jamk

Itse isännöidyn Wordpress-palvelimen tietoturva

Aaro Frondelius

Opinnäytetyö, AMK
Tammikuu 2023
Tietojenkäsittelyn tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Frondelius, Aaro

Itse isännöidyn Wordpress-palvelimen tietoturva

Jyväskylä: Jyväskylän ammattikorkeakoulu. Tammikuu 2023, 50 sivua.

Tietojenkäsittelyn tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tutkimuksessa tarkastellaan tietoturvallisen itse isännöidyn Wordpress-palvelimen käytänteitä. Wordpress on maailman suosituin sisällönhallintajärjestelmä, joka on pohjana miljoonilla verkkosivuilla. Sivujen pystytyksen helppokäyttöisyyden ansiosta aiempaa laajemmalla yleisöllä on mahdollisuus luoda omat verkkosivut. Itse isännöityjen sivujen tietoturvasta on laajasti tietoa eri taitotasoille, joten alkuun pääsy voi olla ylivoimaista aloittelijoille. Sen takia tärkeiden käytänteiden yhteen kokoamisesta on hyötyä.

Tutkimuksessa selvitettiin, mitä käytänteitä itse isännöidyllä Wordpress-palvelimella kannattaa käyttää sekä miksi tietoturva on tärkeää. Tutkimuksen toteutustapa oli kehittämistutkimus kvalitatiivisia menetelmiä hyväksi käyttäen. Tutkimuksen tuloksena tuotettiin opas parhaiden käytänteiden toteuttamiseen, jota seuraamalla voi tehdä samat asiat, mitä työssä tutkittiin.

Tutkimuksessa saatiin selville, että tietoturvallinen palvelin koostuu lukemattomista pienistä osista. Kaikkia osa-alueita ei käsitelty työssä, mutta silti tutkimuksessa havaittiin aiheen laajuus. Saatiin selville, että moneen asiaan on useita eri ratkaisuja, ja yhtä oikeaa ratkaisua on harvoin vaikea löytää. Selvisi myös, että työkaluja näiden ongelmien ratkaisuun on tarjolla eri tieto- ja taitotasoille.

Tutkimuksen käytännön osassa toteutettiin tutkitut vaiheet oikeassa ympäristössä, kirjoitettiin toimista opas ja todennettiin tehtyjen toimien validiteetti läpäisytestauksella. Työkalujen avulla todistettiin, että tehdyistä asioista oli ollut suurilta osin hyötyä palvelimen tietoturvan kannalta. Näin saatiin todennettua oppaan oikeudenmukaisuus.

Avainsanat (asiasanat)

Palvelin, tietoturva, kehittämistutkimus

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Frondelius, Aaro

Security of the self-hosted Wordpress server

Jyväskylä: JAMK University of Applied Sciences, January 2023, 50 pages.

Business Information Technology degree programme. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The study concerns the practices of a secure self-hosted Wordpress server. Wordpress is the world's most popular content management system that millions of websites are based on. Due to the ease of starting a website, wider audiences have the ability to create their own websites than before. A large amount of information already exists on the security of self-hosted websites directed to different skill levels, so the start can be intimidating for newcomers. It's therefore useful to gather the important practices.

The purpose of the study was to find out which practices to use on a self-hosted server and why security is important. The implemented method of research was development research using qualitative methods. As a result of the study, a guide detailing the implementation of good security practices was produced. By following the guide, the same steps can be taken towards better security.

The study found that a secure server consists of countless smaller parts. Not all areas of cyber security were taken into account in the study, but the large scope of the subject still became apparent. It became clear that there are multiple different solutions to problems, and it is often difficult to find one right solution to a problem. It was also discovered that there are tools for persons of different knowledge and skill levels.

In the practical part of the study the previously examined steps were carried out in a live environment and a guide was written on them. The validity of previously performed actions was verified through various penetration testing methods. These methods were used to prove that the performed steps had been of benefit considering the security of the server. The validity of the guide was thus verified.

Keywords/tags (subjects)

Server, cybersecurity, development research

Miscellaneous (Confidential information)

Sisältö

Sanasto

Ajuri – Ohjelmisto, joka kommunikoi tietokoneen fyysisten osien kanssa. Ajureita tarvitaan esimerkiksi näytönohjaimen käyttöön.

CAPTCHA – Ohjelmisto, joka suojaa verkkosivuja botteja vastaan luomalla testejä, joista ihmiset pääsevät läpi mutta botit eivät.

IP-osoite – Laitteen yksilöivä osoite, jonka avulla laitteen voi tunnistaa paikallisessa verkossa tai internetissä.

Läpäisytestaus – Tapa järjestelmän testaukseen, jossa simuloidaan hyökkäystä. Tarkoituksena löytää heikkouksia, joista hyökkääjä voisi oikeassa tilanteessa päästä läpi.

Portti – Yhteyden muodostukseen liittyvä numero, jolla voidaan tunnistaa eri yhteyksiä samasta IP-osoitteesta.

root-käyttäjä – Pääkäyttäjä Unix- tai Linux-pohjaisissa järjestelmissä. Käyttäjällä on laajimmat mahdollisuudet oikeudet järjestelmässä.

SSH – Protokolla, jolla voidaan yhdistää kahden tietokoneen välille suojattu yhteys.

Tietokanta – Kokoelma tietoja, jonka sisältö on muutettavissa ja haettavissa. Tarvitaan verkkosivuilla esimerkiksi tallentamaan käyttäjätietoja.

Virtuaalikone – Ohjelmallisesti toisen tietokoneen sisällä toteutettu tietokone.

