jamk.fi

Tietoturvanäkökohdat Amazon Elastic Compute Cloud käytössä: tapaus Contri-board

Joni Paananen

Opinnäytetyö
Huhtikuu 2015

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Paananen, Joni	Opinnäytetyö	15.04.2015
	Sivumäärä 52 + 20	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Tietoturvanäkökohdat Amazon Elastic Compute Cloud käytössä: tapaus Contriboard

Koulutusohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Karo Saharinen
Sampo Kotikoski

Toimeksiantaja(t)
N4SJAMK
Jarmo Viinikanoja

Tiivistelmä

Opinnäytetyön toimeksiantaja on N4SJAMK, joka on Digilen Need For Speed tutkimusohjelmassa mukana oleva Jyväskylän ammattikorkeakoulun projekti. Projektin päätarkoituksena on tutkia, kehittää ja luoda ratkaisuja Digilen N4S kumppaneiden kanssa.

Työn tavoitteena oli kartoittaa, testata ja kehittää palvelimien tietoturvaa jotka sijaitsevat Amazon EC2 pilvipalvelussa. Kaikki työssä käytettävät testausohjelmistot olivat ilmaisia, ohjelmistot olivat Nmap ja Nessus. Testattavia laitteita oli kahdeksan.

Työssä suoritettiin kahta erilaista tietoturvatestausta: portti skannausta ja haavoittuvuus skannausta. Tulosten saannin jälkeen haavoittuvuudet tutkittiin, etsittiin korjaustoimenpiteet ja ne suoritettiin järjestelmään. Korjausten jälkeen suoritettiin vielä toiset testaukset korjaustoimenpiteiden toimimisen varmistamiseksi.

Lopputuloksena järjestelmästä tehtiin tietoturvallinen laitteiden ja verkon osalta.

Avainsanat (asiasanat)
N4SJAMK, tietoturva, Nmap, Nessus

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Description

Author(s)	Type of publication	Date
Paananen, Joni	Bachelor's thesis	15.04.2015
		Language of publication: Finnish
	Number of pages 52 + 20	Permission for web publication: x

Title of publication

Security Aspects in use of The Amazon Elastic Compute Cloud: Case Contriboard

Degree programme

Networking Technology

Tutor(s)

Saharinen, Karo
Kotikoski, Sampo

Assigned by

N4SJAMK
Jarmo Viinikanoja

Abstract

The thesis was assigned by N4SJAMK which is a project within JAMK University of Applied Sciences. N4SJAMK is also a part of the Digile N4S research programme. The purpose of the project is to research, develop and create new solutions with Digile's N4S partners.

The aim of the thesis was to chart out, test and develop N4SJAMK server's security. The servers are located in the Amazon Elastic Compute Cloud. The security tools used were Nmap and Nessus. Nmap is a free and open source utility and Nessus is a closed-source security testing software. The amount of tested devices was eight.

Two kinds of security testing were performed in the thesis: port scanning and vulnerability testing. After getting results from the scans, the vulnerabilities were researched, fixes were searched and applied to the system. After the fixes were applied, the tests were performed again to make sure the fixes were effective.

As a result the system was made secure regarding the devices and network.

Keywords/tags (subjects)

N4SJAMK, security, Nmap, Nessus

Miscellaneous

Sisältö

Kuviot

TAULUKOT

LYHENTEET

AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Services
CBC	Cipher Block Chaining
CIA	Confidentiality Integrity Availability
CIDR	Classless Inter-Domain Routing
CSA	Cloud Security Alliance
CTR	Counter
DoS	Denial of Service hyökkäys
DDoS	Distributed Denial of Service hyökkäys
EC2	Amazon Elastic Compute Cloud
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS/SSL
IEEE	Institute of Electrical and Electronics Engineers
IaaS	Infrastructure-as-a-Service
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
MAC	Message Authentication Code
NAT	Network Address Translation
OSSTMM	Open Source Security Methology Manual
PaaS	Platform-as-a-Service
ROI	Return on investment
SaaS	Software-as-a-Service
SLA	Service Lever Agreement
SSH	Secure Shell
SSL	Secure Sockets Layer
S3	Amazon Simple Storage Service
TLS	Transport Layer Security
VMM	Virtual Machine Monitor
VPC	Virtual Private Cloud

1 TYÖN LÄHTOKOHDAT

1.1 Toimeksiantaja

Työn toimeksiantaja oli N4SJAMK. N4SJAMK on Jyväskylän ammattikorkeakoulun projekti, joka on osa Need For Speed -yhteistyökonsortiota.

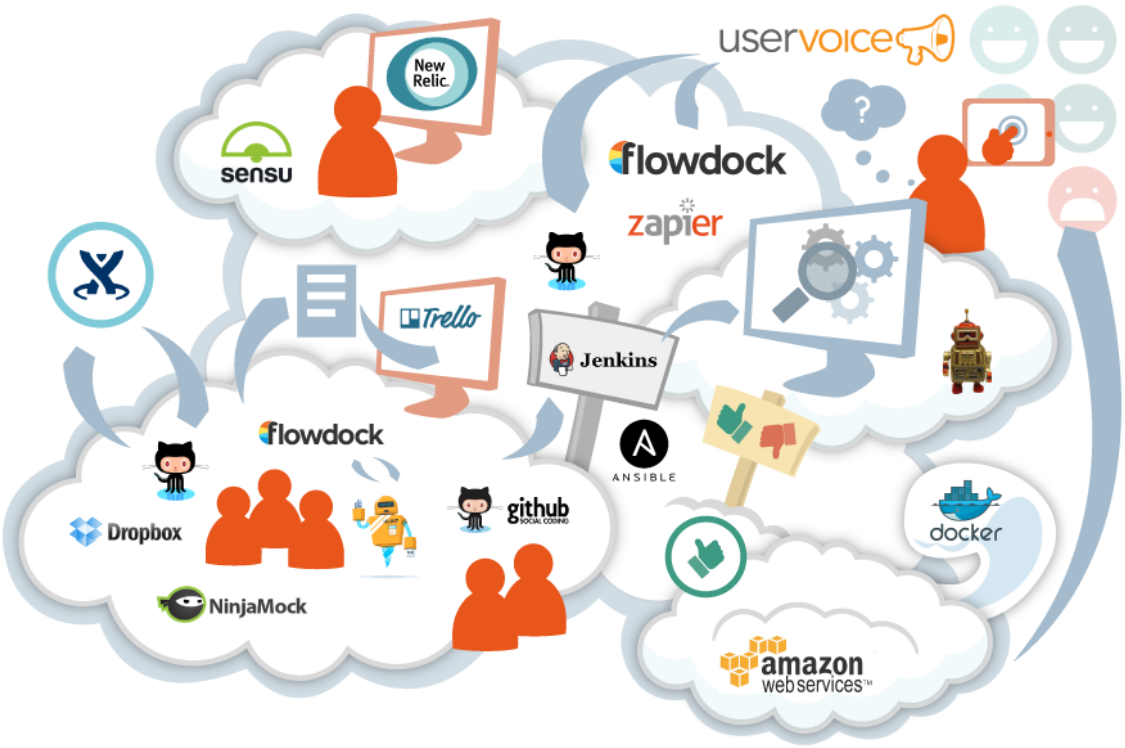
N4SJAMKin päätavoite on tutkia, kehittää ja luoda ratkaisuja yhteistyössä Digilen N4S-kumppaneiden kanssa.

Digilen N4S-yhteistyökonsortion tarkoituksena on luoda perusta suomalaisten ohjelmistoalan yrityksien menestykselle nykyaikaisessa digitaalisessa taloudessa. Ohjelmassa testataan käytännössä reaaliaikaisia liiketoimintamalleja, jotka perustuvat syvään asiakastuntemukseen, mikä mahdollistaa välittömän arvon tuottamisen. Ohjelman toteuttavat suuret suomalaiset ohjelmistoyritykset. Digilen N4S-ohjelma on nelivuotinen 2014–2017. (N4S-Ohjelma 2014.)

1.2 Tavoitteet

N4SJAMKin palvelimet sijaitsevat Amazon EC2-pilvipalvelussa. Työn tavoitteena oli kartoittaa palvelimien tietoturva sekä tutkia Amazon EC2-pilvipalvelun osa-alueet liittyen tietoturvaan. Lisäksi tarkoitus oli testata kyseisen palvelun tietoturvaa. Toimeksiantajalla oli toive tietoturvan yhdistämisestä jatkuvan julkaisun malliin.

Kuviosta 1 nähdään kehitysketju Corolla.



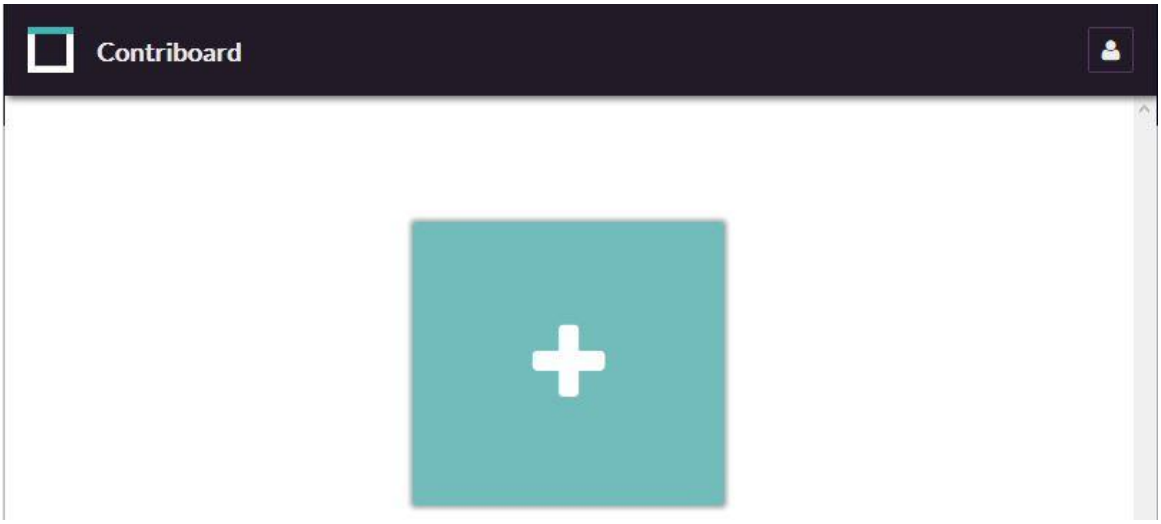
Kuvio 1. Jatkuvan kehityksen malli

1.3 Contriboard

N4SJAMKin tuote on Contriboard, joka on avoimen lähdekoodin reaaliaikainen yhteistyökalu tiimien toimintaa varten. Contriboardia kehitetään modernien teknologioiden ja työnkulun avulla jotka sallivat nopean käyttöönoton sekä julkaisun. (About the product. 2014)

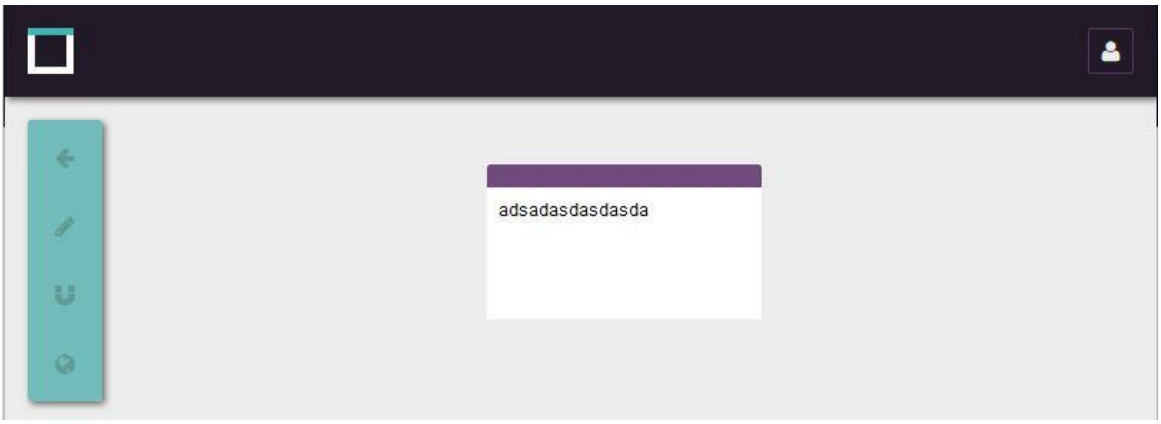
Contriboard on referenssi tuote joka on tehty Corolla-ketjulla. Työ tehdään tutkimus tarkoituksessa Jyväskylän ammattikorkeakoululle. (About the product. 2014)

Kuviosta 2 nähdään Contriboardin käyttöliittymä.



Kuvio 2. Contriboardin käyttöliittymä

Kuviosta 3 nähdään Contriboardissa luotu tiketti.



Kuvio 3. Contriboard-tiketti

2 PILVIPALVELUT

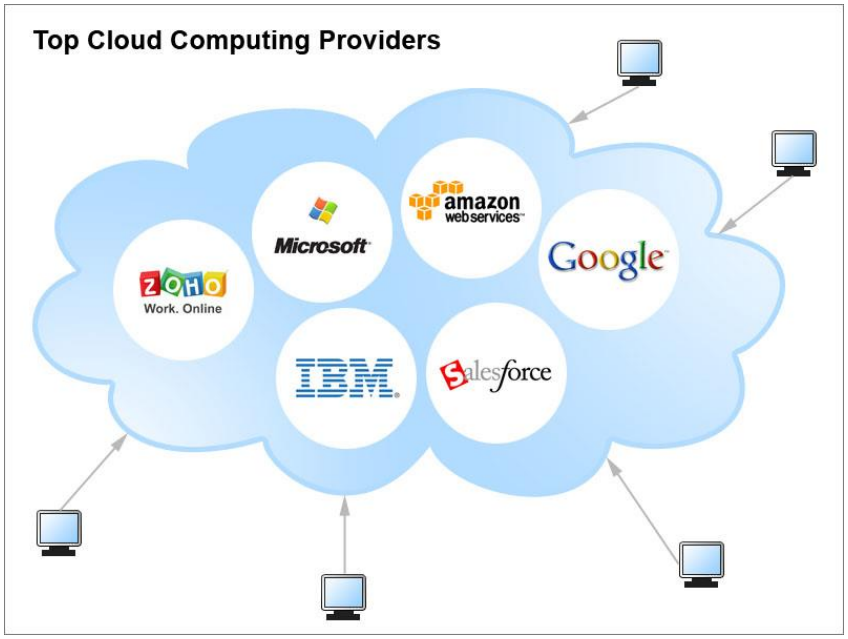
2.1 Yleistä

Yksinkertaisuudessaan pilvipalvelut tarkoittavat datan ja ohjelmien tallentamista ja käsiksi pääsyä internetin yli sen sijaan, että nämä asiat sijaitsisivat paikallisella tietokoneella. Tilanne, jossa palvelinlaitteet sijaitsevat paikallisissa tiloissa, ei tarkoita pilveä. Pilvi-nimityksellä tarkoitetaan Internetiä. Käyttäjällä ei saata olla mitään ideaa siitä, kuinka paljon datan prosessointia tapahtuu yhteyden toisessa päässä. (Griffith 2013, 1.)

Raja paikallisen ja pilviprosessoinnin välillä voi välillä hämärtyä, koska pilvi on suuri osa tietokoneita nykypäivänä. Esimerkkinä Microsoft Office 365-sovellusperhe, jossa tarjotaan pilvitallennustilaa Microsoft Skydriven muodossa, mutta Microsoftilla on myös tarjolla verkkosovelluksia, jotka ovat hyvin samanlaisia kuin Microsoft Word, Excel, Powerpoint ja OneNoten työpöytäversiot. Markkinoilla on tarjolla laitteita, jotka on periaatteessa tarkoitettu pilvikäyttöön kuten Samsung Chromebook-sarjan kannettavat tietokoneet joissa on prosessointikapasiteettia juuri internetselaimen käyttöä varten ja sovellukset löytyvät pilvestä (Griffith 2013, 2.)

Yksi suuri kysymys pilvipalveluiden käytössä on tullut vastaan: kuka omistaa datan, joka tallennetaan pilveen? Pilvipalveluita ei valvo mikään yksi organisaatio mutta IEEE-organisaatio loi IEEE Cloud Computing Initiativen vuonna 2011, jolla he yrittävät luoda standardit pilvipalveluiden käyttöä varten. (Griffith 2013, 3.)

Kuviossa 4 nähdään suurimpia pilvipalvelun tarjoajia.



Kuvio 4. Suurimpia pilvipalvelun tarjoajia (Suhkraj 2013)

Pilvipalvelu on malli, joka sallii kaikkialla läsnä olevan, heti saatavilla olevan verkkoyhteyden jaettuun resurssialtaaseen joka sisältää konfiguroitavia tietokoneresursseja esim.

- verkkoja

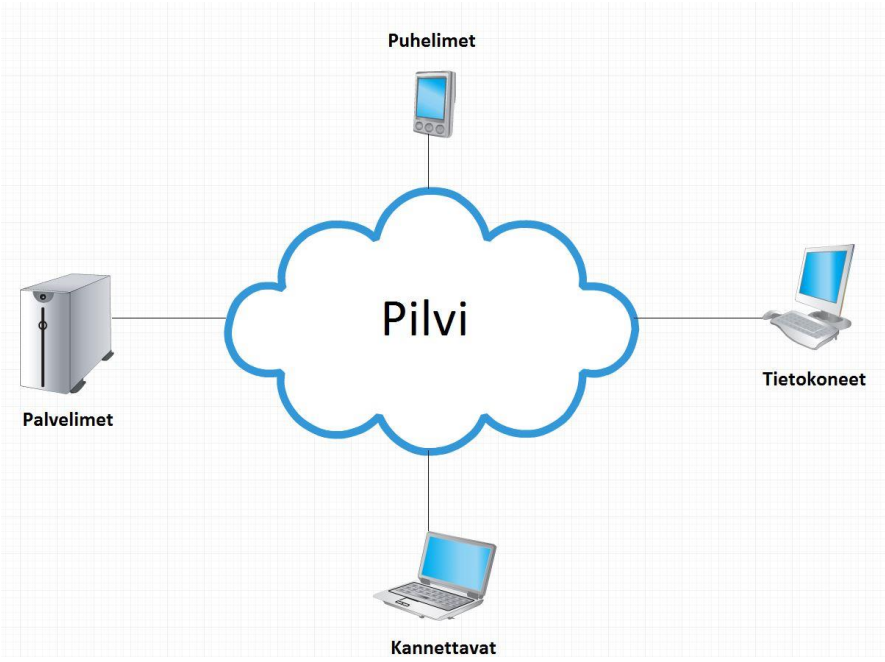
- palvelimia
- tallennustilaa
- sovelluksia
- palveluita
- laskentatehoa.

