http-requests-for-get-and-post-packets

37. Docs CSC. SSH client on Windows. [Internet] 7.8.2024 [viitattu 4.12.2024]. Saatavilla: https://docs.csc.fi/computing/connecting/ssh-windows/

38. Ellingwood J, Boucheron B. How To Configure SSH Key-Based Authentication on a Linux Server. [Internet] 17.6.2021 [viitattu 4.12.2024]. Saatavilla: https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-key-based-authentication-on-a-linux-server