1 Johdanto

Opinnäytetyön tarkoituksena on selvittää, mistä osista tietoturvallinen palvelin yksityiseen Wordpress-käyttöön koostuu. Tietoturva on ollut tärkeä osa IT-maailmaa lähestulkoon sen alusta asti, ja aihe on erityisen tärkeä nykyaikana, kun kenen tahansa yksityishenkilön on mahdollista pystyttää palvelin ilman suurempaa tietämystä aiheesta. Yhdysvaltalainen faktapankki Pew Research Center teki tutkimuksen amerikkalaisten ihmisten tietoturvatiedoista. Kyselyn 13 kysymyksestä suurin osa vastaajista osasi vastata oikein vain kahteen kysymykseen. (Olmstead 2017). Tämän takia yleistä tietämystä tietoturvasta täytyy lisätä. Vaikka kysely oli vain suhteellisen pieni kokonaisuus, se kertoo huolestuttavaa sanomaa yleisen tietoturvatiedon puutteesta, joka tekee tällaisen pienen skaalan työnkin tekemisestä kannattavaa.

Opinnäytetyössä tarkastellaan Linux- ja Windows- pohjaisia palvelimia, sillä ne ovat yleisimmät käyttöjärjestelmät palvelinkäytössä (Usage statistics of web servers 2022). Tarkasteluun otetaan myös FreeBSD sen tietoturvaominaisuuksien takia. Toisena rajauksena opinnäytetyössä tarkastellaan palvelinten tietoturvaa erityisesti ajatellen käyttöä Wordpress-käytössä. Wordpress-sisällönjulkaisujärjestelmä on käytössä 43 prosentilla kaikista verkkosivuista, joka tekee siitä todella suuren osan verkossa vierailevan käyttäjän kokemusta (Usage statistics and market share of Wordpress 2022). Koska Wordpress on näin laajassa käytössä, pitäisi sen tietoturvaan kiinnittää huomiota sivuston ylläpitäjän ja etenkin käyttäjäkunnan turvaksi.

2 Tutkimusasetelma ja -kysymykset

Tässä opinnäytetyössä toteutettava tutkimus keskittyy yksittäisen käyttäjän itse isännöimään paikalliseen Wordpress-palvelimeen. Opinnäytetyössä keskitytään erityisesti perustason käytänteisiin, joista on hyötyä pienen skaalan verkkosivuston isännöinnissä. Opinnäytetyössä on tarkoitus käydä läpi eri palvelinohjelmistojen, käyttöjärjestelmien ja Wordpressin tietoturvaa, sekä yleisemmällä tasolla tietoturvaa. Tutkimuksessa käydään myös läpi yleisimpiä tällaiseen palvelimeen kohdistuvia uhkia ja käytänteitä uhilta suojautumiseen. Tärkeimmät kysymykset, joiden vastauksia tässä työssä selvitetään ovat mitkä ovat itse isännöidyn Wordpress-palvelimen tärkeimmät käytänteet tietoturvan suhteen ja miksi tietoturva on tärkeää?

Työ toteutetaan kehittämistutkimuksena. Ojasalon, Moilasen & Ritalahden (2015, 18) mukaan tutkimuksellisessa kehittämisessä pyritään etsimään ratkaisuja käytännöstä nousseisiin ongelmiin tai uudistamaan jo olemassa olevia käytäntöjä. Kehittämistutkimuksella ei kuitenkaan ole yhtä kaiken kattavaa määritelmää. Edelsonin (2002) mukaan kehittämistutkimuksessa kehittäminen ja tutkimus yhdistyvät prosessissa, joka sisältää sekä teoreettisia että kokeellisia vaiheita. Näitä vaiheita käydään tutkimuksen aikana syklisessä prosessissa, jossa teoria ja käytäntö vuorottelevat.

Tässä työssä pyritään etsimään parhaita toimintatapoja Wordpress-palvelimen omaan isännöintiin tietoturvan saralta. Kuten kehittämistutkimukselle on ominaista, käytännön vaihe saa pohjansa teoreettiselta osuudelta, jossa määritetään työn raamit. diSessasin ja Cobbin (2004) mukaan kehittämistutkimuksen keskeinen ajatus on kehittäminen, joka perustuu teoriaan sekä teorian tuottaminen edeltävästä kehittämisestä. Kyseiseen periaatteeseen pohjautuu tämäkin opinnäytetyö. Käytännön osuus, jossa määritetään järjestelmä ja testataan sen turvallisuutta, perustuu aiemmin tehdyn tutkimustyön ja tietoperustan pohjalle. Bisterin (2019) mukaan kehittämistyön tuloksena syntyy yleensä jokin osittainen tai kokonainen tuote, esimerkiksi ohjelmisto tai ratkaisu. Tätäkin tullaan noudattamaan tässä työssä, jossa lopulliseksi tuotteeksi syntyy ohjeistus kuvaamaan tehtyjä ratkaisuja. (Bister 2019.)

3 Tavoitteet

Tämän opinnäytetyön tavoitteena on selvittää yksityisen itse isännöidyn Wordpress-palvelimen tärkempiä tietoturvakäytänteitä. Tavoite toteutetaan keräämällä tietoa nykyisestä tietoturvatilanteesta sekä eri osien ominaisuuksista ja haavoittuvuuksista. Tietoihin perustuen tehdään päätökset teknologioista ja ohjelmista, joita käytetään. Järjestelmä asennetaan ja otetaan käyttöön parhaaksi havaitulla tavalla, jonka jälkeen järjestelmän tietoturvaa testataan läpäisytestauksella, jossa yritetään hyödyntää yleisimpiä tietoturva-aukkoja. Läpäisytestaus on tärkeää, sillä sen avulla voidaan todentaa tietoperustan luotettavuus ja tehtyjen toimenpiteiden toimivuus käytännössä. Ilman turvatoimenpiteiden testausta ei olisi minkäänlaista tietoa siitä, onko suojattu palvelin ollenkaan suojattu ja ovatko tehdyt toimenpiteet toimivia tällaiseen käyttötarkoitukseen.