Näitä resursseja voidaan nopeasti varata ja vapauttaa pienellä hallinnollisella vaivalla tai palveluntarjoajan toimesta. (Mell & Grance 2011, 6.)

Pilvipalveluilla yleensä haetaan säästöjä, koska yrityksien tai organisaatioiden ei tarvitse palkata henkilöstöä paikalliseen laitteiden hallinnointiin tai ostaa kyseisiä laitteita.

Pilvipalvelu-termin alkuperästä ei ole tarkkaa tietoa mutta jossain vaiheessa sitä alettiin käyttämään verkkojen ja niiden palvelujen kuvailuun.

Kuviossa 5 nähdään pilvipalvelun yleiskuva.

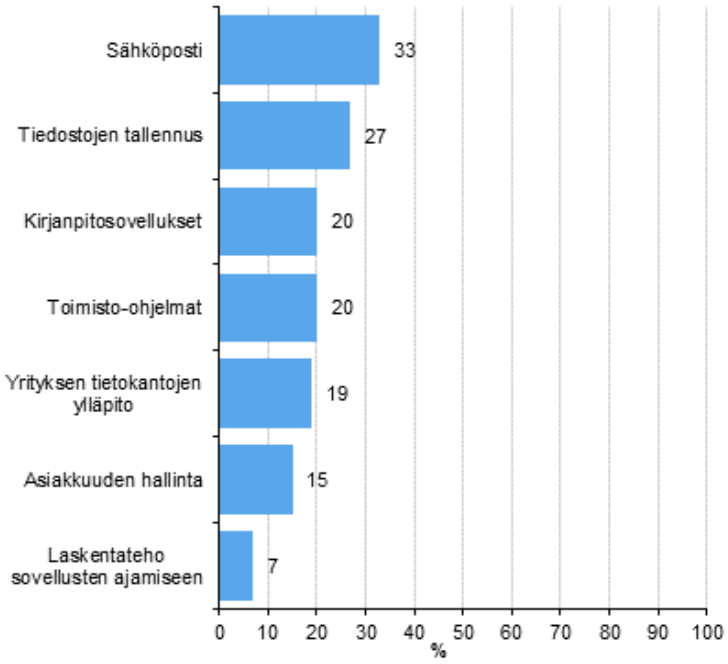


Kuvio 5. Pilven rakenne

2.2 Pilvipalvelujen käyttö

Tilastokeskuksen mukaan suomalaisista yrityksistä 51 % käyttää maksullisia pilvipalveluita. Jos pilvipalveluiden käyttö jaotellaan toimialoittain, yleisimmin palveluita käytetään informaation ja viestinnän alan yrityksissä, joissa käyttö on 81 %, ja harvimmin vähittäiskaupan toimialalla, jossa käyttö on 31 %. (Tietotekniikan käyttö yrityksissä 2014.)

Kuviossa 6 nähdään suomalaisten yritysten maksullisien pilvipalveluiden käyttötarkoitukset vuoden 2014 aikana.

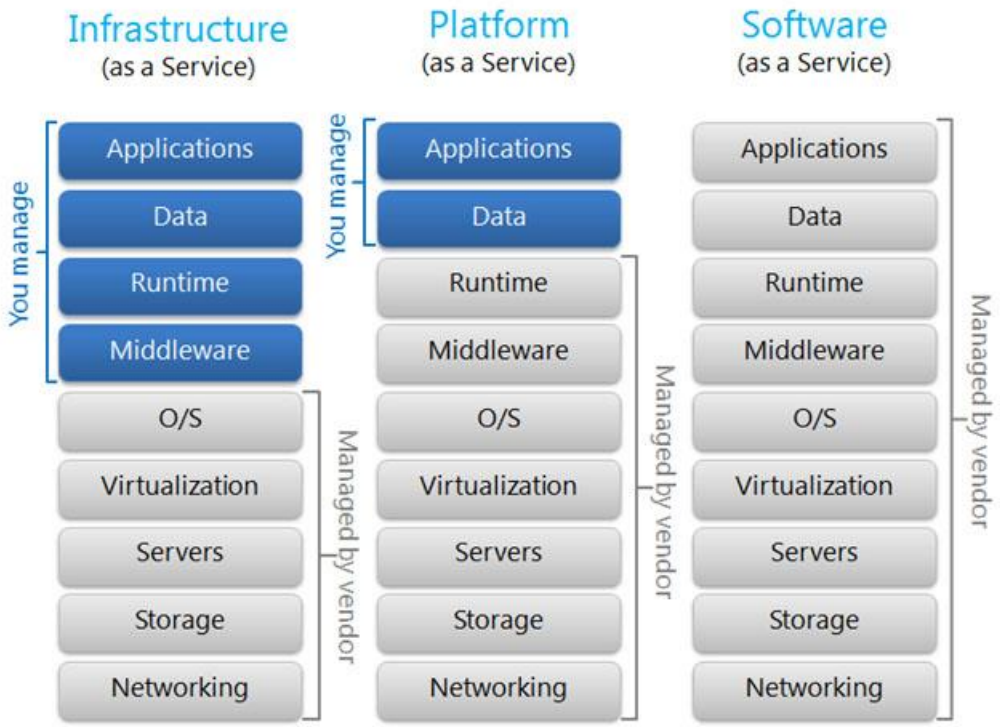


Kuvio 6. Maksullisten pilvipalveluiden käyttö yrityksissä(Tietotekniikan käyttö yrityksissä 2014)

2.3 Pilvipalvelumallit

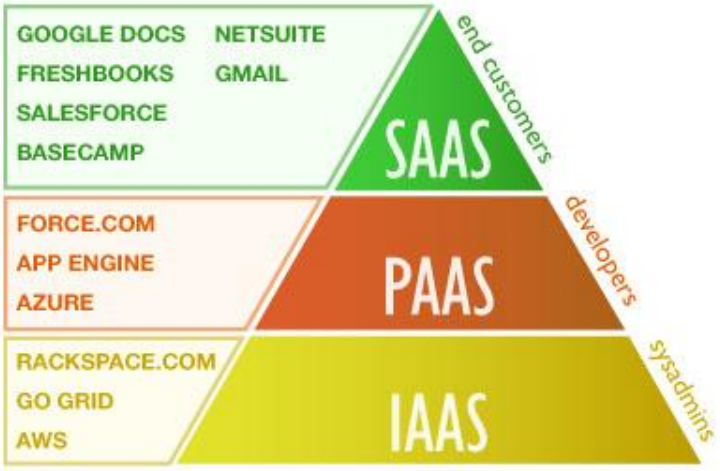
Pilvipalvelumalleja on kolme: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) ja Software-as-a-Service (SaaS). Jokaisella on jotakin yhteistä, mutta kuitenkin omaavat omat eronsa. Kaikki pilvipalveluiden palvelut sopivat johonkin näistä mainituista malleista. (Hemmings 2012.)

Kuviossa 7 nähdään, mitä resursseja eri pilvipalvelumallit tarjoavat.



Kuvio 7. Pilvipalvelumallit (Mahadik 2013)

Kuviossa 8 nähdään yrityksiä ja palveluita pilvipalvelumallien käytön mukaan.



Kuvio 8. Palvelumalleja käyttäviä yrityksiä (Sukhraj 2013)

2.3.1 Infrastructure-as-a-Service

Infrastructure-as-a-Service on ensimmäinen taso ja pilvipalvelun perusta. Käyttämällä tätä mallia voidaan hallinnoida omia sovelluksia, dataa, käyttöjärjestelmiä, väliohjelmistoja ja käyttöaikoja. Pilvipalvelun tarjoaja hallinnoi virtualisoinnin, palvelimet, verkot ja tallennustilan. Tämä sallii säästöt laitteistossa ja henkilöstössä, voidaan vähentää ROI riskiä, virtaviivaistaa ja automatisoida skaalautumista. Suurimpia Infrastructure-as-a-Servicen palvelujen tarjoajia tällä hetkellä ovat Amazon, Microsoft, VMware, Rackspace ja RedHat. (Hemmings 2012.)

Tätä mallia käyttävät esimerkiksi henkilöt/yritykset, jotka tarvitsevat prosessointitehoa ajoittain. Infrastructure-as-a-Service sallii resurssien käytön, kun niitä tarvitaan, ja ei tarvitse maksaa muusta kuin käytetyistä resursseista. (Hemmings 2012.)

2.3.2 Platform-as-a-Service

Platform-as-a-Service-mallia voidaan ajatella toisena kerroksena pilvipalveluissa. Palvelun käyttäjä hallinnoi dataa ja sovelluksia ja palvelun tarjoaja hallinnoi muita osa-alueita. Platform-as-a-Servicen suurimpia hyötyjä ovat virtaviivainen versioiden käyttöönotto sekä vaihto tai päivitys ja kulujen minimointi. Yksi suosittu tätä mallia käyttävä palvelu on Googlen hakukone. (Hemmings 2012.)

Yritys, jonka tarkoituksena on kehittää ohjelmistoja, voi nähdä Platform-as-a-Servicen hyvänä keinona vähentää kuluja laitteiston ylläpidosta, koska ei tarvitse palkata henkilöstöä tähän tarkoitukseen (Hemmings 2012).

2.3.3 Software-as-a-Service

Software-as-a-Service on kolmas ja viimeinen taso pilvipalvelumalleista. Tämä malli sallii sovelluksien ajamisen pilvessä, ja palvelun tarjoaja hallinnoi kaikkia osa-alueita. Käyttäjät saavat saman kokemuksen, koska kaikki käyttävät samoja sovelluksia. Yrityksen ei tarvitse maksaa ylimääräisiä lisensointimaksuja, ja käyttäjien lisäys on helppoa. Nykyään

kaikki internetin käyttäjät käyttävät tietämättään tähän malliin pohjautuvia sovelluksia joka päivä, esimerkkinä verkkopankit ja Gmail (Hemmings 2012).

Kun yritykset käyttävät Software-as-a-Service-mallin palveluita, palveluihin päästään käsiksi monella eri laitteella paikasta riippumatta mikä helpottaa yhteistyötä työntekijöiden välillä (Hemmings 2012).

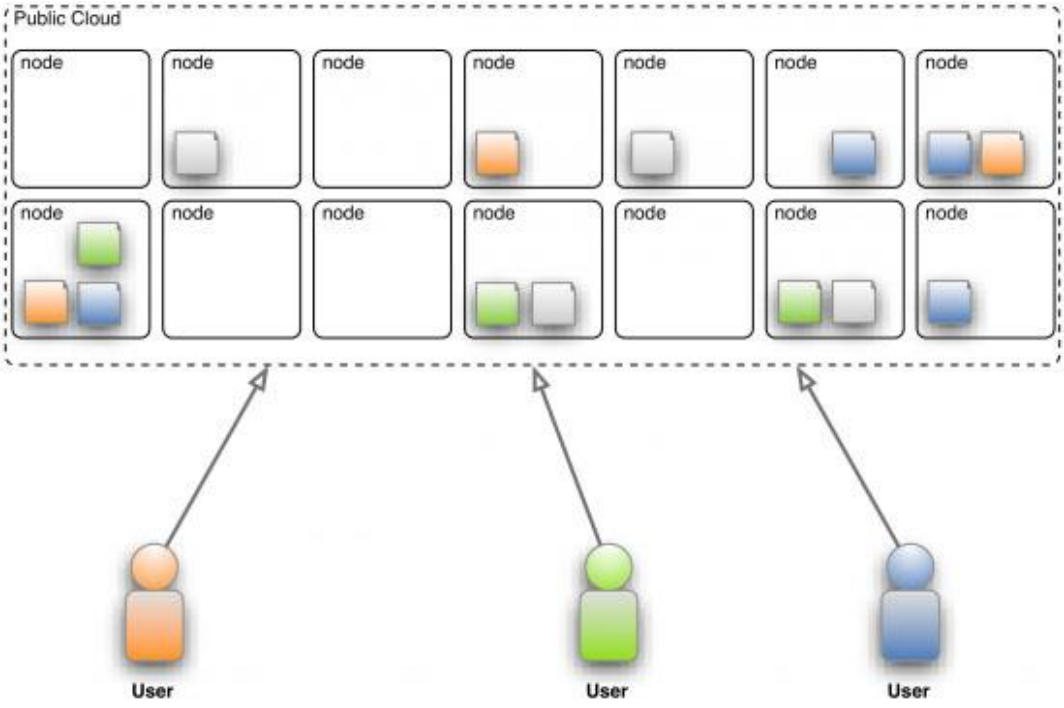
2.4 Pilvipalveluiden käyttöönottomallit

Pilvipalveluita voidaan ottaa käyttöön usealla eri tavalla riippuen organisaation rakenteesta ja varausten sijainnista. Yleisesti ottaen käyttöönottomalleja on neljä: julkinen, yksityinen, yhteisö ja hybridi pilvi.

2.4.1 Julkinen pilvi

Julkiselle pilvelle on tunnusomaista se, että palvelu on julkisesti saatavilla kaikille ja verkko, jonka kautta ollaan yhteydessä palveluun, on julkinen. Pilvipalvelut ja resurssit ovat saatavilla suurista resurssialtaista, jotka on jaettu käyttäjien kesken. Nämä IT-tehtaat, jotka on rakennettu pyörittämään pilvipalveluita, osaavat säännöstellä resursseja tarkasti haluttujen määrien mukaan. Jos pilvipalvelun tarjoaja pyörittää useampaa datakeskusta, resursseja voidaan jakaa näiden keskusten välillä, jotta kuorma pysyisi tasaisena. (What are Deployment Models in Cloud Computing? n, d.)

Kuviosta 9 nähdään esimerkki siitä, kuinka resursseja käytetään julkisessa pilvipalvelussa käyttäjien kesken.



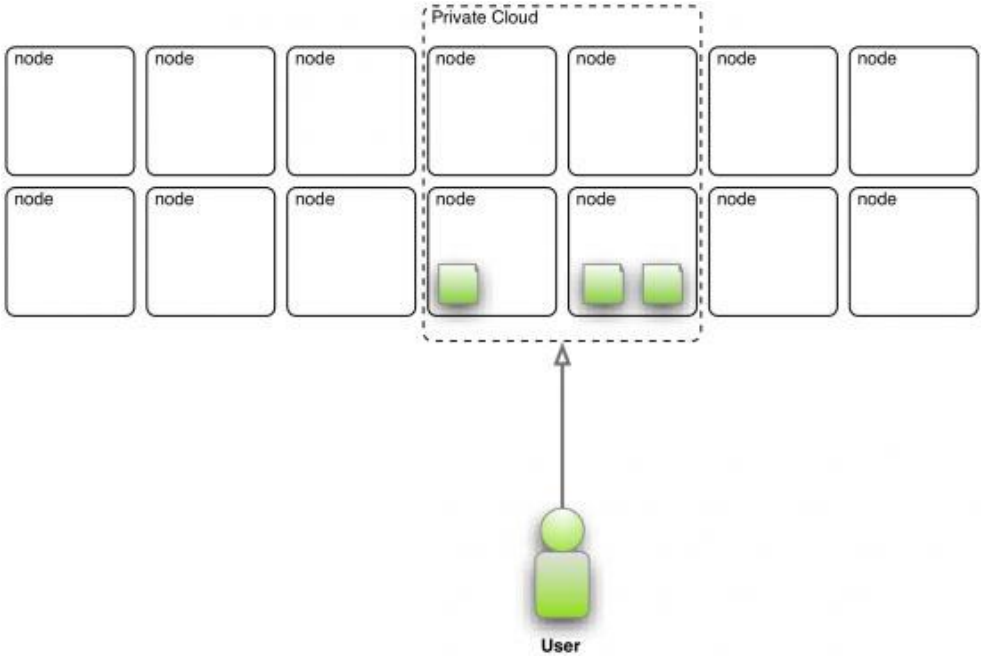
Kuvio 9. Julkisen pilven käyttö kolmella käyttäjällä (What are Deployment Models in Cloud Computing? n.d.)

Hyvänä esimerkkinä julkisen pilven järjestelmistä on Amazon Web Services (AWS), joka sisältää Elastic Compute Cloud (EC2) ja Simple Storage Servicen (S3), mikä muodostaa Infrastructure-as-a-Service palvelutarjonnan (What are Deployment Models in Cloud Computing? n, d.).

2.4.2 Yksityinen pilvi

Yksityiset pilvijärjestelmät jäljittelevät julkisen pilven antia, jotta palvelu voidaan tarjota yksittäiselle organisaatiolle. Yksityiset pilvet käyttävät virtualisointiratkaisuja ja keskittyvät yhdistämään jaettuja palveluita usein datakeskuksissa, jotka ovat yrityksen omistuksissa. Suurin hyöty näissä palveluissa on se, että yritys säilyttää täyden hallinnan yrityksen dataan, turvaohjesääntöihin ja järjestelmän suorituskykyyn. (What are Deployment Models in Cloud Computing? n. d.)

Kuviossa 10 nähdään, kuinka yksityisessä pilvipalvelussa resurssit ovat käyttäjien käytössä.

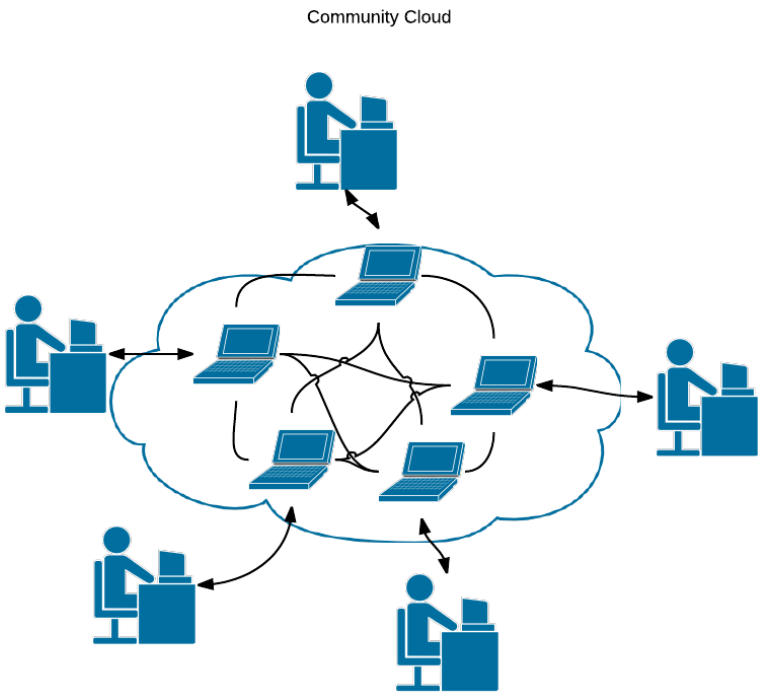


Kuvio 10. Käyttäjä käyttää yksityistä pilveä (What are Deployment Models in Cloud Computing? n. d.)