Lopullisena tuloksena työstä tehdään tiivis ohjeistus, jossa lukijoille kerrotaan parhaita käytäntöjä itse isännöidyn Wordpress-palvelimen tietoturvan parantamiseen. Näiden käytäntöjen toimivuus

on testattu aiemmin läpäisytestauksella. Ohjeistus tehdään, koska sen pohjalta muiden on mahdollista tehdä samat toimenpiteet, joiden toimivuus ja luotettavuus on testattu jo tässä työssä. Oppaassa ei tulla käymään läpi kaikkia verkkosivun pystytykseen johtavia toimia, vaan painostus on toimissa, jotka kasvattavat palvelimen tietoturvaa.

Tämä opinnäytetyö tehdään opiskelijan näkökulmasta ja se keskittyy verrattain pienen skaalan palvelimiin ja prosesseihin. Suuremman skaalan tietoturva ja palvelininfrastruktuuri kuuluu toiseen työhön.

Wordpress valittiin sen takia, että se on tällä hetkellä suosituin verkon sisällönhallintajärjestelmistä, ollen käytössä 43 prosentilla kaikista verkon sivustoista ja 64,3 prosentilla kaikista sivustoista, joissa on käytössä sisällönhallintajärjestelmä (w3techs 2022b). Wordpress valittiin tutkimukseen myös sen työllistävän vaikutuksen sekä oman kiinnostuksen takia. Kuten tuli jo aiemmin mainittua, tutkimusta ei ole rajattu vain yhteen käyttöjärjestelmään perustuviin palvelimiin, vaan tutkimuksessa otetaan huomioon Windows- ja Linux-pohjaiset palvelimet. Ratkaisussa otettiin myös huomioon se, että tutkimuksessa etsitään turvallisinta palvelinratkaisua, eikä siksi kannata sulkea suurta osaa vaihtoehdoista pois heti alkuvaiheessa.

Aihe ei ole mikään uusi, joten siitä on ennalta kerättyä tietoa laajalti. Myös Jyväskylän ammattikorkeakoulussa on tehty useita samaa aihetta sivuavia opinnäytetöitä. Tietoturva on kuitenkin jatkuvasti kehittyvä aihe, ja uusia uhkia sekä mahdollisuuksia nousee esiin päivitysten ja muutosten myötä.

4 Tietoturva

Tietoturva on hallinnollista ja teknistä toimintaa, jolla suojataan tietoa, järjestelmiä ja tietoliikennettä ja vähennetään niihin kohdistuvaa uhkaa. Se on myös yksi keinoista, joilla toteutetaan tietosuojaa. Usein nykyaikana tietoturva mielletään tärkeäksi vain digitaalisissa ympäristöissä, mutta aivan yhtä tärkeitä osa-alueita ovat ihmisten välinen kommunikaatio ja esimerkiksi tieto paperilla. Tietoturvan osiksi lasketaan yleensä saatavuus, luottamuksellisuus ja eheys. (Tietoturva 2020.)

Tiedon saatavuudella tarkoitetaan tiedon saatavilla olemista oikeutetuille tarvittaessa. Esimerkiksi salattu tiedosto on luottamuksen ja eheyden suhteen loistava idea, mutta saatavuus kärsii käyttäjän joutuessa purkamaan salauksen joka kerta tiedostoa käytettäessä. (Tietoturva 2020.)

Tiedon luottamuksellisuus tarkoittaa, että tiedon käsittelyä voivat tehdä vain siihen oikeutetut henkilöt. Helppona käytännön esimerkkinä voi pitää esimerkiksi henkilön työsähköpostia. Vain oikeutetuilla henkilöillä on pääsy sähköposteihin ja tietoihin ja mikäli salasana annetaan jollekin ulkopuoliselle, kaikkien sähköpostissa olevien tietojen luottamuksellisuus on uhan alla. (Tietoturva 2020.)

Tiedon eheys tarkoittaa tiedon muuttumattomuutta ja pysyvyyttä. Tiedon tulee olla ajan tasalla ja luotettavaa, eikä tietoa pitäisi pystyä muuttamaan esimerkiksi inhimillisen vahingon tai ohjelmistohäiriön seurauksena. Tärkeä elementti eheyden ylläpitämisessä on varmuuskopiointi, jonka avulla voidaan varmistaa, että alkuperäisestä tiedosta on ainakin yhdessä paikassa alkuperäinen versio tallessa. (Tietoturva 2020.)

Tässä opinnäytetyössä käsitellään tietoturvaa palvelinkäytön näkökulmasta, joten edellä mainituista osa-alueista keskitytään erityisesti luottamuksellisuuteen ja eheyteen, sillä saatavuuden oletetaan olevan kunnossa.

IBM:n vuonna 2022 toteuttaman X-Force Threat Intelligence Index-tutkimuksen mukaan käyttäjätietojen kalastelu on yleisin tapa päästä hyökkäyksen kohdeverkkoon käsiksi. Tämän tutkimuksen mukaan siis 41 prosenttia kaikista hyökkäyksistä alkaa käyttäjätietojen kalastelulla eli phishingillä. Aiemmin, vuonna 2014 julkaistussa tutkimuksessa tultiin lopputulokseen, jossa havaittiin, että jopa 95 prosenttia tietoturvaloukkauksista johtuu käyttäjien omasta toiminnasta ja inhimillisistä virheistä. (IBM Security Services 2014 Cyber Security Intelligence Index, 2014.) Nykyisin yleisin tapa eli tietojen kalastelu on yllättävänkin yksinkertainen. Tällaisessa hyökkäyksessä voidaan esimerkiksi lähettää yrityksen edustajille virallisen näköisiä sähköposteja, joissa pyydetään kirjautumaan omilla tunnuksilla verkkosivulle, joka on kuitenkin hyökkääjän hallinnassa. Tätä kautta hyökkääjä sitten saa tunnukset haltuunsa ja pääsee yrityksen sisäisiin järjestelmiin tunnuksilla. (Protect yourself from phishing n.d.)