2.4.3 Yhteisöpilvi

Yhteisöpilvessä yritykset, joilla on samankaltaiset tarpeet, jakavat pilvirakenteen. Pilven infrastruktuuri säännöstellään yksinomaisesti tietylle yhteisölle käyttäjiä, joilla on jaetut huolenaiheet, esim. tehtävä, tietoturvatarpeet. Pilven voi omistaa ja hallinnoida yksi tai useampi organisaatio yhteisössä, kolmas osapuoli tai jokin yhdistelmä näitä. (Mell & Grance 2011, 7.)

Kuviossa 11 nähdään, kuinka yhteisöpilvi-palvelussa resurssien jako toimii käyttäjien kesken.

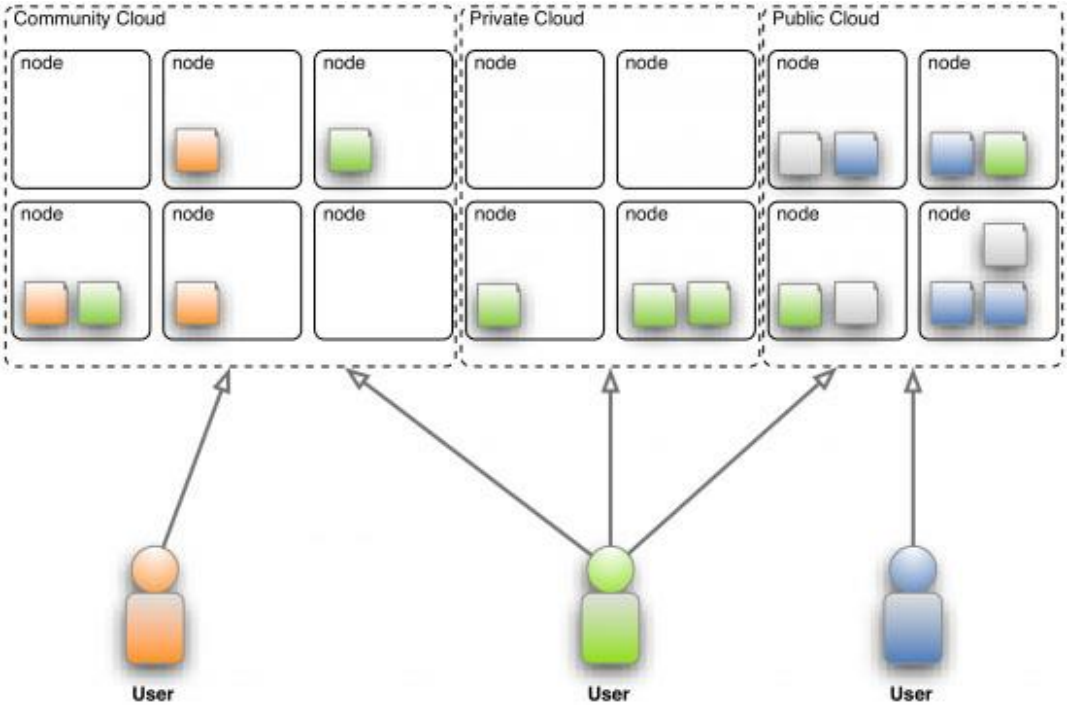


Kuvio 11 Yhteisöpilven malli

2.4.4 Hybridipilvi

Pilven rakenne koostuu kahdesta tai useammasta erilaisesta pilvirakenteesta (yksityinen, julkinen tai yhteisö), jotka ovat kuitenkin oma kokonaisuutensa. Nämä rakenteet ovat sidottuja toisiinsa standardoidulla tai jollakin eri teknologialla, joka sallii datan ja sovellusten siirtämisen esimerkiksi pilvipuhkeamisella, joka sallii kuorman tasauksen pilvien välillä. (Mell & Grance 2011, 7.)

Kuviossa 12 nähdään esimerkki siitä, kuinka hybridi pilvipalvelu voi sisältää aiemmin mainittuja pilvipalveluita ja kuinka käyttäjät käyttävät resursseja näistä palveluista.



Kuvio 12 Hybridi pilven käyttö (What are Deployment Models in Cloud Computing? n. d.)

2.5 Pilvipalveluiden tietoturva

Pilvipalveluiden tietoturva on hankala asia, koska ei ole paikallisia laitteita, joihin voisi soveltaa fyysistä tai sähköistä tietoturvaa. On siis lähdettävä ajattelemaan asioita eri kantilta.

Cloud Security Alliance teki vuonna 2013 listan yhdeksästä pahimmasta uhkasta pilvipalveluille.

Kohta 1: Tietomurrot

Esimerkkinä kyseisestä on tapaus, jossa tutkijat saivat varastettua kryptografisia avaimia virtuaalisella tietokoneella muilta virtuaalisilta koneilta, jotka pyörivät samalla fyysisellä laitteistolla. Hyökkäys onnistui ainoastaan, jos hyökkääjän ja uhrin virtuaali tietokoneet pyörivät samalla fyysisellä laitteistolla. Tutkijat keskittyivät Xen Hypervisoriin, joka on (VMM) eli virtuaalitietokoneiden seurantajärjestelmä jota myös Amazonin EC2 pilvipalvelu käyttää. (Goodin 2012.)

Kohta 2: Datan häviäminen

Tähän asiaan ei asiakas voi ottaa kantaa periaatteessa millään tavalla. Asiakas voi tietysti kysyä palveluntarjoajalta, miten ja kuinka usein varmuuskopiot otetaan talteen. (Samson 2013, 1.)

Kohta 3: Tilin tai palvelu liikenteen kaappaus

Jos hyökkääjä saa haltuunsa asiakkaan tilitiedot, hän voi seurata liikennettä tai tapahtumia, manipuloida dataa, väärentää tietoja ja ohjata asiakkaiden liikenteen haitallisille sivuille tai osoitteisiin. On mahdollista että, jos hyökkääjä on saanut haltuunsa uhrin tiedot, hyökkääjä voi käyttää tämän tietoja tai palveluita tukikohtana uusille hyökkäyksille ja käyttää uhrin mainetta hyväkseen. Tämän estämiseksi olisi pidettävä huolta fyysisesti ja sähköisesti tilitietojen ja salasanojen säilytyksestä. (Mts. 1.)

Kohta 4: Haavoittuvaiset liitännät sekä (API) ohjelmistorajapinnat

Järjestelmänvalvojat käyttävät liitäntöjä käyttäjien oikeuksien hallintaan, yleiseen palvelun hallintaan sekä monitorointiin. Ohjelmistorajapinnat ovat elintärkeitä tietoturvalle sekä palvelun saatavuudelle. Haavoittuvaiset liitännät sekä rajapinnat voivat altistaa yrityksen tietoturvan liittyen luottamuksellisuuteen, eheyteen, saatavuuteen ja vastuullisuuteen. (Mts. 2.)

Kohta 5: (DOS) Palvelunestohyökkäykset

Palvelunestohyökkäykset ovat olleet uhkana jo vuosien ajan internetissä mutta pilvipalvelun tarjoajille se on vielä isompi haitta, kun kaikille palveluille halutaan tarjota ympärivuorokautinen saatavuus. Hetkellinenkin palvelun kaatuminen voi maksaa palveluntarjoajille paljon rahaa, mutta samoin voi käydä myös asiakkaalle, jos palveluntarjoaja veloittaa käsittelyajasta ja hyökkäyksen takia ei kyseisiin laitteisiin päästä käsiksi, mutta aika kuluu. (Mts. 2.)

Kohta 6: Pahantahtoiset sisäpiiriläiset

Tällainen voi olla nykyinen tai entinen työntekijä tai henkilö, jolla on pääsy verkkoon, järjestelmiin tai dataan haitallisessa tarkoituksessa. Tilanteet, joissa pilvipalveluntarjoaja on ainoastaan vastuussa turvallisuudesta, riskit voivat olla suuria. (Mts. 2.)

Kohta 7: Pilven väärinkäyttö

Esimerkkinä voi olla tapaus, jossa henkilö käyttää pilvipalvelun prosessointitehoa salauksen rikkomiseen, koska ei pysty siihen omilla laitteillaan. Toinen tapaus voisi olla sellainen jossa haitallinen hakkeri käyttää pilvipalvelimia laukaistakseen (DDOS) hajautetun palvelunestohyökkäyksen, jakaa vakoiluohjelmia tai jakaa laittomasti ladattua materiaalia. (Mts. 2.)

Kohta 8: Riskien ymmärtämättömyys

Riskien ymmärtämättömyydestä esimerkkinä on, että yritys käyttää pilvipalveluita ymmärtämättä pilven ympäristöä ja riskejä. Vastaan voi myös tulla operatiivisia ja arkkitehtuurisia ongelmia, jos esimerkiksi yrityksen tuotantotiimi ei ole perillä pilvipalveluteknologioista, kun laittavat sovelluksen pilveen. (Mts. 2.)

Kohta 9: Jaetut teknologiset heikkoudet

Yhdeksäntenä ja viimeisenä listalla ovat jaetut teknologiaheikkoudet. Pilvipalvelun tarjoajat jakavat infrastruktuureja, alustoja ja sovelluksia, jotta palveluita voidaan tarjota skaalautuvasti. Jos jokin keskeinen komponentti haavoittuu, kuten virtuaalilaitemonitori tai sovellus, se voi altistaa koko järjestelmän avoimeksi hyökkäyksille. (Mts. 2.)

Yleensä pilvipalveluiden tietoturvaa hallinnoidaan (SLA) palvelutasosopimusten avulla. Palveluntarjoaja määrittää tietoturvamenettelyt ja laatutasot. Yksityisissä pilvipalveluissa tietoturvaan on mahdollista vaikuttaa tietoturvatasoihin, mutta isot tekijät kuten Amazon ja Google eivät luultavasti anna vaihtoehtoja. (Pilvipalveluiden tietoturvasta yritysjohdolle 2010, 7.)

Palvelun tarjoajan dokumentointiin on hyvä tutustua huolellisesti. Vaikka dokumentointi olisi hoidettu huolellisesti, se ei tarkoita että kaikkea, mikä on suunniteltu, on toteutettu. Asiakas voi testata, onko palvelu toteutettu huolellisesti esimerkiksi tietoturva-auditoinnilla. Jos palveluntarjoaja ei suostu asiakkaan auditoitavaksi, voidaan vaatia kolmatta osapuolta tämän toteuttamiseksi. (Pilvipalveluiden tietoturvasta yritysjohdolle 2010, 8.)

Tietoturvahaavoittuvuudet paljastuvat pilvipalvelumallissa, kun oman verkon palomuurit eivät enää suojaa sisäisiä järjestelmiä. Pilvipalveluntarjoajalta tulee edellyttää haavoittuvuuksien hallintaprosessia, esimerkiksi web-sovellukset ovat etenkin haavoittuvia, jos näille sovelluksille ei ole tehty haavoittuvuustarkastusta eikä löydettyjä ja dokumentoituja löydöksiä ole korjattu, on melko varmaa että sovellukset ovat haavoittuvaisia. (Pilvipalveluiden tietoturvasta yritysjohdolle 2010, 8.)

Keskeisiä kysymyksiä palvelutasosopimuksen laatimisessa ovat seuraavat:

- Minkä maan lakeja noudatetaan?
- Kuka hallinnoi tietoa?
- Kuka omistaa tiedon?
- Kenellä on pääsy tietoon?
- Kuinka tietoon päästään käsiksi?
- Paikalliset lainsäädökset koskien tiettyä dataa ja sovellusta?
- Missä suhteessa korvaukset vikatilanteissa ovat palvelusta maksettuun hintaan tai kohde datan arvoon nähden? (Pilvipalveluiden tietoturvasta yritysjohdolle 2010, 9.)

2.6 Yleinen tietoturva

Tietoturvan tarkoituksena on suojata tietojärjestelmien luotettavuus, eheys ja saatavuus haitallisilta aikeilta. Luotettavuutta, eheyttä ja saatavuutta kutsutaan CIA tietoturva kolmikoksi. Tämä kolmikko on kehittynyt käsitteeksi jota kutsutaan nimellä Parkerian

Hexad, joka sisältää luotettavuuden, omistuksen (tai hallinnan), eheyden, aitouden, saatavuuden ja hyödyllisyyden. Näitä käsitteitä käytetään kun luodaan tietoturvapolitiikoita. (Janssen n, d.)

Tietoturva hoitaa riskien hallinnan. Mikä tahansa voi olla riski CIA tietoturva kolmikolle tai Parkerian Hexadille. Arkaluontoinen materiaali täytyy säilyttää, sitä ei saa muuttaa, muokata tai siirtää ilman lupaa. Esimerkkinä viesti joka on lähetetty matkaan ja joku kaappaa sen ennen kuin se pääsee vastaanottajalle ja sitä muokataan. Hyvät kryptografiset työkalut voivat auttaa estämään tällaisia uhkia. (Janssen n. d.)

2.6.1 Fyysinen

Fyysisellä tietoturvalla tarkoitetaan organisaation tilojen, niissä sijaitsevien laitteiden ja tallennusmedioiden suojaamista. Fyysisellä tietoturvalla taataan organisaatiolle ympäristö joka on turvallinen ja häiriötön. (Vedenoja 2007, 1.)

Kaikki organisaation tilat eivät ole fyysisen turvallisuuden kannalta samanarvoisia. Korkeaa suojausta vaativat tilat ovat organisaation oman toimialaan liittyvät tilat kuten tuotekehitystilat, atk-tilat ja hallinnolliset tilat. Yleisesti ottaen fyysiseen turvaan kuuluvat kaikki tilat jossa käsitellään organisaatiolle merkityksellistä tietoa. (Vedenoja 2007, 3.)

Toimitiloja varten on omat vaatimuksensa. ISO 27001 – standardissa on omat vaatimuksensa, Suomen puolustusvoimilla määritellään turvalliset tilat tarkasti. Myös VAHTI – ohjeissa otetaan kantaa fyysiseen turvaan.

Toimitilat tulisi suojata ainakin seuraavilta asioilta:

- varkaus
- tulipalo
- vesi ja kosteus
- sähköhäiriöt
- pöly (Vedenoja 2007, 4.)

Tärkeää on myös kulunvalvonta tiloihin joissa sijaitsee toiminnassa käytettäviä laitteita.

2.6.2 Tekninen

Teknisen tietoturvan päämääränä on se että käytetyissä laitteissa ja ohjelmistoissa ei ole tietoturvapuutteita. Tietoturvan suunnittelu ja mietintä on aloitettava jo siinä vaiheessa kun laitteita ja ohjelmistoja hankitaan. Jotta tietojärjestelmät ja niissä säilytettävät tiedot pysyvät luottamuksellisina, niihin pääsyä valvotaan käyttäjätunnuksien ja salasanojen avulla. Käyttäjätunnuksilla voidaan määrittää käyttäjäkohtaisesti mihinkä tietoihin käsiksi pääsyyn on oikeudet. (Suojausmenetelmät N.d.)

Käyttäjätunnukset ja salasanat eivät ole parhaimpia tietoturvaratkaisuja. Parempia ratkaisuja laajempia tietojärjestelmiä varten ovat palomuuriratkaisut ja datan salaus. (Suojausmenetelmät N.d.)

2.6.3 Hallinnollinen

Hallinnollinen tietoturva on tietoturvan johtamistoiminto ja organisaation koko tietoturvan lähtökohta. Siihen sisältyy johdon hyväksymän periaatteet, vastuunjako, tarkoitukseen varatut resurssit sekä riskien arviointi. (Väistö 2005.)

Varsinaiset toimenpiteet perustuvat hallinnollisiin ohjeisiin, joiden pohjana toimivat johdon määrittelemät periaatteet. Hallinnollisen tietoturvan tarkoituksena on luoda organisaatiolle tietoturvalliset toimintatavat. Toimintamallien pohjalta luodut henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä tietoturvan kehittämiseksi ja ylläpitämiseksi. (Väistö 2005.)

Käyttäjille oleellisia asioita hallinnollisessa tietoturvassa ovat:

- Organisaation tietoturvapolitiikka
- Tietoturvavastuiden jako
- Tietoturvaohjeiden laatu, kattavuus ja niiden koulutus
- Allekirjoitetut vakuutukset tietoturvaohjeiden lukemisesta ja noudattamisesta (Väistö 2005.)

Käyttäjän tulee olla tietoinen ohjeista ja erityisesti niistä ohjeista jotka koskevat hänen työtään. Lisäksi organisaation tietoturvavastuut tulee olla selkeästi määritelty ja kirjattu tarkasti muistiin. Käyttäjiä koskevat vastuut tulee kouluttaa ja ohjeistaa, jotta jokainen työntekijä on tietoinen omista tietoturvavastuistaan ja pystyy toimimaan vastuun edellyttämällä tavalla. (Väistö 2005.)

2.7 Tietoturva-auditointi

Tietoturva auditointi on systemaattinen arviointi organisaation tietoturvajärjestelmistä mittaamalla kuinka hyvin se noudattaa asetettuja kriteereitä. Läpikohtaisella auditoinnilla yleensä arvioidaan järjestelmän fyysinen konfiguraatio ja ympäristö, sovellukset, tiedon käsittely menetelmät ja käyttäjä käytännöt. (Rouse 2005.)

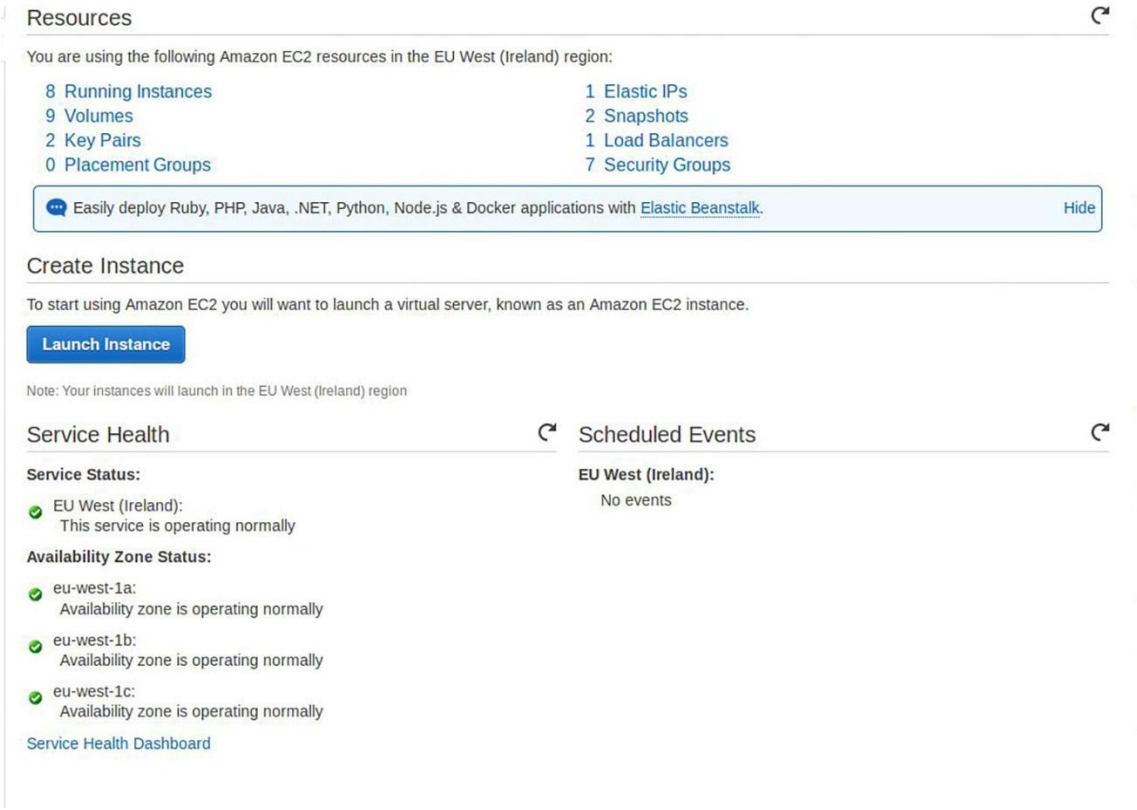
Yleensä tietoturva auditointeja järjestetään koska halutaan varmistaa että organisaatio noudattaa virallisia tietoturva säännöksiä. Suomessa puolustusvoimien ja muiden valtiollisten laitosten käytössä oleva Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on yksi tällainen virallinen säännös. Tällaisten säännösten avulla määritellään kuinka organisaation pitäisi käsitellä informaatiota. (Rouse 2005.)

3 AMAZON EC2

Amazon Elastic Compute Cloud (EC2) tarjoaa skaalautuvaa prosessointi kapasiteettia Amazon Web Services (AWS) pilvipalvelussa.

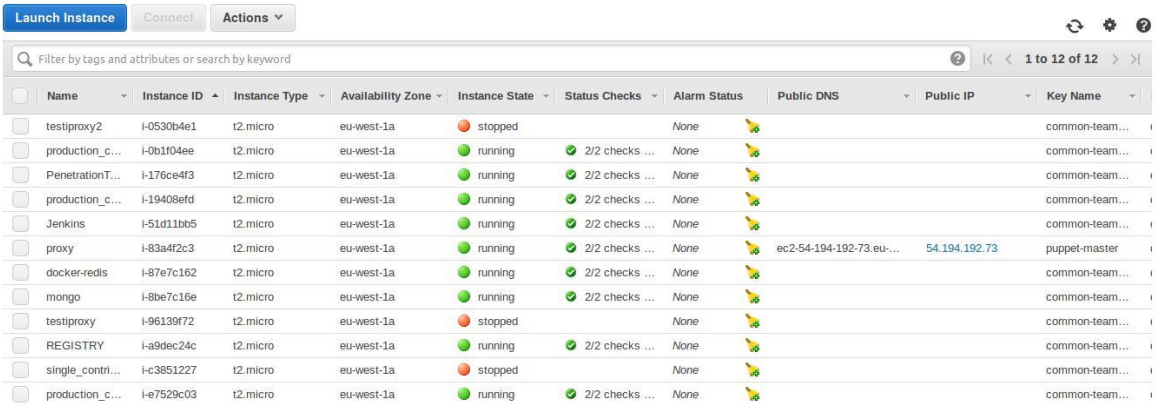
3.1.1 Käyttöliittymä

Kuviossa 13 nähdään Amazon EC2 pilvipalvelun ohjauspaneeli, josta nähdään palvelussa käytettävät resurssit ja palvelun terveys.



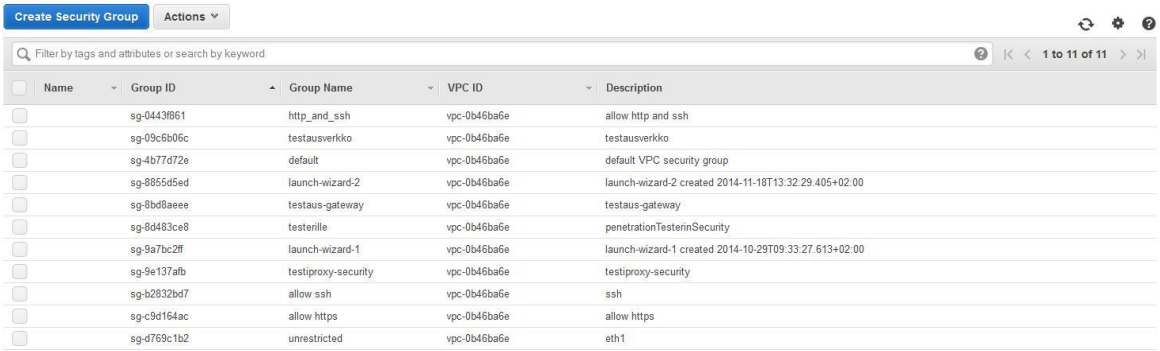
Kuvio 13. Amazon EC2-pilvipalvelun ohjauspaneeli

Kuviosta 14 nähdään N4SJAMKin käyttämät instanssit Amazon EC2 pilvipalvelussa. Instanssilla tarkoitetaan virtuaali tietokoneita ja jokainen instanssi toimii virtuaali yksityisenä palvelimena. Kun instanssi laukaistaan, instanssi tyyppi joka valitaan määrittää käytettävän isäntätietokoneen raudan. Joka instanssi tyyppi tarjoaa eri prosessointi, muisti ja tallennuskapasiteettia. Instanssi tyypin valinta pohjautuu ohjelmisto ja sovellus tarpeisiin. (Instance Types 2014.)



Kuvio 14. Instanssit

Kuviossa 15 nähdään N4SJAMKin käytössä olevat turvallisuusryhmät.



Kuvio 15. Turvallisuusryhmät

Turvallisuusyhmät toimivat virtuaalisina palomuurina jotka hallinnoivat yhden tai useamman instanssin liikennettä. Kun instanssi käynnistetään, yksi tai useampi turvallisuus ryhmä liitetään instanssiin. Sääntöjä lisätään jokaiseen turvallisuus ryhmään joka sallii liikennettä sisään tai ulos siihen liitetyistä instansseista. (Amazon EC2 Security Groups for Linux Instances 2014.)

Turvallisuusryhmän sääntöjä voidaan muuttaa milloin tahansa, muutetut säännöt asetetaan kaikille instansseille jotka ovat liitetty turvallisuus ryhmään. Kun päätetään sallitaanko liikenteen päästä instanssiin, arvioidaan säännöt kaikista turvallisuus ryhmistä jotka ovat liitettyinä instansseihin. (Amazon EC2 Security Groups for Linux Instances 2014.)

Turvallisuusryhmän säännöt kontrolloivat sisään tulevaa liikennettä joka sallitaan instansseille jotka ovat yhdistetty turvallisuus ryhmiin ja ulospäin liikennettä joka on sallittu lähteä. Oletuksena kaikki ulospäin liikenne on sallittu. (Amazon EC2 Security Groups for Linux Instances 2014.)

Sääntöjä voidaan lisätä tai poistaa milloin tahansa. Muutokset päivittyvät turvallisuusryhmiin pienen ajan kuluttua. Sääntöjä voidaan kopioida olemassa olevasta turvallisuusryhmästä uuteen turvallisuus ryhmään. EC2-classic palvelussa ei voi ulospäin liikenteen sääntöjä muuttaa. Turvallisuusryhmän säännöt ovat aina sallivia, kieltäviä sääntöjä ei voi luoda. (Amazon EC2 Security Groups for Linux Instances 2014.)

Joka sääntöä varten täytyy ilmoittaa seuraavat asiat:

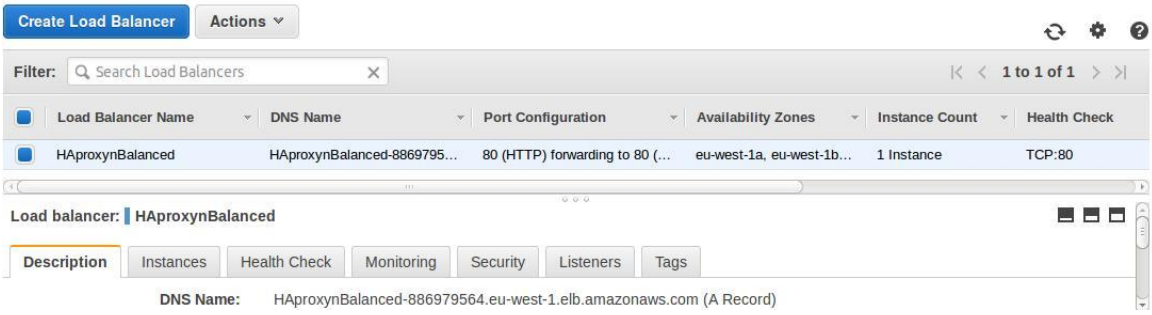
- Protokolla joka sallitaan (kuten TCP, UDP tai ICMP)
- TCP, UDP tai jokin muu protokolla: portti alueet
- ICMP: ICMP tyyppi ja koodi
- Yksi tai useampi seuraavista vaihtoehdoista lähteelle (sisäänpäin) ja päätepisteelle (ulospäin)
    - Yksittäinen IP osoite CIDR päätteellä
    - IP osoite avaruus CIDR päätteellä
    - Turvallisuusryhmän nimi (EC2-Classic) tai ID (EC2-Classic tai EC2-VPC). Tällä tavalla sallitaan instanssien jotka ovat yhteydessä määrättyyn turvallisuusryhmään keskustella muiden instanssien kanssa jotka ovat yhteydessä tähän turvallisuusryhmään. Yksi seuraavista turvallisuusryhmistä voidaan määrittää:
        - Nykyinen turvallisuusryhmä
        - EC2-Classic: eri turvallisuusryhmä EC2-Classic palvelulle samalla alueella
        - EC2-VPC: eri turvallisuusryhmä samalle VPClle
        - EC2-Classic: turvallisuusryhmä toiselle AWS tilille samalla alueella (Amazon EC2 Security Groups for Linux Instances 2014.)

Kuviosta 16 nähdään N4SJAMKin käytössä olevat elastiset IP osoitteet. Elastinen IP osoite on staattinen IP osoite joka on suunniteltu dynaamisiin pilvipalveluihin. Elastisella IP osoitteella voi piilottaa instanssin tai sovelluksen kaatumisen vaihtamalla osoitetta toiselle instanssille nopealla syklillä. Elastinen IP osoite on sidottu yhteen Amazon Web Services tiliin ja se pysyy voimassa ellei sitä vapauteta.

Kuvio 16. Elastiset IP osoitteet

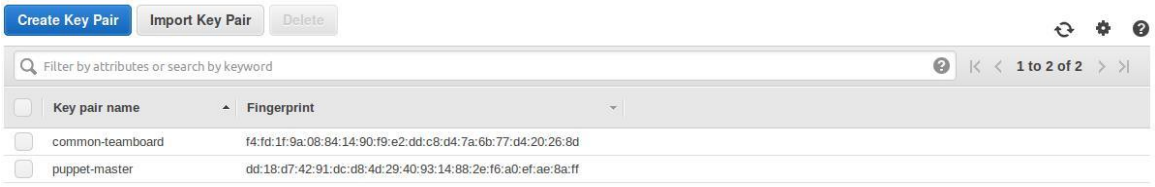
Oletuksena Amazon jakaa kaksi IP osoitetta, yksityisen ja julkisen IP osoitteen joka on sidottu yksityiseen osoitteeseen käyttäen Network Address Translationia (NAT). (Elastic IP Addresses (EIP) 2014)

Kuviosta 17 nähdään N4SJAMKin käytössä olevat kuorman tasaajat. Elastinen kuorman tasaus automaattisesti jakaa sisään tulevaa liikennettä useiden Amazon EC2 instanssien välillä pilvessä. Tämä sallii suuremman vikasietoisuuden sovelluksille, tällöin saadaan saumattomasti tarvittava määrä kuorman tasaus kapasiteettia jotta voidaan jakaa sovellus liikennettä. Elastinen kuorman tasaus toimii Amazon VPC palvelun kanssa tarjotakseen vankkaa verkostoitumista ja hyvät tietoturvaominaisuudet. (Elastic Load Balancing N,d)



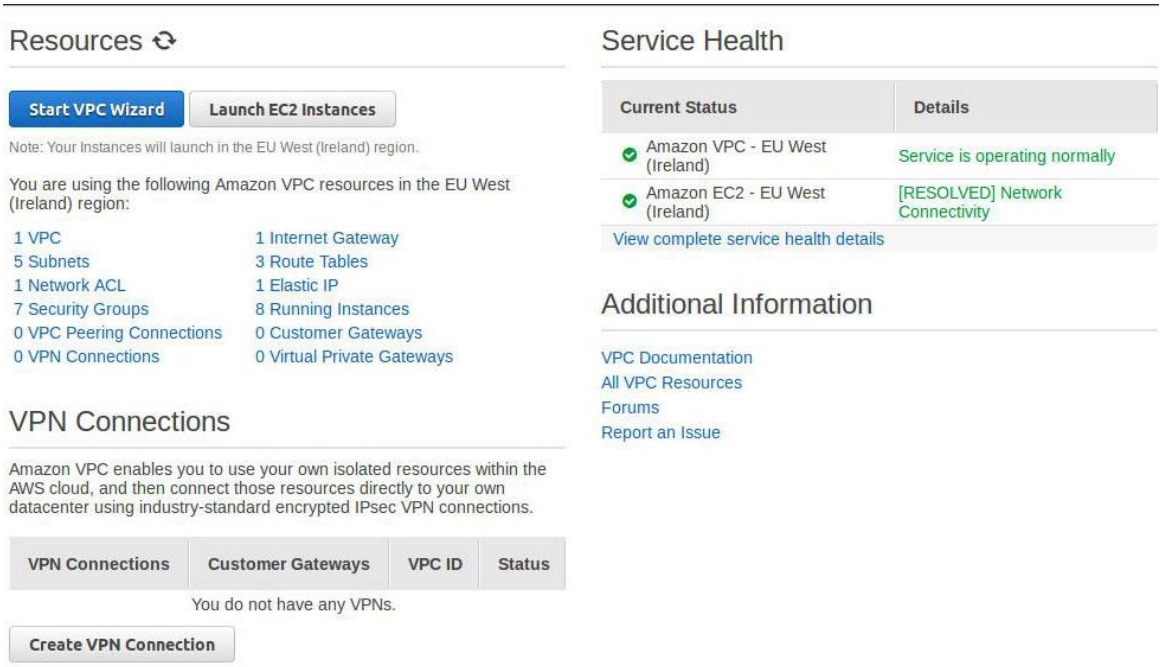
Kuvio 17. Kuorman tasaus

Kuviosta 18 nähdään N4SJAMKin käyttämät avain parit. Amazon EC2 käyttää avoin-avain kryptografiaa enkryptaamaan ja dekryptaamaan sisäänkirjautumis tietoja. Avoin-avain kryptografia käyttää avointa avainta enkryptaamaan dataa kuten salasanoja, sitten vastaanottaja käyttää yksityistä avainta dekryptaamaan dataa. Avointa ja yksityistä avainta kutsutaan avain pariksi. (Amazon EC2 Key Pairs 2014)



Kuvio 18. Avainparit

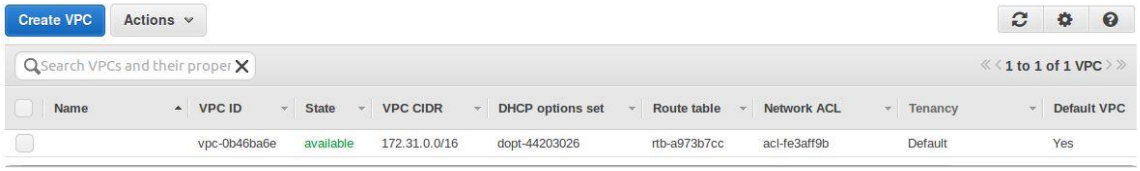
Kuviosta 19 nähdään VPC hallintapaneeli jossa näkyy yleiskuva käytössä olevista VPC resursseista.



Kuvio 19. VPC hallintapaneeli

Kuviosta 20 nähdään N4SJAMKin käytössä olevat VPCt. Amazon Virtual Private Cloud (VPC) sallii loogisesti eristetyn osion säännöstelyn Amazon Web Services (AWS) pilvessä jossa voidaan käynnistää AWS resursseja virtuaalisessa verkossa joka on käyttäjän määritettävissä. Käyttäjällä on täysi valta virtuaalisesta verkko ympäristöstä, kuten IP osoite

avaruuksien valinta, aliverkkojen luonti, reititystaulujen ja verkon yhdyskäytävien muokkaus ja hallinta. (Amazon VPC n. d.)



Kuvio 20. N4SJAMK VPC

3.1.2 Palvelutasosopimus

Nykyinen SLA sopimus on päivätty 1.6.2013. Sopimuksessa lukee että Amazon Web Services käyttää kaupallisesti kohtuullisia toimenpiteitä tehdäkseen Amazon EC2 ja Amazon EBS palvelut saataville kuukausittaisella ylläpito prosentilla joka on ainakin 99.95 %, kummassakin tapauksessa kuukausittaisen laskutus kauden aikana. Tapauksessa jossa Amazon EC2 tai Amazon EBS eivät vastaa palvelusitoumusta niin asiakas on oikeutettu saamaan palvelu hyvitystä kuten on alla mainittu.

Palvelu hyvitykset lasketaan prosentteina kaikista maksetuista kuluista Amazon EC2 tai Amazon EBS palveluista, alueella johon kuukausittainen laskutus kausi vaikuttaa jossa palvelun saavuttamattomuus tapahtuu alla olevan aikataulun mukaisesti. Taulukosta 1 nähdään Amazon EC2 pilvipalvelun SLA aikataulukko. (Amazon EC2 Service Level Agreement N,d.)