Myös tavallisessa jokapäiväisessä käytössä on havaittavissa lukemattomia tietoturvapuutteita tai -ongelmia. Tietokoneilta ei kirjauduta ulos käytön jälkeen, salasanat ovat yksinkertaisia tai jopa samoja kaikissa palveluissa eikä esimerkiksi mobiililaitteilla käytetä lukituskoodeja. Varsinkin salasanat ovat ja tulevat olemaan ikuinen ongelma niin kauan ennen kuin toinen korvaava ratkaisu keksitään. Nykyään jokaisella ihmisellä, joka digitaalisia palveluita käyttää, on sama ongelma; Jokaiseen palveluun tarvitaan salasana, mutta mitä enemmän salasanoja kertyy, sitä vaikeampi niitä on muistaa. Asiasta vaikeamman tekee suositellun salasanan muoto, joka sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Monet siis luovuttavat ja tyytyvät käyttämään samaa salasanaa useissa palveluissa, joka tietenkin vähentää salasanan hyödyllisyyttä ja pienentää turvaa, sillä jos vaikka tietomurrossa salasana ja käyttäjätunnus saadaan selville, samalla yhdistelmällä olevat tunnukset muissakin palveluissa ovat vaarassa vain murretun palvelun sijaan. (Tietoturvan inhimilliset ja fyysiset tekijät n.d.)

Ennen kuin salasanattomat tunnistautumismenetelmät alkavat yleistyä, täytyy salasanoihin turvautua. Monivaiheinen tunnistautuminen on nykyään laajalti käytössä oleva tapa, joka lisää tilien turvallisuutta lisäämällä tunnistautumiseen yhden ylimääräisen vaiheen. Esimerkiksi Office 365-palvelussa sähköpostin ja salasanan syöttämisen jälkeen tarvitaan vielä koodi, jonka voi saada puhelimeen tekstiviestinä tai mobiilisovelluksesta. Näin ollen, mikäli salasana ja käyttäjätunnus olisivat päätyneet jonkun ei-toivotun käsiin, kirjautuminen ei onnistu ilman käyttäjän matkapuhelinta. (What is Two-Factor Authentication? n.d.)

4.1 Palvelinohjelmistojen tietoturva

Apache on alun perin vuonna 1995 julkaistu verkkopalvelinalusta. Tänä päivänä Apache on käytössä 31,4 prosentissa kaikista verkkopalvelimista (w3techs). Apachen käyttöönotto on tehty helpoksi, mutta tehokäyttäjille on massiivinen määrä eri vaihtoehtoja. Apache koostuu moduuleista, joita vaihtamalla voi muuttaa palvelimen ominaisuuksia ja toimintaa. Esimerkiksi SSL- ja PHP-moduulit ovat lisättävissä palvelimelle. (Apache HTTP Server Project n.d.)

NGINX on uudempi tulokas palvelinkentällä mutta se on kasvattanut suosiotaan jatkuvasti ja tällä hetkellä se on käytössä 34,2 prosentissa verkkopalvelimista, eli se on ohittanut Apachen käyttömäärässä. Myös NGINXiin sisältyy asennuksessa runsaasti erilaisia moduuleja, joista kuitenkin kannattaa poistaa sellaiset, joita ei tule tarvitsemaan käytössä. Apacheen on helppoa lisätä moduuleja

asennuksen jälkeen, mutta NGINX-moduulit tulee lähtökohtaisesti valita asennusvaiheessa, sillä moduulien jälkeenpäin lisääminen on monimutkaisempaa. (NGINX n.d.)

NGINX ja Apache eroavat toisistaan tietyissä ominaisuuksissa. Apache pystyy käsittelemään dynaamista sisältöä natiivisti mutta NGINX ei. NGINX taas toimii staattisen sisällön kanssa paljon tehokkaammin käyttäen vähemmän muistia kuin Apache. Palvelinohjelmistojen konfiguroinnissakin on eroja: NGINX käyttää keskitettyä metodia, jossa asetuksiin on vain yksi tiedosto palvelimella. Apache taas käyttää .htaccess-tiedostoja, joita voi lisätä palvelimelle useampaan tiedostosijaintiin. Joka kerta, kun palvelimelle tehdään pyyntö, Apache tarkistaa reitin asetustiedostoon. NGINX toimii suoraviivaisemmin, koska käytössä on vain yksi tiedosto, jonka sijainti on aina tiedossa, joten sijaintia ei tarvitse tarkastaa joka pyynnölle. (Apache HTTP Server Project n.d.; NGINX n.d.)

Palvelinohjelmistojen tietoturvaan on monta lähtökohtaa, mutta pohjimmiltaan kuitenkin turvallisin on palvelin, jota ei kytketä ollenkaan ulkoiseen verkkoon. Tässä työssä käsitellään kuitenkin palvelinten Wordpress-käyttöä, joten palvelinohjelmiston joutuu avaamaan ulkoiselle maailmalle ja siitä lähtöisin oleville uhille. Niin Apache kuin NGINX on suunniteltu olemaan perustasolla turvallinen. Se ei tarkoita, että ohjelmistoissa ei olisi eroja. Apachen koodikanta on jo ohjelmiston iänkin takia massiivisesti laajempi kuin uudemman tulokkaan NGINXin, joka kasvattaa mahdollisuutta ohjelmistobugeille ja hyökkäyskohteille koodissa. NGINX, toisin kuin Apache myös piilottaa oletuskonfiguraatiossaan hakemistolistaukset, joilla kuka tahansa voisi selata sivuston hakemistoa vapaasti. Oletuskonfiguraatioon kannattaa kuitenkin tehdä joitain muutoksia kumpaa tahansa palvelinohjelmistoa käytettäessä. (Apache HTTP Server Project n.d.; NGINX n.d.)

Jos katsotaan Apachen ja NGINXin tietoturvan tasoa tilastojen perusteella, vaikuttaa NGINX huomattavasti turvallisemmalta vaihtoehdolta. CVEdetails-sivuston (n.d) tilastojen mukaan Apachessa on tällä hetkellä 252 erilaista haavoittuvuutta, joista 8 on saanut 10 pistettä, eli ne on määritelty erittäin vaarallisiksi (Apache Security Vulnerabilities n.d.) Saman sivuston mukaan NGINXillä on vastaavia haavoittuvuuksia vain kaksi kappaletta, ja niistä korkein pistemäärä on 5, eli uhan taso ei ole läheskään yhtä vakava kuin kilpailijalla (NGINX Security Vulnerabilities, N.d). Näistä tilastoista voidaan tehdä johtopäätös, että NGINX on tällä hetkellä ainakin tietoturvan saralla Apachea varteenotettavampi vaihtoehto.

4.2 Käyttöjärjestelmien tietoturva

Linux on käyttöjärjestelmäperhe, joka perustuu Linus Torvaldsin 1991 kehittämään Linux-ytimeen. Linux on maailman suurin verkkopalvelimissa käytetty käyttöjärjestelmä 96,3 prosentin osuudella kaikista verkkopalvelimista (Linux Statistics 2022).

Linuxin käyttöön levittäminen tapahtuu eri jakelupaketteina eli distribuutioina. Kaikki distribuutiot pohjautuvat Linux-ytimeen. Aktiivisia distribuutioita on tällä hetkellä yli 600, joista suosituimpia ovat Ubuntu, Debian ja CentOS (Linux Statistics 2022). Distribuutioita on eri käyttötarkoituksiin, esimerkiksi Ubuntu on suunnattu enemmän koti- ja työpöytäkäyttöön, kun taas CentOS keskittyy laajemmin yritys- ja palvelinkäyttöön. (Ubuntu User Statistics n.d.; The CentOS Project n.d.) Työpöytäkäyttöön suunnatut Linux-distribuutiot sisältävät yleensä visuaalisen käyttöliittymän, kun taas palvelinversioissa sitä joko ei ole tai se saatetaan jättää pois muista syistä.

Windows Server on Microsoftin suunnittelema käyttöjärjestelmä palvelinkäyttöön. Se pohjautuu kotikäyttöön tarkoitettuun Windowsiin, mutta sen ominaisuuksissa ja toiminnallisuudessa on eroja, riippuen versiosta. Ensimmäinen Windows Server-nimen alla oleva käyttöjärjestelmä julkaistiin vuonna 2003. Windows Server 2003 perustui Windows XP:lle ja nykyinen uusin versio, Windows Server 2022 perustuu Windows 11-käyttöjärjestelmälle. (Windows Server 2022.)

Windows Server on muihin tässä työssä esitettyihin ratkaisuihin verrattuna palvelinkäyttöjärjestelmistä ehdottomasti aloittelijaystävällisin vaihtoehto. Se on helppo ottaa käyttöön ja se ei ole erityisen riippuvainen jatkuvasta ylläpidosta ja huollosta järjestelmään sisältyvien automaatiomahdollisuuksien vuoksi. (Tucadov 2021.)

Seuraava vaihtoehto, FreeBSD on vuonna 1993 julkaistu, alun perin Berkeley Software Distribution-käyttöjärjestelmään perustuva avoimen lähdekoodin käyttöjärjestelmä. FreeBSD perustuu Unix-käyttöjärjestelmäpohjalle, vaikka tekijänoikeuksien takia asiaa ei mainitakaan FreeBSD Project-kotisivuilla. (The FreeBSD Project 2022.)

Käyttöjärjestelmien maailmassa FreeBSD:llä on monia yhtäläisyyksiä Linuxin kanssa, mutta erot liittyvät eniten järjestelmän tekijänoikeuksiin, lisensointiin ja käyttötarkoitukseen (Pedamkar n.d.).

Siinä missä Linux-distribuutioita on moneen tarkoitukseen kotikäytöstä suuren skaalan palvelinsaleihin, FreeBSD on tähdätty erityisesti palvelinkäyttöön ja sen ominaisuudet ovat kehittyneet käyttökohteen mukaan (The FreeBSD Project 2022).

4.3 Käyttöjärjestelmien tietoturvaerot

Yksi Linuxin tietoturvan kulmakivistä on käyttäjäoikeuksien laaja hallinta. Esimerkiksi uusille käyttäjille distribuutiosta riippuen Linux ei anna root-tason oikeuksia, vaan käyttäjillä on vähemmän oikeuksia hallita koko järjestelmän toimintaa. Linux on avoimen lähdekoodin käyttöjärjestelmäperhe, joten kuka tahansa käyttäjistä voi periaatteessa löytää haavoittuvuuksia koodista ja auttaa järjestelmän turvallisuuden parantamisessa kaikille käyttäjille. (What is Linux? n.d.) Työpöytäkäytössä Windows on niin dominoiva 76 prosentin osuudellaan, että jopa 95 prosenttia Ransomware-hyökkäyksistä kohdistuu Windows-käyttäjiin (Virustotal Ransomware Activity Report 2021).