Taulukko 1. SLA-aikataulukko

Kuukausittainen päälläolo %	Palvelu hyvitys %
Alle 99.95 % mutta yhtä kuin tai enemmän kuin 99.0 %	10 %
Alle 99.0 %	30 %

4 TIETOTURVATESTAUS

4.1 Yleistä

Tietoturva testauksella varmistetaan että organisaation järjestelmät ja sovellukset eivät sisällä tietoturva aukkoja joista voi tulla isoja häviöitä rahallisesti tai datan muodossa. Minkä tahansa järjestelmän tietoturvan testauksen tarkoituksena on löytää kaikki aukot ja heikkoudet mitkä voivat aiheuttaa datan häviämistä työntekijöiden tai ulkopuolisten tekijöiden toimesta. (What is Security Testing? N,d.)

Tietoturvan testauksen päämäärä on tunnistaa järjestelmän uhkat ja mitata heikkoudet. Asiaa myös auttaa tunnistaa kaikki mahdolliset tietoturva riskit ja auttaa sovelluskehittäjiä ohjelmoinnin avulla. (What is Security Testing? N,d.)

4.2 Testausmenetelmät

Testaus menetelmiä on seitsemän Open Source Security Testing Methology Manualin (OSSTMM) mukaan. Tässä on nämä keinot listattuna:

- Haavoittuvuus skannaus
- Tietoturva skannaus
- Penetraatio testaus
- Riskien tunnistaminen
- Tietoturva auditointi
- Asento arviointi
- Eettinen hakkerointi

Haavoittuvuus skannaus suoritetaan automatisoidulla ohjelmistolla jolla tarkastetaan järjestelmä tunnettuja haavoittuvuus allekirjoituksien varalta. (What is Security Testing? N,d.)

Tietoturva skannauksessa tunnistetaan verkossa ja järjestelmässä heikkouksia ja myöhemmin tarjotaan keinoja näiden heikkouksien vähentämiseksi. Tämä skannaus voidaan suorittaa automaattisesti tai manuaalisesti. (What is Security Testing? N,d.)

Penetraatio testauksessa simuloidaan hyökkäys haitalliselta hakkerilta. Tämä testaus sisältää järjestelmän analyysin jossa tunnistetaan mahdolliset heikkoudet ulkoista hakkerointia vastaan. (What is Security Testing? N,d.)

Riskien tunnistamisen testauksessa suoritetaan analyysi uhkista organisaatiossa. Riskit luokitellaan seuraavasti: alhainen, keskitaso ja korkea. Testausta varten suositellaan valvontaa ja toimenpiteitä riskien vähentämistä varten. (What is Security Testing? N,d.)

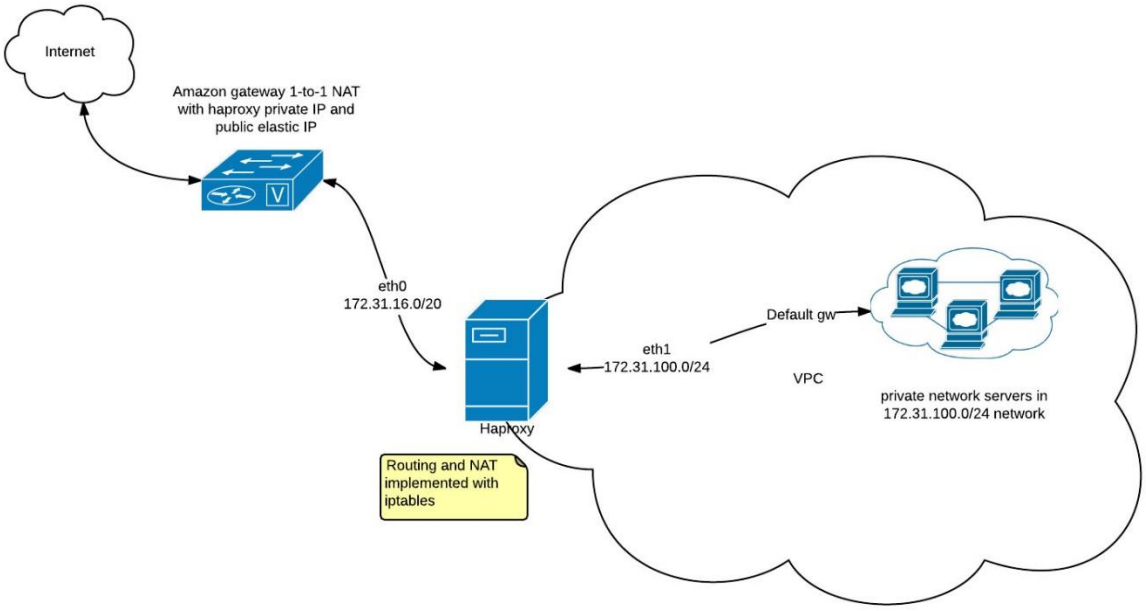
Tietoturva auditointi on sisäinen sovellusten ja käyttöjärjestelmien tarkistus tietoturva heikkouksien varalta. Auditointia voi olla myös koodin rivi riviltä tarkastamista. (What is Security Testing? N,d.)

Asento arviointi yhdistää tietoturva skannauksen, eettisen hakkeroinnin ja riskien tunnistamisen joiden avulla tarkastetaan organisaation kokonais tietoturva asento. (What is Security Testing? N,d.)

Eettinen hakkerointi on organisaation järjestelmien hakkerointia tarkoituksena tunnistaa järjestelmän viat toisin kuin haitalliset hakkerit jotka varastavat omiin tarkoituksiinsa. (What is Security Testing ? N,d.)

4.3 Amazon EC2 ympäristö

Kuviosta 21 nähdään yleiskuva N4SJAMKin ympäristöstä Amazon EC2 pilvipalvelussa.



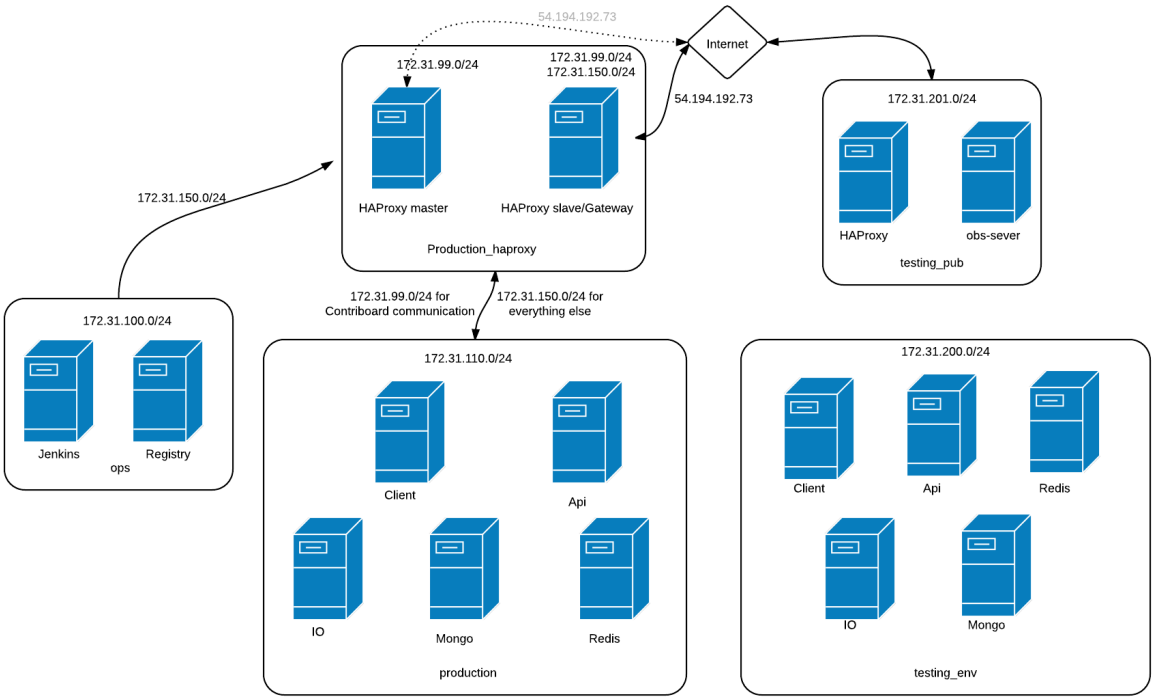
Kuvio 21. N4SJAMK Amazon EC2 ympäristö

4.4 Uusi verkon rakenne

Alustavien tietoturva testauksien aikana huomattiin epäkohtia kuten että sisäverkossa sallittiin periaatteessa kaikki liikenne Amazon tietoturvasäännöksissä. Laitteita kontrolloidaan ottamalla niihin SSH yhteys, joka oli tuolla hetkellä sallittu kaikkialta. Jenkins palvelin oli kaatumisen partaalla porttiskannauksen jälkeen koska liitännäisessä JmDNS oli bugi, jonka takia Jenkins keräsi yli neljän gigatavun verran loki tiedostoja. JmDNS on java implementaatio ryhmälähetys DNS:stä jota käytetään palvelun rekisteröintiin ja löytöön lähiverkossa.

Näiden syiden vuoksi Amazon EC2 verkko rakenne suunniteltiin uudelleen.

Kuviossa 22 nähdään uusi verkko rakenne.



Kuvio 22. Amazon EC2 uusi verkkorakenne

Verkon rakenteen uudistaminen selkeyttää palomuuri sääntöjen laatimista, koska tarvitaan säännöt vain eri alueiden välille, jolloin on helpompi rajata mitä sallitaan.

4.5 Amazon EC2 tietoturvatestaus lomake

Amazonin järjestelmiä ei saa noin vaan lähteä testaamaan vaan täytyy täyttää virallinen AWS Vulnerability / Penetration Testing Request Form. Lomakkeessa ilmoitetaan skannattavat IP osoitteet, laitteiden virtuaali tunnisteet, ovatko nämä virtuaali palvelimet skannauksen lähde vai vastaanottaja, skannauksen lähde osoite, missä alueella laitteet sijaitsevat sekä ajankohta milloin skannaus tapahtuu. Amazon sanoo että asiakkaalta ei vaadita mitään jatkotoimenpiteitä mutta jos huomaa testien lomassa bugeja järjestelmästä, ne täytyy ilmoittaa Amazonille. Ainoa asia jonka Amazon kieltää testauksissa on palvelunestohyökkäys. Amazonin mukaan pyyntöön vastataan 2-3 arkipäivässä.

N4SJAMKin Amazon EC2 ympäristössä jatkuva tietoturvatestaus ei ole mahdollista tämän lomakkeen odottamisen takia eikä ole tarpeellista sen vuoksi että järjestelmä on

tässä työssä jo testattu, joten tarvetta tarkastuksille on vain sellaisessa tapauksessa että järjestelmään lisätään laitteita tai rakennetta muutetaan.

Liitteessä 1 nähdään tietoturvatestaus lomakkeen sisältö.

4.6 Testaustyökalut ja niiden asennus

N4SJAMKin palvelimet sijaitsevat Amazon EC2 pilvipalvelussa joten näiden laitteiden testausta varten valittiin kaksi testaus ohjelmistoa jotka soveltuvat verkon välityksellä tapahtuvaan tietoturva testaukseen.

4.6.1 Nmap

Nmap (”Network Mapper”) on ilmainen ja avoimen lähdekoodin työkalu verkkojen löytöön ja tietoturva auditointiin. Monet järjestelmän- ja verkonvalvojat toteavat työkalun olevan hyödyllinen tehtävissä kuten verkon inventaario, palvelun päivitys aikataulun hallinnassa sekä laitteiden tai palvelun käytettävyyden monitoroinnissa.

Nmap käyttää käsittelemättömiä IP paketteja erilaisilla keinoilla joiden avulla selvitetään minkälaisia laitteita verkossa on, mitä palveluita (ohjelmien nimet ja versiot) nämä laitteet tarjoavat, mitä käyttöjärjestelmiä ja versioita laitteet käyttävät, minkälaisia paketti filttereitä/palomuureja on käytössä ja monia muita eri tietoja. Ohjelma on suunniteltu skannaamaan suuria verkkoja nopeasti mutta toimii myös hyvin yksittäisten laitteidenkin kanssa.

Nmap toimii kaikilla yleisimmillä käyttöjärjestelmillä ja viralliset binääri paketit ovat saatavilla Linuxille, Windowsille ja Mac OSXlle. (Introduction N,d.)

Nmap asennetaan käskyllä:

sudo apt-get install nmap

4.6.2 Nessus

Nessus on etä tietoturva skannaus työkalu, joka skannaa tietokoneen ja nostaa hälytyksen jos se löytää heikkouksia joita pahantahtoiset hakkerit voivat käyttää kaikkien tietokoneiden käsiksi pääsyyn verkossa. Ohjelma tekee näin ajamalla yli 1200 erilaista testiä tietokoneelle, joiden avulla selvitetään onko yksikään näistä hyökkäyksistä sellainen jonka avulla voidaan murtautua tietokoneelle ja vahingoittaa sitä. (Nessus : A security vulnerability scanning tool N,d.)

Nessuksen asennus Amazon EC2 verkon testausta varten tarvitsi lisätoimenpiteitä koska kuviossa 19 näkyvään production verkkoon luotiin testausta varten tietokone ja näitä tietokoneita voidaan hallita vain SSH yhteyden avulla. Ensin täytyy ottaa SSH yhteys Haproxy palvelimeen josta taas otetaan SSH yhteys haluttuun sisäverkon tietokoneeseen.

Nessuksen asennusta varten täytyy ladata asennus paketti osoitteesta:

http://www.tenable.com/products/nessus/select-your-operating-system

Nessuksen asennus täytyy suorittaa loppuun verkkoselaimessa jota kautta myös ohjelmaa käytetään. Asennuspaketti siirretään välityspalvelimelle komennolla:

scp -i puppet_master.pem ubuntu@54.194.71.219:/home/ubuntu/Nessus_6.3.2_ubuntu1110_amd64.deb

Tämän jälkeen mentiin välityspalvelimelle johon tiedosto siirrettiin josta tiedosto siirretään testi koneelle komennolla:

scp ubuntu@172.31.110.140:/home/ubuntu/Nessus_6.3.2_ubuntu1110_amd64.deb

Nessus asennetaan tiedostosta komennolla:

sudo dpkg -i Nessus_6.3.2_ubuntu1110_amd64.deb

Nessuksen ilmaisversiolla sallitaan ainoastaan yksityisten IP osoitteiden skannaus. Vaikka käytössä on ilmaisversio, ohjelma täytyy aktivoida koodilla jonka saa osoitteesta:

> *http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code*

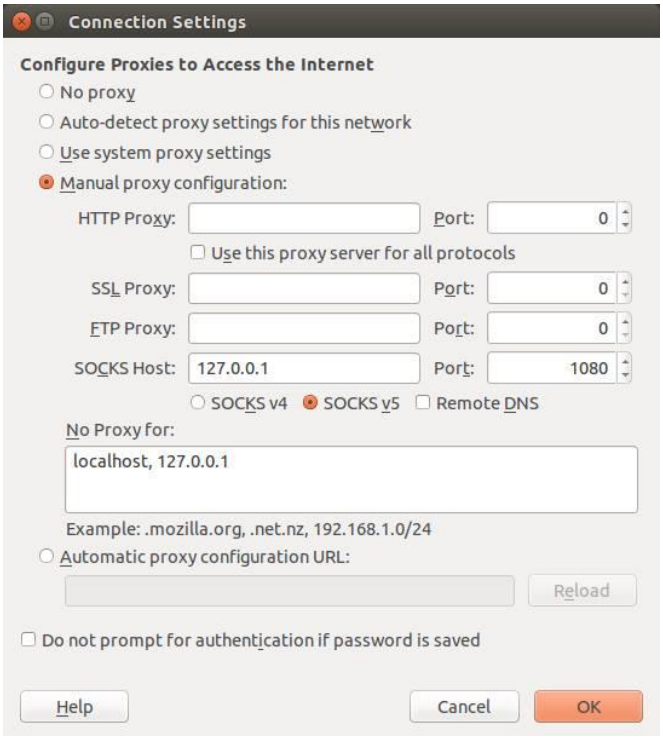
Koska ohjelmaa voidaan käyttää vain selaimen kautta, täytyy tehdä SSH tunneli. SSH tunneli on tunnelointi protokolla, jonka avulla päästään käsiksi verkko palveluun jota taustalla oleva verkko ei tue tai anna suoraan. Kuviossa 19 näkyvään Haproxy slave välityspalvelimeen tehtiin SSH tunneli kuviossa 23 näkyvällä komennolla.

```
joni@joni-System-Product-Name:~/Desktop$ ssh -i puppet-master.pem ubuntu@54.194.
71.219 -D 1080 -C
```

Kuvio 23. SSH tunnelin luominen

SSH yhteyden luonti aloitetaan komennolla ssh, -i puppet-master.pem ilmoittaa käytettävän yksityisen avaimen jota käytetään autentikointiin, ubuntu@54.194.71.219 ensin ilmoitetaan käyttäjä joka on olemassa vastaanottavassa palvelimessa ja @x.x.x.x kertoo mihin osoitteeseen yhteys otetaan, -D 1080 kertoo SSH tunnelissa käytettävän portin ja –C kertoo että yhteys kompressoidaan.

Kuviosta 24 nähdään selaimeen asetettavat välityspalvelimen asetukset.



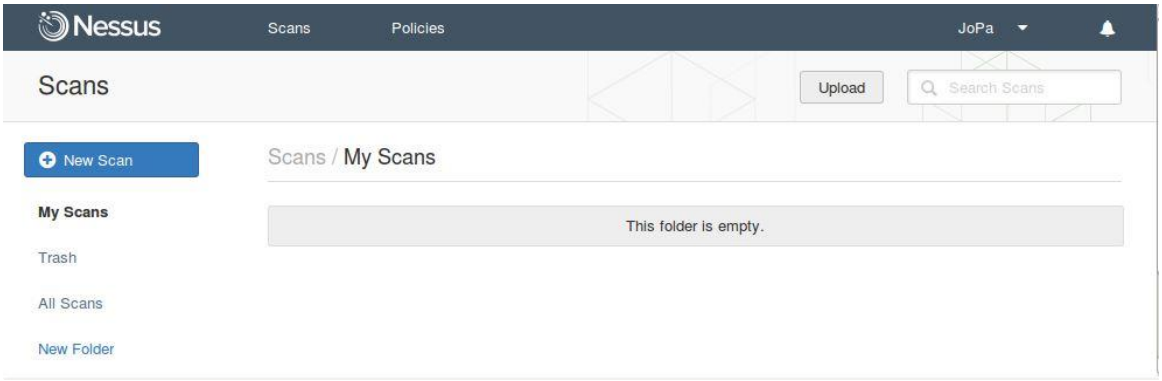
Kuvio 24. Selaimen välityspalvelin asetukset

Lopuksi siirrytään osoitteeseen:

https://172.31.110.140:8834/

Asennusta jatketaan painamalla continue, seuraavissa vaiheissa luodaan käyttäjä ohjelman käyttöä varten, syötetään aikaisemmin hankittu aktivointi koodi, annetaan ohjelman ladata päivitykset ja viimeisessä vaiheessa kirjaudutaan itse ohjelmaan.