Käyttöjärjestelmät eroavat myös siinä, kuinka iso ongelma onnistunut hyökkäys niitä vastaan voi olla. Windowsissa kaikilla käyttäjillä on täydet oikeudet koko järjestelmään ja kaikkiin käyttäjiin, joka tarkoittaa mahdollisesti koko järjestelmän korruptoitumista hyökkäyksen sattuessa (Windows Server 2022.) Linuxilla ja FreeBSD:llä, joissa käyttäjien oikeudet järjestelmään voi rajata hyvin tarkasti, on paremmat mahdollisuudet säilyttää joitain tietoja ulottumattomissa. Koska käyttäjät Linuxissa ja FreeBSD:ssä eivät ole automaattisesti järjestelmänvalvojia, virukset eivät pysty leviämään koko järjestelmään. (Oracle n.d.)

Yksi etu Linuxissa verrattuna muihin on päivitysten tiheys. Monia Linuxin distribuutioita päivitetään tiiviiseen tahtiin ja niistä voi olla eri versioita, esimerkiksi Ubuntu tarjoaa sivustollaan LTS-version, joka saa päivityksiä useaksi vuodeksi sekä uudemman version, jossa on uusia ominaisuuksia mutta jota tuetaan vain alle vuoden ajan (Ubuntu n.d.). Myös Windows server ja FreeBSD saavat kuitenkin pitkän tähtäimen tukea, Windows serverin uusinta versiota tuetaan 5 vuotta kuten myös jokaista isompaa FreeBSD-julkaisua (FreeBSD Security Information n.d; Base image servicing lifecycles 2022.)

Linux, Windows Server ja FreeBSD tarjoavat jokainen erilaisen kokemuksen erilaisille käyttäjille ja käyttäjäryhmille. Tähän työhön kuitenkin parhaiten sopii Linux, joka tarjoaa yksittäiselle käyttäjälle

loistavan määrän vaihtoehtoja ollessaan kuitenkin tarpeeksi käyttäjäystävällinen. Linux-distribuutioiden suosion perusteella myös apua on helposti löydettävissä, mikäli ongelmia esiintyy.

4.4 Oikeudet

Palvelimella oikeudet määrittävät, kuka pääsee käsiksi sivujen tiedostoihin ja hakemistoihin. Oikeudet määrittävät myös käyttäjäkohtaisesti, kuka voi lukea, kirjoittaa tai suorittaa tiedostoja. On ongelmallista, jos sivuston kaikilla käyttäjillä on täydet oikeudet. Tämän takia oikeuksia joudutaan muokkaamaan käyttäjäkohtaisesti tarvittavien oikeuksien mukaan. Käyttäjäoikeuksia löytyy kolmea eri tyyppiä, jotka ovat luku-, kirjoitus- ja suoritusoikeus. (Oracle n.d.)

Unix-pohjaisissa järjestelmissä näistä oikeuksista voi myös luoda erilaisia yhdistelmiä. Jos halutaan antaa tietylle käyttäjälle esimerkiksi luku- ja kirjoitusoikeus, tulee käyttäjän oikeudeksi numerosarja 644, joka antaa oikeuden lukea ja muokata tiedostoja samalla käyttäjällä, mutta ei muiden saman ryhmän käyttäjien tai koko järjestelmän tietoja. Ensimmäinen numero viittaa käyttäjän oikeustasoon, toinen ryhmän tasoon ja kolmas muuhun. Kaikista ”vaarallisin” oikeuksista on numerosarja 777, joka antaa oikeuden muokata mitä vain, joten näin laajaa oikeutta ei kannata antaa kuin tietyissä erityistapauksissa. (Oracle n.d.) Wordpress itse suosittelee hakemisto- ja kansio-oikeuksiksi 755 ja php-tiedostojen käyttöoikeuksiksi 644. Näillä oikeuksilla myös Wordpressin automaattiset päivitykset pysyvät toiminnassa. (Changing File Permissions n.d.)

4.5 Kovettaminen

Kovettaminen tietoturvamaailmassa tarkoittaa suojattavan järjestelmän haavoittuvuuden vähentämistä vähentämällä järjestelmän hyökkäyspisteitä. Hyökkäyspisteet ovat kohtia ja ominaisuuksia järjestelmässä, joista hyökkääjä voisi saada pääsyn sisään. (Intel n.d.) Tähän työhön liittyviä vastaavia pisteitä ovat esimerkiksi ylimääräiset Wordpress-lisäosat, oikeudet, käyttäjät ja toiminnallisuudet.

4.6 Päivitykset

Wordpressin virallisten tietojen mukaan 42,6 prosenttia käyttäjistä käyttää edelleen vanhoja versioita palvelusta (Wordpress Statistics n.d). Sen lisäksi vain 0,7 prosenttia käyttäjistä on päivittänyt

PHP:n uusimpaan versioon (Wordpress Statistics n.d). Wordpressissä on ollut versiosta 3.7 asti mahdollisuus automaattisiin päivityksiin. Tätä mahdollisuutta suositellaan käytettäväksi, sillä Wordpressin ytimen sekä lisäosien ja teemojen päivittäminen on yksinkertainen mutta toimiva tapa lisätä sivujen turvallisuutta. Suurimmassa osassa Wordpress-sivuihin kohdistuneista hyökkäyksistä, sivusto on vaarantunut juuri lisäosan takia (Jackson 2022). Tästä syystä sivuilta kannattaa poistaa käyttämättömät lisäosat sekä asentaa vain luotettavaksi havaittuja lisäosia.

4.7 SSL/HTTPS

SSL-sertifikaatti (Secure Socket Layer) on digitaalinen tunniste, joka todentaa verkkosivun salatun yhteyden ja sivuston identiteetin oikeaksi. Sertifikaatti on pakollinen kaikille HTTPS-salatuille verkkosivuille. SSL-sertifikaatti todistaa, että sivuston käyttäjä on yhteydessä oikeaan domainin omistamaan palvelimeen. Nykyään SSL:n käyttö vähenee, kun uudempi salausprotokolla TLS on tullut markkinoille. Usein SSL ja TLS- nimikkeitä käytetään kuitenkin sekaisin, sillä niillä ei ole suurta eroa, merkitys on sama. (What is TLS? n.d.)

HTTPS (Hypertext transfer protocol secure) on protokolla, jonka avulla data liikkuu verkkoselaimen ja sivuston välillä. HTTPS eroaa HTTP:stä salaamalla kaiken viestiliikenteen, joka lisää turvallisuutta, etenkin arkaluonteisten salasanojen ja muiden tunnusten käytössä. Kun tietoa siirretään HTTP:n kautta, lähetetty data jaetaan ”paketeiksi” jotka on helppo siepata. HTTPS:n kautta lähetetyt paketit ovat salattuja, joten vaikka paketit saataisiinkin siepattua, data näyttäytyy salattuna merkkijonona, joka ei tarkoita mitään ilman salauksen purkua. (What is HTTPS? n.d.)

5 Yleisimmät uhat ja suojautuminen

Gallin (2023) mukaan yleisin uhka Wordpressille on varastettujen käyttäjätunnusten käyttäminen sisäänkirjautumisessa. Muut hyökkäystyypit ovat kuitenkin lyhentäneet välimatkaa vuosien varrella, ja vuoden 2022 Wordpress-turvallisuutta käsittelevässä raportissa havaittiin tämä muutos viime vuosiin verrattuna (Gall 2023). Tässä osiossa käydään läpi yleisimpiä Wordpress-sivustoon kohdistuvia hyökkäyksiä ja esitellään tapoja kyseisiltä hyökkäyksiltä suojautumiseen.

5.1 Brute force

Brute force-hyökkäyksen toimintaperiaate pohjimmiltaan hyvin yksinkertainen: Perinteisessä hyökkäyksessä kokeillaan eri salasanoja tunnettujen käyttäjätunnusten kanssa. Käänteisessä brute force-hyökkäyksessä taas salasanat ovat tiedossa esimerkiksi tietomurron seurauksena ja niitä kokeillaan eri käyttäjätunnusten kanssa. Tällainen hyökkäys voikin olla yllättävän tehokas, jos palvelimen salasanakäytänteitä ei ole laitettu kuntoon ja käyttäjillä on yksinkertaiset salasanat ja käytössä on esimerkiksi admin-käyttäjätunnus, jolloin vain salasana täytyy arvata. Brute force-hyökkäyksestä on myös muita muotoja: Dictionary attack eli sanakirjahyökkäys toimii nimensä mukaisesti. Hyökkääjällä on käytössään laaja lista yleisiä sanoja ja termejä, joita juuri sanakirjasta löytyy. Hyökkäys voidaan myös kohdistaa tiettyyn henkilöön, jolloin hyökkääjä ottaa henkilöstä selvää ja lisää hyökkäyksessä käytettävään sanakirjaan esimerkiksi kohteen harrastuksiin liittyvää sanastoa. (Norton 2021.)

Kaikkein helpoin suojautumiskeino on tietenkin monimutkaisempi käyttäjätunnus ja salasana, mutta Wordpressissä on muitakin suojautumismenetelmiä. Yksi keino on rajoittaa pääsy wp-login-tiedostoon vain tietyille IP-osoitteille. Tämä on käytännöllistä tilanteissa, joissa vain yksi henkilö tarvitsee pääsyn Wordpressin asetuksiin. Käyttäjällä pitää olla staattinen IP-osoite, jotta rajoituksen voi tehdä. Toinen keino on asettaa salasana wp-login-tiedostoon pääsemiseksi. Se on melko simppeli mutta toimiva lisävastus. (Brute Force Attacks n.d.) Toinen metodi salasanojen lisäsuojaukseen on niiden suolaaminen. Kun käyttäjä asettaa salasanan, se salataan ja siitä tulee epämääräinen merkkisarja. Jos salasana on yksinkertainen, ei tämäkään välttämättä ole täydellinen ratkaisu, sillä hyökkääjillä saattaa olla jo purkuavain yksinkertaisiin salasanoihin. Suolauksen avulla salasanan turvallisuutta voidaan lisätä, ja purkaminen muuttuu vaikeammaksi. Suolauksessa salasanan alkuun tai loppuun lisätään pätkä numeroita ja kirjaimia, jolloin esimerkiksi qwerty-salasanasta tulee 5j32h8iqwerty. Kun tämä yhdistelmä vielä salataan, on purku vaikeampaa, sillä vaikka hyökkääjillä olisi mahdollisuus purkaa pelkkä qwerty-yhdistelmä, satunnaisen merkkisarjan kanssa se vaikeutuu. Suolausyhdistelmän kuuluu lisäksi olla uniikki jokaiselle salasanalle. (Kinsta 2022.)

Myös rate limiting eli pyyntöjen määrän rajoittaminen palvelimella vaikeuttaa hyökkääjien toimintaa. Sen avulla voidaan asettaa raja sille, kuinka usein yksittäinen käyttäjä voi toistaa jonkin toimen, esimerkiksi kirjautumisen omaan profiiliin. Pyyntöjen määrää rajoittamalla voidaan siis rajoittaa sellaisten bottien toimintaa, jotka pommittavat kirjautumissivua jatkuvasti yrittäessään löytää

oikeita kirjautumistunnuksia. Yleensä käyttäjiä rajoitetaan ip-osoitteen tai käyttäjänimen perusteella. Molempia rajoituksia käyttämällä hyökkääjällä ei ole mahdollisuutta koettaa yleisiä salasanoja suurelle määrälle käyttäjänimiä, sillä pyyntöjen määrä katsotaan ip-osoitteen perusteella. (Cloudflare n.d.)