Kuviosta 25 nähdään ohjelman käyttöliittymä.



Kuvio 25. Nessus-käyttöliittymä

5 TYÖN TOTEUTUS

5.1 Tietoturvatestaukset

Amazon EC2 verkossa sijaitsee yhdeksän laitetta joista kahdeksaa testattiin. Taulukossa 2 nähdään lista skannatuista laitteista.

Taulukko 2. Sisäverkon skannatut laitteet

IP osoite	Laitteen nimi
172.31.99.110	haproxy_master
172.31.99.234	haproxy_slave
172.31.100.102	REGISTRY
172.31.110.24	production_contriboard_client
172.31.110.70	production_redis
172.31.110.71	production_mongo
172.31.110.86	production_contriboard_io
172.31.110.125	production_contriboard_api

Jenkins palvelin jätettiin skannaamatta aikaisempien alustavien mittauksien perusteella. Kuviossa 19 näkyviä verkkoja testing_pub ja testing_env ei testauksien ajon aikana ollut luotuna vielä joten näitä verkkoja ei ole skannattu.

5.1.1 Nmap skannaukset

Tietoturva testauksissa Nmap ajettiin intense scan asetuksilla jossa muuttujat ovat -T4 –A –p ”*” -vv. – T muuttujalla ilmoitetaan ajoitus malli, –vv muuttuja vaikuttaa skannauksen tarkkuuteen, -p ”*” avulla skannataan kaikki avoimet portit ja –A muuttujalla selvitetään skannattavan kohteen käyttöjärjestelmä.

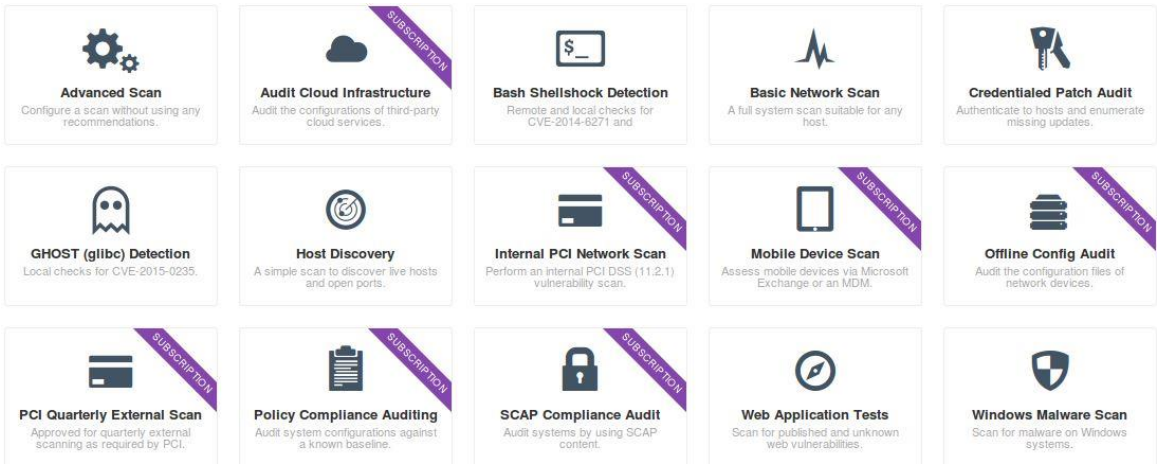
Liitteissä 2-4 nähdään sisäverkon laitteiden nmap skannauksen tulokset. Nmap skannausten perusteella voidaan sanoa että verkon laitteissa ei ole ylimääräisiä portteja auki. Production verkossa ei ole mitään portteja auki koska näihin laitteisiin voidaan muodostaa SSH yhteys vain Haproxy palvelimien kautta. Haproxy_master palvelimella on auki

portit 22, 80 ja 443 palvelun toimivuuden vuoksi, Haproxy_slave palvelimella on auki ainoastaan portti 22 koska tämä laite toimii porttikäytävänä. REGISTRY palvelimella on auki portti 22. Portti 22 on SSHn käytössä, portti 80 on HTTP (Hypertext Transfer Protocol) käytössä ja portti 443 on HTTPS (Hypertext Transfer Protocol over TLS/SSL) portti.

Nmap ei pysty tarkasti kertomaan mikä käyttöjärjestelmä skannatuissa laitteissa on käytössä, joka on tietoturvan kannalta hyvä asia.

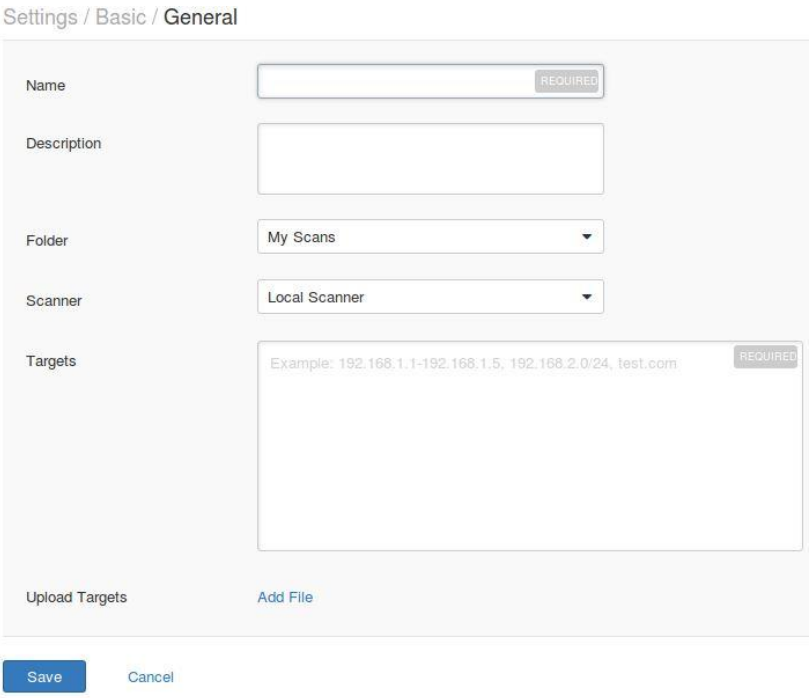
5.1.2 Nessus skannaukset

Kuviossa 26 nähdään Nessuksen ilmaisversion skannaus vaihtoehdot, violetilla merkityt skannaukset ovat käytössä vain maksullisessa versiossa.



Kuvio 26. Nessus-skannausvaihtoehdot

Nessus skannauksissa käytettiin ilmaisversiota ja skannauksena käytettiin Advanced scania. Kuviossa 27 nähdään advanced scan vaihtoehdot.



Kuvio 27. Advanced Scan

Liitteessä 5 nähdään sisäverkon laitteiden Nessus skannauksen tulokset. Production verkon laitteista ei löytynyt mitään aukkoja koska tietoturva säännöillä on estetty kaikki ylimääräiset portit. Haproxy_master palvelimesta löytyi viisi haavoittuvuutta, kolme näistä liittyvät SSL protokollan salaukseen ja ovat keskitason ja alhaisen tason haavoittuvuuksia ja kaksi alhaisen tason haavoittuvuutta jotka liittyvät SSHn käytössä oleviin salausavaimiin. Nämä kaksi alhaisen tason SSH haavoittuvuutta löytyivät myös Haproxy_slave ja REGISTRY palvelimista.

Keskitason haavoittuvuudet

Raportin mukaan välityspalvelin käyttää SSL (Secure Sockets Layer) liikenteen salausta joka on todettu vanhentuneeksi ja haavoittuvaiseksi. SSLn uusin versio on 3.0. Tästä johtuen N4SJAMKin välityspalvelin on haavoittuvainen mies välissä hyökkäykselle jota kutsutaan POODLE hyökkäykseksi. On suositeltavaa kytkeä SSL pois päältä ja korvata se TLS (Transport Layer Security) liikenteen salauksella.

TLS liikenteen salauksesta löytyy kolmea versiota: 1.0, 1.1 ja 1.2. Nämä kaikki sisältävät taaksepäin sopivuuden SSL protokollaan jotta voidaan taata toimiva käyttökokemus. TLS

kättelyssä tarjotaan korkeinta TLS versiota mutta jos tämä kättely epäonnistuu, niin yritetään vanhemmilla protokolla versioilla. Virheellisessä version neuvottelussa esimerkiksi asiakas laite tarjoaa TLS 1.2 versiota ja palvelin voi tarjota TLS 1.0 versiota, tämä version alennus voi tapahtua verkon ongelmien takia tai jos hyökkääjä pääsee vaikuttamaan verkkoon. Jos hyökkääjä joka pääsee hallitsemaan verkkoa joka on palvelimen ja asiakkaan välillä, vaikuttaa tähän versio kättelyyn jossa tarjotaan TLS 1.0 tai uudempaa versiota niin osapuolet tyytyvät käyttämään SSL 3.0 versiota. Yhteenvetona jos asiakkaan tai palvelimen puolelta kytketään SSL protokolla pois käytöstä, ollaan turvassa tältä hyökkäykseltä. Mutta jos jompikumpi osapuoli tukee vain SSL 3.0 versiota, niin silloin haavoittuvuus on olemassa. (Möller, Duong & Kotowicz 2014, 1-3.)

Mongo palvelimessa havaittiin haavoittuvuus MongoDB Service Without Authentication Detection, joka johtui toimeksiantajan mukaan uuteen versioon siirtymisen johdosta. Tämän haavoittuvuuden korjaa toimeksiantaja.

Alhaisen tason haavoittuvuus 1

Nessus ilmoittaa alhaisen tason haavoittuvuuden otsikoksi SSL RC4 Cipher Suites Supported. Tämä tarkoittaa että etäpalvelu tukee RC4 enkryptaus algoritmiä joka koetaan haavoittuvaiseksi. Tämän haavoittuvuuden korjaamiseksi suositellaan palvelun konfigurointia RC4 enkryptauksen välttämiseksi ja TLS 1.2 liikenteen salausta AES (Advanced Encryption Standard)-GCM (Galois/Counter Mode) enkryptauksen kanssa.

Alhaisen tason haavoittuvuus 2

SSH palvelin on konfiguroitu tukemaan CBC (Cipher Block Chaining) enkryptausta. Tämä voi sallia hyökkääjän noutavan selkoteksti viestin salatekstistä. Ratkaisuna tämän korjaamiseksi on CBC enkryptauksen poisto käytöstä ja tilalle CTR (Counter) tai GCM enkryptaus menetelmä.

Alhaisen tason haavoittuvuus 3

SSH palvelin on konfiguroitu sallimaan MD5 ja 96-bit MAC (Message Authentication Code) algoritmejä. Molempia pidetään heikkoina ja käyttöä ei suositella. Suosituksena on että kummatkin otetaan pois käytöstä.

5.2 Korjaustoimenpiteet

Kaikki havaitut haavoittuvuudet korjataan muokkaamalla Amazon EC2 tietoturva sääntöjä, ssh_config ja sshd_config tiedostoja sekä haproxy.cfg tiedostoa haproxy palvelimilla.

ssh_config ja sshd_config tiedostojen muokkaus

ssh_config tiedostosta löytyy rivit joissa lukee: # Ciphers ja # MACs. Haavoittuvuuksien estämiseksi muokataan näitä rivejä. Rivit on kommentoitu ssh_config tiedostossa # merkillä, tämä täytyy poistaa. Samat Ciphers ja MACs rivit täytyy olla myös sshd_config tiedostossa.

Korvataan Ciphers rivillä olevat salausavaimet seuraavilla:

> *aes128-ctr, aes192-ctr,aes256-ctr,arcfour256,arcfour128, aes128-gcm@openssh.com,aes256-gcm@openssh.com, chacha20-poly1305@openssh.com,arcfour*

Korvataan MACs rivillä olevat seuraavilla:

> *hmac-sha1-etm@openssh.com, umac-64-etm@openssh.com,umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com, hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com, hmac-sha2-256,hmac-sha2-512,hmac-ripemd160, hmac-sha1-96,hmac-md5-96, hmac-md5-etm@openssh.com*

Riveillä olevat salausavaimet ovat tärkeysjärjestyksessä sen mukaan mikä on ensimmäisenä. Näiden toimenpiteiden jälkeen käynnistetään ssh palvelu komennolla:

sudo service sshd restart

Käynnissä olevat ssh yhteydet eivät katkea mutta käyttävät ennen muokkauksia käytettyjä salausavaimia. Kun käyttäjä ottaa ssh yhteyden muokkauksien jälkeen niin käytetään asetettuja avaimia.

Haproxy.cfg muokkaus

Keino tämän mies keskellä hyökkäyksen estämiseksi on SSLv3 pois käytöstä ottaminen ja laittaa lista sallituista salausavaimista ja menetelmistä Haproxyn konfigurointi tiedostoon. Ubuntu käyttöjärjestelmässä etsitään seuraava tiedosto ja avataan se omalla tiedostonmuokkausohjelmalla. Tässä tapauksessa tiedoston avaaminen onnistuu seuraavalla komennolla

sudo nano /etc/haproxy.cfg

N4SJAMKin välityspalvelin käyttää ohjelmistoa jonka nimi on Haproxy ja ohjelman tarkoituksena on kuorman tasaus sekä TCP ja HTTP käyttöön välityspalvelimena toimiminen.

Etsitään tiedostosta rivi jossa lukee bind ja viitataan porttiin 443 (SSL).

Esimerkki rivistä:

bind :443 ssl crt <crt> no-sslv3 ciphers EECDH+ECDSA+AES-GCM:EECDH+aRSA+AES-GCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4

Tässä rivissä ssl crt kertoo että käytetään sertifikaattia, <crt> kohdassa kerrotaan sertifikaatin sijainti ja nimi, no-sslv3 kertoo että ei sallita SSLv3 salausta ja ciphers kohdassa kerrotaan mitä salauksia sallitaan. (Russel 2014.)

Kuviosta 28 nähdään miten kyseisessä tapauksessa SSLv3 on otettu pois käytöstä.

```
frontend all_ssl
    bind :443 ssl crt /etc/haproxy/n4sjamk.org_bundle.pem no-sslv3
    reqadd X-Forwarded-Proto:\ https
```

Kuvio 28. Haproxy sslv3:n käytöstä poisto

Tiedoston muokkauksen jälkeen palvelu täytyy käynnistää uudelleen joka onnistuu komennolla:

sudo service haproxy restart

Amazon EC2 tietoturvasäännöt

Taulukosta 3 nähdään production haproxy verkossa käytössä olevat tietoturvaryhmä säännöt.

Taulukko 3. Production_haproxy säännöt

111_production_haproxy				
Type	**Protocol**	**Port Range**	**Source**	**Description**
SSH	TCP	22	172.31.150.0/24	Management rule
HTTP	TCP	80	0.0.0.0/24	http from any
HTTPS	TCP	443	0.0.0.0/24	https from any
All UDP	UDP	0 - 65535	172.31.99.0/24	Keepalived

Production_haproxy säännöissä sallitaan SSH portti joka hallinta käytössä. HTTP ja HTTPS portit sallitaan kaikkialta jotta Contriboardia voidaan käyttää verkon välityksellä. Keepalivedia varten on kaikki avoinna kaikki UDP portit jotka ovat välillä 0-65535, keepalived on reititys ohjelmisto. Sillä suoritetaan kuorman tasausta kuten haproxyllä, keepalived on asennettu molemmille haproxy palvelimelle jossa se tarkkailee että nämä palvelimet pysyvät pystyssä ja jos toinen näistä palvelimista häviää verkosta niin se osaa ottaa toisen haproxy palvelimen osoitteet käyttöön ja jatkaa toimintaa ilman palvelun katkeamista.

Taulukosta 4 nähdään yhdyskäytävä verkon säännöt.

Taulukko 4. Yhdyskäytävä säännöt

111_gateway				
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/24	SSH from any
All Traffic	TCP	All	172.31.0.0/16	Gateway rule

Gateway säännöksissä on sallittu SSH portti kaikkialta ja kaikki liikenne sisäverkosta on sallittu yhdyskäytävän suuntaan.

Taulukosta 5 nähdään production verkossa käytössä olevat säännöt.

Taulukko 5. Production säännöt

111_production				
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	172.31.150.0/24	Management rule
Custom	TCP	6379	172.31.110.0/24	Redis
Custom	TCP	27017	172.31.110.0/24	Mongodb
Custom	TCP	9001-9002	172.31.99.0/24	API & IO
HTTP	TCP	80	172.31.99.0/24	Client
Custom	TCP	8080	172.31.99.0/24	New Client

Production säännöissä on sallittu SSH portti yhdyskäytävästä joka löytyy verkosta 172.31.150.0/24. Portit 6379 ja 27017 ovat sallittu production verkosta. Portit 9001–9002, 80 ja 8080 ovat sallittu haproxy verkosta.

Taulukosta 6 nähdään ops verkossa olevat säännöt.

Taulukko 6. Ops säännöt

111_ops				
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	172.31.150.0/24	Management rule
Custom	TCP	5000	172.31.110.0/24	Registry
Custom	TCP	5000	172.31.100.0/24	Registry
Custom	TCP	5000	172.31.200.0/24	Registry

SSH portti on sallittu yhdyskäytävä verkosta, portti 5000 on sallittu production, ops ja testing_env verkosta.

5.3 Korjausten jälkeiset testaukset

Nmap skannauksissa ei löydetty ylimääräisiä portteja skannatuista laitteista joten päätettiin että korjausten jälkeen ei nmap skannauksia enää suoritettaisi laitteisiin.

Production verkon laitteista ei ensimmäisessä Nessus skannauksessa löydetty tietoturva haavoittuvuuksia joten niiden skannausta ei korjausten jälkeen suoritettu. Haproxy_master, haproxy_slave ja REGISTRY palvelimet skannattiin korjausten jälkeen uudelleen ja näiden skannausten tulokset löytyvät liitteestä 6.

Korjausten jälkeisten testauksien tulosten perusteella voidaan sanoa että suoritetut korjaukset toimivat koska aikaisemmin havaittuja tietoturva haavoittuvuuksia ei löydetty.

5.4 Yhteenveto

5.4.1 Testauksissa ja korjauksissa huomioon otettavia asioita

Testauksista

Nessuksen ilmaisversiolla sallitaan vain yksityisosoitteiden skannaaminen.

Jotkin palvelin komponentit eivät pidä portti skannauksista, kuten aiemmin mainittu Jenkins palvelin joka keräsi portti skannauksen jälkeen neljä gigatavua loki tiedostoja jumittaen koko laitteen.

Amazon EC2 ympäristöä saa testata vasta sen jälkeen että on saanut vastauksen tietoturvalomakkeeseen.

Korjauksista

Joka kerta kun muutetaan laitteiden asetuksia, niin olisi hyvä ottaa varmuuskopiot talteen.

5.4.2 Suositukset jatkossa

Viimeisenä suosittelisin N4SJAMKille laitteiden tietoturvan testausta jos ja kun verkon rakennetta muutetaan jolloin myös Amazon EC2 palvelun tietoturva säännöksiä muutetaan. Mutta loppupelissä tietoturvatestauksien ajo jää N4SJAMKin henkilöstön harkinnan varalle.

6 POHDINTA

Tavoitteet

Työn tavoitteena oli kartoittaa palvelimien tietoturva, testata tietoturvaa, kehittää palvelimien tietoturvaa sekä tutkia Amazon EC2 pilvipalvelun osa-alueet liittyen tietoturvaan.

Kirjoittaminen

Teorian kirjoittaminen onnistui hyvin, koska tietoturva on viime vuosien aikana tullut enemmän puheeksi joten myös materiaalia löytyy paljon. Ensin tutkittiin niin sanottua normaalia tietoturvaa jota sovelletaan paikallisiin eli omissa tiloissa oleviin laitteisiin, ku-

ten verkkolaitteisiin ja tietokoneisiin. Tietoturvan soveltaminen pilvipalveluihin oli tekijälle uutta asiaa joten näiden keinojen tutkiminen ja näistä oppiminen oli mielenkiintoista.

Tietoturva testauksen teorian kirjoittamiseen löytyi paljon materiaalia internetistä joten kirjoittaminen onnistui hyvin. Alustavasti tietoturva testausta varten valittiin toimeksiantajan ehdotuksesta F-Securen mittn joka on sarja tietoturvatestaus työkaluja. Tarkemmin tutkittuna mittn sisälsi maksullisia ohjelmistoja ja testauksissa haluttiin käyttää ilmaisia työkaluja, jotten mittn unohdettiin tässä vaiheessa.

Työn teko

Ilmaisten tietoturvatestaus ohjelmistojen valinnassa ei kauaa käytetty aikaa koska kirjoittaja oli nmapia aikaisemmin käyttänyt ja Nessus valittiin toiseksi testaus työkaluksi työn ohjaajan suosittelun perusteella. Tietoturva testaukset sujuivat muuten hyvin mutta joka kerta kun Amazon EC2 ympäristö halutaan testata, täytyy lähettää työssä mainittu penetraatiotestaus pyyntö lomake josta vastauksen saa 2-3 päivässä. Tämä hidasti työn tekoa koska työn teon aikana oli taukoja tämän odottamisen vuoksi, hidastuksia myös tuotti se että N4SJAMK muutti Amazon EC2 verkon rakennetta jonka seurauksena täytyi odottaa lisää ja suorittaa testauksia taas uudelleen. Itse testaukset sujuivat hyvin koska ohjelmat olivat helppo käyttöisiä ja ohjelmien tulosteet olivat helposti tulkittavissa. Tietoturva korjauksien suorittaminen onnistui todella hyvin koska löydetyt haavoittuvuudet olivat tunnettuja ja näihin löytyi korjaus menetelmät nopeasti.

Tulokset

Lähtötilanteessa Amazon EC2 verkossa sallittiin periaatteessa kaikki liikenne. Alustavien tietoturvatestauksien ja huomioiden perusteella verkon rakennetta ja Amazon EC2 tietoturvasäännöksiä muutettiin.

Laitteista löydettiin keskitason ja alhaisen tason haavoittuvuuksia. Nämä haavoittuvuudet olivat tunnettuja joten myös korjaustoimenpiteet oli helppo löytää.

Kaikki löydetyt haavoittuvuudet saatiin korjattua.

Tulosten luotettavuus

Testikone sijaitsi production verkossa josta skannattiin kaikki testattavat laitteet, tarkimmat tulokset olisi saatu jos testikone sijoitetaan jokaiseen aliverkkoon mutta tätä ei nähty tarpeelliseksi. Nessuksen liitännäiset päivitetään joka päivä, Nessus käyttää yli 60000 erilaista liitännäistä. SSL todettiin haavoittuvaiseksi 2014, tämä nähdään myös Nessuksen skannaus tuloksista. Haavoittuvuuksia jotka löydettiin ennen korjaustoimenpiteitä, ei löydetty enää korjausten jälkeen.

Näiden tietojen perusteella arvioin että tulokset ovat luotettavia ja tarkkoja.

Hyöty

Alustavana kysymyksenä toimeksiantajalla oli että missä kunnossa meidän järjestelmien tietoturva on Amazon EC2 pilvipalvelussa. Voidaan sanoa että tähän kysymykseen on vastattu ja työn tuloksia voidaan tulevaisuudessa käyttää jos ollaan suorittamassa tietoturvatestauksia pilvipalvelussa. Työstä myös nähdään se että jos testataan sisäverkkoja pilvipalvelussa, kuinka käytetään esim. Nessusta tässä tapauksessa (SSH-tunneli).

Lopputulos

Lopputuloksena voidaan sanoa että työn tavoitteissa onnistuttiin. Järjestelmästä tehtiin tietoturvallinen laitteiden ja verkon osalta. Työn teko oli miellyttävää koska aihe oli mielenkiintoinen ja teon aikana oppi uutta tietoturvasta, pilvipalveluista ja Amazon EC2 pilvipalvelusta.

LÄHTEET

About the product. 2014. Viitattu 28.3.2015. https://github.com/N4SJAMK/teamboard-meta/wiki/about-product

Amazon EC2 Key Pairs. 2014. Artikkeli Amazonin sivustolla. Viitattu 13.2015. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

Amazon EC2 Security Groups for Linux Instances. 2014. Artikkeli Amazonin sivustolla. Viitattu 9.2.2015. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

Amazon EC2 Service Level Agreement. N. d. Artikkeli Amazonin sivustolla. Viitattu 13.2.2015. http://aws.amazon.com/ec2/sla/

Amazon VPC. N. d. Artikkeli Amazonin sivustolla. Viitattu 13.2.2015. http://aws.amazon.com/vpc/

Elastic IP Addresses (EIP). 2014. Artikkeli Amazonin sivustolla. Viitattu 13.2.2015. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

Elastic Load Balancing. N. d. Artikkeli Amazonin sivustolla. Viitattu 13.2.2015. http://aws.amazon.com/elasticloadbalancing/

Goodin, D. 2012. Virtual machine used to steal crypto keys from other VM on same server. Viitattu 29.1.2015. http://arstechnica.com/security/2012/11/crypto-keys-stolen-from-virtual-machine/

Griffith, E. 2013. What Is Cloud Computing? Viitattu 28.1.2015. http://www.pcmag.com/article2/0,2817,2372163,00.asp

Hemmings, K. 2012. 3 Types of Cloud Service Models. Viitattu 28.1.2015. http://blog.appcore.com/blog/bid/168247/3-Types-of-Cloud-Service-Models

Instance Types. 2014. Artikkeli Amazon sivustolla. Viitattu 13.2.2015. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html

Introduction. N. d. Kuvaus nmap sivustolla. Viitattu 18.2.2015. http://nmap.org/

Janssen, C. N. d. Information Security (IS). Viitattu 4.2.2015. http://www.techopedia.com/definition/10282/information-security-is

Mahadik, K. 2013. PLM in the Cloud: Computer System Validation in FDA Regulated Industries. Viitattu 28.1.2015. https://www.spkaa.com/plm-in-the-cloud-computer-system-validation-in-fda-regulated-industries

Mell, P & Grance, T. 2011. The NIST definition of Cloud Computing. Viitattu 28.1.2015. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Möller, B, Duong, T & Kotowicz, K. 2014. This POODLE Bites: Exploiting The SSL 3.0 Fallback. Viitattu 26.2.2015. https://www.openssl.org/~bodo/ssl-poodle.pdf

N4S-Ohjelma. 2014. Artikkeli Digilen N4S sivuilla. Viitattu 27.1.2015. http://www.n4s.fi/fi/

Nessus : A security vulnerability scanning tool. N. d. Artikkeli cs.emu.edu sivustolla. Viitattu 18.2.2015. http://www.cs.cmu.edu/~dwendlan/personal/nessus.html

Pilvipalveluiden tietoturvasta yritysjohdolle. 2010. Artikkeli Nixu Oyj:n sivuilla. Viitattu 31.1.2015. http://www.nixu.com/fi/julkaisut/pilvipalvelujen-tietoturvallisuudesta

Rouse, M. 2005. Security audit. Viitattu 4.2.2015. http://searchcio.techtarget.com/definition/security-audit

Russell, D. 2014. Disabling SSLv3 for POODLE. Viitattu 2.3.2015. https://www.linode.com/docs/security/security-patches/disabling-sslv3-for-poodle

Saba, M. 2014. SSH – weak ciphers and mac algorithms. Viitattu 2.3.2015. http://linux.uits.uconn.edu/gms02004/2014/06/25/ssh-weak-ciphers-and-mac-algorithms/

Samson, T. 2013. 9 top threats to cloud computing security. Viitattu 29.1.2015. http://www.infoworld.com/article/2613560/cloud-security/9-top-threats-to-cloud-computing-security.html

Sukhraj, S. 2013. What is Cloud Computing? Viitattu 31.1.2015. http://thegadgetsquare.com/1552/what-is-cloud-computing/

Suojausmenetelmät. N. d. Artikkeli Suomen internetopas-sivustolla. Viitattu 4.2.2015. http://www.internetopas.com/yleistietoa/tietoturva/suojausmenetelmat/

Tietotekniikan käyttö yrityksissä 2014. 2014. Artikkeli Tilastokeskuksen sivuilla. Viitattu 28.1.2015. http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_kat_003_fi.html

Vedenoja, J. 2007. Yrityksen fyysinen tietoturva. Viitattu 4.2.2015. https://www.theseus.fi/bitstream/handle/10024/11928/2007-12-03-18.pdf?sequence=1

What are Deployment Models in Cloud Computing? N. d. Artikkeli Cloud Competance Centerin sivuilla. Viitattu 31.1.2015. http://www.cloud-competence-center.com/understanding/cloud-computing-deployment-models/

What is Security Testing ? N. d. Artikkeli guru99 sivustolla. Viitattu 13.2.2015. http://www.guru99.com/what-is-security-testing.html

Väistö, H. 2005. Hallinnollinen tietoturvallisuus. Viitattu 2.3.2005. http://www2.amk.fi/digma.fi/www.amk.fi/material/attachments/van-haamk/etuotanto/041005/5h2DTrXIx/Hallinnollinen_tietoturva.pdf

LIITTEET

Liite 1. Amazon EC2 tietoturvatestaus lomake

AWS Vulnerability / Penetration Testing Request Form

In order to request permission to conduct vulnerability and penetration testing on instances in the AWS cloud, the following information is required. The requesting party must also accept the Terms and Conditions and AWS's policy regarding the Use of Security Assessment Tools and Services. Upon receipt and validation of the information, an authorization email approving the test plan will be sent to the addresses provided below. Testing is not authorized until the requesting party receives that authorization.

Contact Information

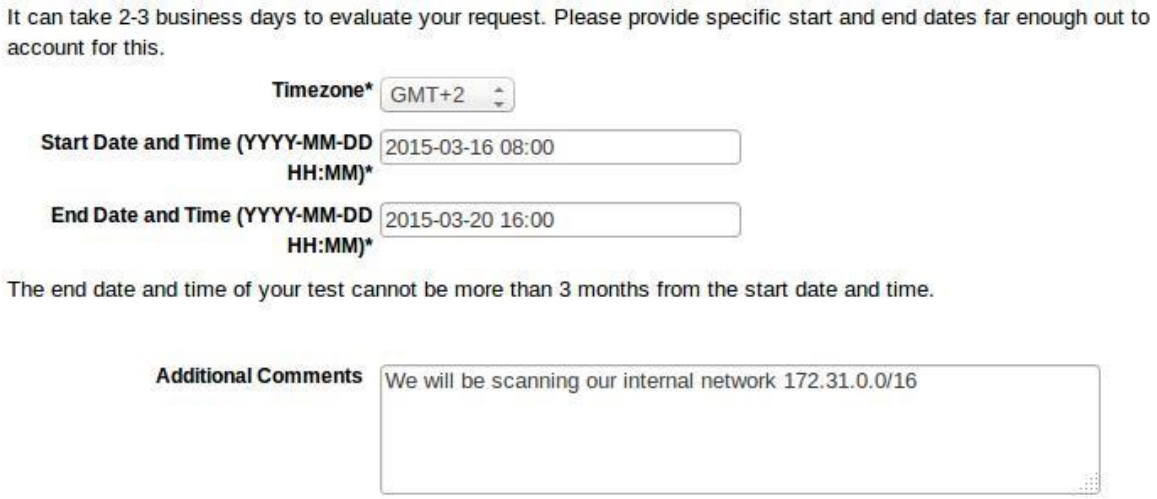
The following contains the email address and the associated AWS account number with which you have logged into the portal. If this information is incorrect, then you must log out and log back in with the account for which you want to test.

Your Name*	Jarmo Viinikanoja
Your Company Name	n4s@jamk
Your Email Address*	n4sjamk@gmail.com
AWS Account Number*	372449744733
Additional email addresses to CC on correspondence	
Third Party Contact Information	If you will have a third party performing the test, please provide the Company Name, Your Contact at the Company, Phone and Email address.

Scan Information

Note that only one region per form submission is allowed.

IP Addresses to be scanned (Destination)*	172.31.0.0/16
Are the instances the source of the scan or the target of the scan?*	☑ Source ☑ Target
Instances IDs*	i-060d61e2 i-1e0d61fa i-2ab1d3ce i-2dfb9bc9 i-30fb9bd4
Scanning IP addresses (Source)*	172.31.110.140
What region are these instances in?*	EU West (Ireland)



Liite 2. Production verkon nmap skannaus

Nmap 6.40 scan initiated Mon Mar 16 10:50:21 2015 as: nmap -oN test1_production.txt -T4 -A -p * -vv 172.31.110.24,70,71,86,125
Nmap scan report for ip-172-31-110-24.eu-west-1.compute.internal (172.31.110.24)
Host is up (0.00036s latency).
All 4243 scanned ports on ip-172-31-110-24.eu-west-1.compute.internal (172.31.110.24) are filtered
MAC Address: 02:6F:B8:B1:AB:95 (Unknown)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.40%E=4%D=3/16%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=026FB8%TM=5506B71C%P=x86_64-pc-linux-gnu)
U1(R=N)
IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.36 ms ip-172-31-110-24.eu-west-1.compute.internal (172.31.110.24)

Nmap scan report for ip-172-31-110-70.eu-west-1.compute.internal (172.31.110.70)
Host is up (0.00035s latency).
All 4243 scanned ports on ip-172-31-110-70.eu-west-1.compute.internal (172.31.110.70) are filtered
MAC Address: 02:52:1A:49:C2:35 (Unknown)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:

SCAN(V=6.40%E=4%D=3/16%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=02521A%T
M=5506B71C%P=x86_64-pc-linux-gnu)
U1(R=N)
IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.35 ms ip-172-31-110-70.eu-west-1.compute.internal (172.31.110.70)

Nmap scan report for ip-172-31-110-71.eu-west-1.compute.internal (172.31.110.71)
Host is up (0.00034s latency).
All 4243 scanned ports on ip-172-31-110-71.eu-west-1.compute.internal (172.31.110.71)
are filtered
MAC Address: 02:F4:34:3F:27:46 (Unknown)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.40%E=4%D=3/16%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=02F434%T
M=5506B71C%P=x86_64-pc-linux-gnu)
U1(R=N)
IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.34 ms ip-172-31-110-71.eu-west-1.compute.internal (172.31.110.71)

Nmap scan report for ip-172-31-110-86.eu-west-1.compute.internal (172.31.110.86)
Host is up (0.00034s latency).
All 4243 scanned ports on ip-172-31-110-86.eu-west-1.compute.internal (172.31.110.86)
are filtered
MAC Address: 02:5F:8B:AA:42:A8 (Unknown)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.40%E=4%D=3/16%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=025F8B%T
M=5506B71C%P=x86_64-pc-linux-gnu)
U1(R=N)
IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS

1 0.34 ms ip-172-31-110-86.eu-west-1.compute.internal (172.31.110.86)

Nmap scan report for ip-172-31-110-125.eu-west-1.compute.internal (172.31.110.125)
Host is up (0.00034s latency).
All 4243 scanned ports on ip-172-31-110-125.eu-west-1.compute.internal (172.31.110.125) are filtered
MAC Address: 02:00:F7:74:61:FF (Unknown)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.40%E=4%D=3/16%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=0200F7%TM=5506B71C%P=x86_64-pc-linux-gnu)
U1(R=N)
IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.34 ms ip-172-31-110-125.eu-west-1.compute.internal (172.31.110.125)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done at Mon Mar 16 10:57:32 2015 -- 5 IP addresses (5 hosts up) scanned in 430.83 seconds

Liite 3. Haproxy master ja slave palvelimien nmap skannaus

Nmap 6.40 scan initiated Mon Mar 16 10:37:34 2015 as: nmap -oN test1_haproxymaster1.txt -T4 -A -p * -vv 172.31.99.110
Nmap scan report for ip-172-31-99-110.eu-west-1.compute.internal (172.31.99.110)
Host is up (0.00080s latency).
Scanned at 2015-03-16 10:37:34 UTC for 47s
Not shown: 4239 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh (protocol 2.0)
| ssh-hostkey: 1024 ae:27:15:73:2b:48:34:20:18:93:85:b8:ce:8e:a1:07 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAAC-
BAN8kzWBFgbu30cBxWp7f5mq9b1T5N8CShAxzQfJLgjb06yf3TYiTgDDKLSR-
biXdW2bCBBpAQtZhSgwhpippUqeL2M8supNoY0czMU8WxCQowu-
xYCBq48o9EKyOPVP2f/90ZvTMevPw3E+kXDSF/NUPK+a2wp7V+jZXE-

qXsp6X1I7AAAAFQCW4vbFDq4ZYr6Rk2CIemAsY0h08wAAAIBfsmlMsKi+MjnF8cYS-
lRLkB9NJl9S51ITDS6/fDx6qJ3DIbhnwnQ6xFk2q1quR06z4Rt+Yj/Nji99Vb3iFJJ467/BofkOZS
F0qRHTGUOvlAoi10vS5tCK06w3F/OUHoG6KOMZDPTgXVWNtPIkvcW29FMvRsDi3dIIp-
ZvQEsrJpfQAAAIB5EIlt9g6CCLn+rUqmMCrqP5d8RXRaDXZcR6AINa5QJgPY-
wFy76W6odXz0WrD55fZLXgxyBnu9/+eyc+Sr99r90ZL/4LlWBF8Asj/Msui5Lcp1hGl0trN+oo
tgYElrhHxHOO5TZr3DQ7Qi6ITdvmtA9HrGYnxmUGfq9emWezSmQA==
| 2048 d9:75:39:f6:22:57:fb:0e:c2:dc:23:b1:fd:67:5e:8a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAA-
BAQCt1PS4fG/8waGDF66VzlCjBgdpOH9WE5ZRiOm/vAQbuB0fphlzMtq0v1s5ReMel/JPdP
9WpSdLJ+Rd1DgXPzOckSJjEhH/1tYAqav8uanmVg4UAtHVfRQXVobiP-
jEQ9PDr1oEKqkiY8Cy4V21kjQ/hxv3RJ7aTl3co+LH9SSd2T8v86W7e91+lH6To-
IOa9lmMO5UZ+fmH+Z3lVk1QpQL0mMPoI1lAx678JzGfVvQdHjYL+Mbj7CuziQq3bt/dy-
iAr/lmtlMN1YxDuA4L5S/ab/szalhxXv4EEweHS388wAvTgzlI3jDlqiPLw8u0YJiME-
KFPS86avWtwvGAWVfZouP
| 256 ac:b4:99:b9:0f:30:54:9a:03:df:e5:d1:ad:0a:26:57 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAI-
bmlzdHAyNTYAAABBBMFXRIZtoMArqN9rEvxKnhKYsM5d37p1FM9BGIZBThQVcYtYR-
jeKnwdIiEzIH3RlNXuy8Qv3s6MU8MJmwHgGWIM=
80/tcp open http nginx 1.6.2
|_http-favicon: Unknown favicon MD5: CE9EDCC65D317B61E689A63F59D538C6
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
|_http-title: Contriboard
443/tcp open ssl/http-proxy Haproxy http proxy
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=*.n4sjamk.org/organizationalUnitName=PositiveSSL
Wildcard
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organiza-
tionName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/country-
Name=GB/localityName=Salford
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2014-06-24T00:00:00+00:00
| Not valid after: 2015-06-24T23:59:59+00:00
| MD5: 11fd a80a da7c 09ba e05d 4aa8 f22c e91c
| SHA-1: 0d90 77fd c78f ddee 13d7 6874 1e52 742b 1796 2cab
| -----BEGIN CERTIFICATE-----
| MIIFUDCCBDigAwIBAgIRAI6K4gz3xhS2uz/RNTGKT1EwDQYJKoZIhvcNAQELBQAw
| gZAxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO
| BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSB-
MaW1pdGVkMTYwNAYD
| VQQDEy1DT01PRE8gUlNBIERvbWFpbiBWYWxpZGF0aW9uIFNlY3VyZSBTZXJ2ZXIg
| Q0EwHhcNMTQwNjI0MDAwMDAwWhcNMTUwNjI0MjM1OTU5WjBaM-
SEwHwYDVQQLExhE
| b21haW4gQ29udHJvbCBWYWxpZGF0ZWQxHTAbBgNVBAsTFFBvc2l0aXZlU1NMIFdp

| bGRjYXJkMRYwFAYDVQQDFA0qLm40c2phbWsub3JnMIIBIjANBgkqhkiG9w0BAQEF
| AAOCAQ8AMIIBCgKCAQEAskl4oUPMWxgIcBS9r+OGydLQtSuBrp+wI55ylt5bcmd8
| 1KPzgEbXekhyOw3/IqpXh5fO8i/lAw5RiDYmPk9bePyDSkXuJzuBH6uaets7wY+o
| OOyY1Xw43nbQTu7v+lR1konJUjhWBBFYwpk7n09Fd6wR7uMr6LRFxIsgel9CFcHD
| dt5bQe+G2z3u2gFrEsP52tQnQWllHv1ijyPArTMErHB82Ff9uZmWQDcVndf25vKc
| MGDxpyR8NO980qD8CJ1bLGCiWa81mUsWnaNpYnIk3vel31bk1SjywXSlq02iQz0S
| tDF4g0rekvAbSHxDpBYoT0puJZCWUnK/KjTlfGXtPQIDAQABo4IB2DCCAdQwHwYD
| VR0jBBgwFoAUkK9qOpRaC9iQ6hJWc99DtDoo2ucwHQYDVR0OBBYEFHbyitb2L+TO
| ZIQA93mQdiR0NdcGMA4GA1UdDwEB/wQEAwIFoDAMBgNVHRM-
BAf8EAjAAMB0GA1Ud
| JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBQBgNVH-
SAESTBHMDsGDCsGAQQBsjEB
| AgEDBDArMCkGCCsGAQUFBwIBFh1odHRwczovL3NlY3VyZS5jb21vZG8ubmV0L0NQ
| UzAIBgZngQwBAgEwVAYDVR0fBE0wSzBJoEegRYZDaHR0cDovL2NybC5jb21vZG9j
| YS5jb20vQ09NT0RPUlNBRG9tYWluVmFsaWRhdGlvblNlY3VyZVNlcnZlckNBLmNy
| bDCBhQYIKwYBBQUHAQEEeTB3ME8GCCsGAQUFBzAChkNodHRwOi8vY3J0LmNvbW9k
| b2NhLmNvbS9DT01PRE9SU0FEb21haW5WYWxpZGF0aW9uU2VjdXJlU2VydmVyQ0Eu
| Y3J0MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5jb21vZG9jYS5jb20wJQYDVR0R
| BB4wHIINKi5uNHNqYW1rLm9yZ4ILbjRzamFtay5vcmcwDQYJKoZIhvcNAQELBQAD
| ggEBAE7kv0CCXnb821s5fuCKqVOzPxsPocFr5CxlHmqvTh/nXMumxDHij5fGZVx0
| o9NAUFI8bfzh9hAFKX82Uc61xubP06DzAoWFnyeKcImObxeM9fCrNE6RL3hxBBm8
| d7r9xhBOKSm/MSKR//iPsgWHLJtca658/7xpCw70RnpPt2rKTvYhvCtND5MoW81D
| 78/vH2s3hioMtFxAyEQso5dPvgykgOPhJLZjdPOIZRNO7tqm7JBNS9xIo6JX8IM4
| b6smgCtEKvuLBhUL+j7VcR13CPDLjaYbfJU9uN4SNqB8Nq1OyUnUonDf6SBQ+Va5
| 8JJg8HBvBkeGEmrr0xeWvgU/CFs=
|_-----END CERTIFICATE-----
|_ssl-date: 2097-12-04T16:10:53+00:00; +82y263d5h32m32s from local time.
1080/tcp closed socks
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=3/16%Time=5506B292%P=x86_64-pc-linux-gnu%r(NULL
SF:,29,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\r\n");
Device type: firewall|general purpose|terminal
Running (JUST GUESSING): IPFire Linux 2.6.X (87%), Linux 3.X|2.6.X (87%), IGEL Linux 2.6.X (85%)
OS CPE: cpe:/o:ipfire:linux:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:igel:linux_kernel:2.6
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: IPFire firewall 2.11 (Linux 2.6.32) (87%), Linux 3.2 - 3.6 (87%), Linux 2.6.32 (87%), IGEL UD3 thin client (Linux 2.6) (85%), Linux 2.6.35 (85%), Linux 2.6.32 - 2.6.35 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:

SCAN(V=6.40%E=4%D=3/16%OT=22%CT=1080%CU=%PV=Y%DS=1%DC=T%G=N%TM=55
06B29D%P=x86_64-pc-linux-gnu)
SEQ(SP=104%GCD=1%ISR=107%TI=Z%TS=8)
OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST
11NW7%O5=M2301ST11NW7%O6=M2301ST11)
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%TG=40%W=6903%O=M2301NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 5.200 days (since Wed Mar 11 05:50:24 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: load balancer

TRACEROUTE (using port 1080/tcp)
HOP RTT ADDRESS
1 0.87 ms ip-172-31-99-110.eu-west-1.compute.internal (172.31.99.110)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done at Mon Mar 16 10:38:21 2015 -- 1 IP address (1 host up) scanned in 47.21
seconds

Nmap 6.40 scan initiated Mon Mar 16 11:02:06 2015 as: nmap -oN
test1_haproxyslave.txt -T4 -A -p * -vv 172.31.99.234
Nmap scan report for ip-172-31-99-234.eu-west-1.compute.internal (172.31.99.234)
Host is up (0.0013s latency).
Scanned at 2015-03-16 11:02:06 UTC for 56s
Not shown: 4240 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh (protocol 2.0)
| ssh-hostkey: 1024 8e:aa:d8:4c:22:bc:d4:bc:8c:6e:99:3e:10:79:e6:83 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBANqpXRTSFc7tM6W0hDk37H0FVolK195WyUFHT-
kWjO+QGGaHYU/STwHvilLn9muamiHhsEm-

nioJ3M09/uyaDQEvJR2QR/RrFnNB9igNE0DYPzAgg4OT1sDAgHri1N/c6t92pla7SoXnhu-
VwPvPNQm6b3MVS+IGFTFUKUs6qe6KNaVAAAAFQDXyF7fVdG/XB96koaiRncVpDGFf-
wAAAIEAvXx9tzd4Yqeo5r25N0Fa/zV3U3n3lLGx1as+ZIrrSXHKENGGKXw0Erpg-
biDh+OT5pZVeq3EjB0ooCj/U1Wuj/R9vfnZxKjhB1rkT4yGan9iv53oiRBfQr1+8z4y1Ltc31Wj
1a78NAJ6kM5PSbCf+JyI0MHmtX07FKeRDtcc5MtgAAACAeLS8+qtGs8mZFFAaT-
vEY/8gOM/pceTVMdPDq++INrK2o78Qto04RdCbntZCqz9ThYSYL7TVL6eIUFhIV/vut-
wjmjHcT2hd+oNDlTer5Jt3dLys/ipiPOuWyHwDLtfS7WBEErLNaswgvlGDGcKmFAL-
SiEdOqkd9EH01VutWfVI1A=
| 2048 c0:e6:c2:d1:6c:e4:42:1f:cd:bf:44:8c:83:2a:bb:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAA-
BAQDABXbTO5TvFrlVlld4McN6Ys/aNQ2sBHigoW43QlwkiHARh8q+J1Fash-
GQslg8HSvrrJn1WeLGMKuuZfMJKPf0lUuESY5hdR1YY5/Z5G2amOy0zgGYJ4lib2pTFi+eS3y
OSn27OlhLw+7XbAyLadwX65l90OuKFeiDCcXdkmSQdNeVs6L7Alac-
GckfpbgsxJgYxa0/Ez7aClsSXi18oJuzGYGd4KKYeVPe0i0vpkTjUfRt5S5xXYKX1L43hYFybxsO
w78/KOOhK+TbdC8zjwtkwCUz-
bjPlr8WshlzvCtbtzF9Kk1lVHcYcqiV4JqmATMf87CWqXeucJ62ME8aidyF3
| 256 a3:c9:1c:3c:41:f6:35:7a:07:91:dc:04:39:bf:40:e1 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAI-
bmlzdHAyNTYAAABBBO2D0axN0YixOx1YN4eL-
Qury1s53u3zotNh3hKp3rqjWPNB4aFquV7VtsqHEHUkOJ4mu/M+YeqkwLVVcB8jk4n0=
80/tcp closed http
443/tcp closed https
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=3/16%Time=5506B861%P=x86_64-pc-linux-gnu%r(NULL
SF:,29,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\r\n");
Device type: firewall|general purpose|WAP|terminal
Running (JUST GUESSING): IPFire Linux 2.6.X (87%), Linux 3.X|2.4.X|2.6.X (86%), IGEL Linux 2.6.X (85%)
OS CPE: cpe:/o:ipfire:linux:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6 cpe:/o:igel:linux_kernel:2.6
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: IPFire firewall 2.11 (Linux 2.6.32) (87%), Linux 3.2 - 3.6 (86%), DD-WRT v24-sp1 (Linux 2.4) (86%), Linux 2.6.32 (86%), IGEL UD3 thin client (Linux 2.6) (85%), Linux 2.6.35 (85%), Linux 2.6.32 - 2.6.35 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=6.40%E=4%D=3/16%OT=22%CT=80%CU=%PV=Y%DS=1%DC=T%G=N%TM=5506B866%P=x86_64-pc-linux-gnu)
SEQ(SP=FC%GCD=1%ISR=107%TI=Z%TS=8)
OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2301ST11NW7%O6=M2301ST11)
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%TG=40%W=6903%O=M2301NNSNW7%CC=Y%Q=)

T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 0.159 days (since Mon Mar 16 07:14:06 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.38 ms ip-172-31-99-234.eu-west-1.compute.internal (172.31.99.234)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done at Mon Mar 16 11:03:02 2015 -- 1 IP address (1 host up) scanned in 56.93 seconds

Liite 4. REGISTRY palvelimen nmap skannaus

Nmap 6.40 scan initiated Mon Mar 16 10:58:25 2015 as: nmap -oN test1_registry.txt -T4 -A -p * -vv 172.31.100.102
Increasing send delay for 172.31.100.102 from 0 to 5 due to 95 out of 237 dropped probes since last increase.
Increasing send delay for 172.31.100.102 from 5 to 10 due to 18 out of 44 dropped probes since last increase.
Nmap scan report for ip-172-31-100-102.eu-west-1.compute.internal (172.31.100.102)
Host is up (0.00062s latency).
Scanned at 2015-03-16 10:58:25 UTC for 88s
Not shown: 4241 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh (protocol 2.0)
| ssh-hostkey: 1024 22:10:5c:80:88:5f:ed:7a:ea:23:70:7f:fb:64:1a:a2 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKdJFnsq4M46nijTZm1yBtnIz20UpS99Sqqb25by-pQERnH89NL0gDgfdW5v1rIxitCXeWM2daGtstlUgsS7VZR1IkrL5KZyMLh68QpwYcpXy-FUfs/7F96NmzjNQwI3FgIaf7Vb3jorBJHuhN3k4ZfpdDq3+i0+/DEVqIwLO3G5y1AAAAFQD-LUOsKkFjcGv/XP33cxi52ai1LNwAAAIAO3776HO3+io42749Yj+v+dGbwgTBOn+4Kw8xDyD

6R25qIE5CUyb6CPcRbTSppDN07hUBZZsi2RiZ-
TVmAHoYYr/R9tLP2MxqcV/fO49O0jT+5lYEsMmvkHvsxgmno6s1npEzA-
dWso/MhkpmHD8gms+BgJjaPIHU9zUgaxsryDy0QAAAIBO-
ZxXCYtF04T5MmcrN98xEIZz188kg1TEk-
crpH2WINsWoyEf5WCOD1f8lunbK2T2yx56XmpYCYHyf8eAy4tAjuBuKTN6D+N35hQKmLS
6bzYwUzNegbreS9yHeKk5Posuimo856jnghKIsop8bl0p5wlC+HtSenjduxTraIyvdYng==
| 2048 3b:44:6d:24:de:e9:3d:4f:33:80:30:d9:ff:1c:85:4a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDum4yNjtITF3j1sMq8B2RCfFQho-
cENIeKM3l1Ws2mJUNVDG7W0lYtw870IWgNb/KwUQUe9rTHc9TkUqcfaC-
mSHvdqSGk4gWAWJJLLmreWIrn/8TCABi5XML9naKpbVi-
Fyeossnp07L+W5POZ50+KwWwEQhZ3Az1/NLsCkzq9glh3yToUshZg2f1PmErGzOikbFcg9jI
sShWceHM-
BvBro0jRY3p6Qamm58Dh8Mk61bl/s/idkLaeA81JkcBxIUNoeJ1K87w2X0CFDv3AGV1WIr7
QWUMIkmrU82VciPSHfju+DOD6z+QOnsdcWjThuD52Geej8Q6dGlQYlln8g1Y9X9b
| 256 53:8a:be:c8:40:b3:bd:10:b1:5a:35:58:55:fc:9d:1d (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAI-
bmlzdHAyNTYAAABBBFS-
jinJRVq10KKhQNOe8cUIx4uLxy1GOfoSvkmaGZiTMFb7izlZUlFJyXxpshV2L74UyU5I8HYfpK
gxfyqKd6qs=
5000/tcp open tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=3/16%Time=5506B794%P=x86_64-pc-linux-gnu%r(NULL
SF:,29,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\r\n");
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=3/16%OT=22%CT=1%CU=31300%PV=Y%DS=1%DC=T%G=Y%T
M=5506B7A
OS:9%P=x86_64-pc-linux-
gnu)SEQ(SP=105%GCD=1%ISR=109%TI=Z%TS=8)OPS(O1=M2301S
OS:T11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=
M2301ST11NW7%
OS:O6=M2301ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=
68DF)ECN(R=Y
OS:%DF=Y%T=40%W=6903%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 67.240 days (since Thu Jan 8 05:14:51 2015)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 8080/tcp)
HOP RTT ADDRESS
1 0.75 ms ip-172-31-100-102.eu-west-1.compute.internal (172.31.100.102)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done at Mon Mar 16 10:59:53 2015 -- 1 IP address (1 host up) scanned in 88.23 seconds

Liite 5. Verkon laitteiden Nessus skannaukset

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.110.24

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.110.70

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.110.71

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	9	10

Details

Severity	Plugin Id	Name
Medium (6.4)	81777	MongoDB Service Without Authentication Detection
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	25220	TCP/IP Timestamps Supported
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	65914	MongoDB Detection

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.110.86

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.110.125

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.99.110

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	3	26	31

Details

Severity	Plugin Id	Name
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)

Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.99.234

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	2	14	16

Details

Severity	Plugin Id	Name
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.100.102

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	2	18	20

Details

Severity	Plugin Id	Name
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11765	UPnP TCP Helper Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

Liite 6. Korjausten jälkeiset Nessus skannaukset

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.99.110

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	20	20

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.99.234

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	20	20

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

172.31.100.102

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11765	UPnP TCP Helper Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type