5.2 Man in the middle

Griman (2022) mukaan man in the middle on hyökkäys, jossa hyökkääjä kaappaa salaamattoman tietoliikenteen käyttäjän ja verkkosivun välillä. Hyökkääjä voi täten esimerkiksi lukea arkaluonteisia tietoja tai muokata kulkevia tietoja. Vaikka siis sivustolla vierailijasta kaikki vaikuttaisi normaalilta, kaikki käyttäjältä sivustolle ja toisinpäin kulkeva tieto on hyökkääjän hallinnassa, ja esimerkiksi käyttäjätunnukset ja salasanat voivat olla vaarassa. (Grima 2022.)

Man in the middle-hyökkäyksiltä suojautuminen on kuitenkin kohtalaisen helppoa. Verkkosivut pitäisi aina konfiguroida käyttämään HTTPS-protokollaa vanhemman HTTP:n sijaan. Tällöin vaikka joku saisikin käsiinsä tietoa, jota kulkee verkkosivun ja käyttäjän välillä, tieto on salattua ja hyödytöntä ilman salauksen purkua. Toinen tärkeä suojautumistapa, varsinkin itse isännöidyillä Wordpress-sivuilla on reitittimen hyvä suojaus ja salaus. Reitittimessä tai modeemissa ei kannata koskaan käyttää valmiina tulleita vakiosalasanoja, vaan käyttää hyvien käytänteiden mukaisia salasanoja. (Grima 2022.)

5.3 Cross Site Scripting (XSS)

Cross Site Scripting (XSS) on brute force-hyökkäysten ja SQL-injektion jälkeen yksi yleisimmistä tavoista hyökätä Wordpress-sivuille (WPHackedHelp 2018). Hyökkäyksessä sivuille tunkeutuja voi suorittaa koodia käyttäjän selaimessa. Hyökkäyksessä verkkoselain ei pysty tunnistamaan, että koodi ei tule alkuperäiseltä sivustolta, vaan luulee sen olevan sivun alkuperäistä sisältöä. Hyökkääjä voi täten nähdä tietoa käyttäjän selainistunnosta ja esimerkiksi viedä käyttäjän kirjautumistunnukset ja pahimmassa tapauksessa jopa maksutiedot. (WPHackedHelp 2018.)

Jos sivusto sisältää käyttäjille mahdollisuuden lisätä sivuille tietoa, kannattaa pitää mielessä hyökkäyksen mahdollisuus. Vastatoimia on kuitenkin olemassa. Wordpressiin on olemassa useita lisäosia, jotka skannaavat sivuston XSS-haavoittuvuuksilta, jonka jälkeen haavoittuvuuksia voi korjata.

Sivuston ylläpitäjän on myös mahdollista lisätä käyttöön lisäosa, joka skannaa käyttäjän lisäämiä tietoja skriptien varalta. Käyttäjäpuolella helppo suojautumistapa on asentaa selaimeen lisäosa, joka poistaa Javascript-tiedostojen suorittamisen selaimessa. Näin ollen haitallisia skriptejä ei voi suorittaa. (WPHackedHelp 2018.)

5.4 Supply chain attack

Tämä hyökkäystyyppi muistuttaa XSS-hyökkäyksiä siinä mielessä, että hyökkäyksen tarkoituksena on saada rehelliset ohjelmistot jakamaan viruksia tietämättään. Supply chain-hyökkäyksessä hyökkääjät etsivät suojaamattomia palvelimia ja epävarmoja verkkoprotokollia, joiden kautta he voivat saada pääsyn järjestelmiin ja voivat muokata kohteena olevan ohjelmiston lähdekoodia ja piilottaa virusohjelmistoja muuten täysin normaaleihin, viattomiin ohjelmistoihin. Tällaisen hyökkäyksen sattuessa tähdätään siihen, että alkuperäistä ohjelmistoa levittävät tahot eivät huomaa hyökkäystä ja siitä johtuneita muutoksia. Näin ollen ohjelmiston levitys ja sen päivittäminen jatkuvat ilman tietoa siitä, että ohjelmiston turvallisuus on rikottu. (Microsoft Learn 2022).

Tämän kaltaisia kyberhyökkäyksiä voi torjua lisäämällä tunnisteavainten ja digitaalisten ”allekirjoitusten” käyttöä. Esimerkiksi kaikki sivuston osat, mukaan lukien asetustiedostot, XML-tiedostot ja skriptit kannattaa allekirjoittaa kehittäjien puolesta, jotta tekijät ja tiedostojen alkuperäisyys voidaan varmistaa. Jos sovellus tai sivusto käyttää avointa lähdekoodia jossain osassa, kannattaa olla tietoinen siihen liittyvistä riskeistä.

5.5 Privilege escalation

Privilege escalation-hyökkäyksessä yritetään nimensä mukaisesti nostaa oikeuksia aina ylemmälle tasolle, niin pitkään että saadaan haltuun oikeudet, joilla päästään käsiksi haluttuihin tietoihin. Hyökkäys alkaa kuin monet muutkin, etsimällä tietoturvaheikkouksia palveluista. Kun pääsy palveluun on saatu, ei hyökkääjällä kuitenkaan todennäköisesti ole kovin korkeatasoisia oikeuksia. Hyökkääjä voi tällaisessa tilanteessa hyödyntää eri käyttäjien oikeuksia, joista jotkut ovat usein laiskasti mietittyjä. Jos perustason käyttäjälle on annettu esimerkiksi johonkin tietokantaan jostain syystä korkeammat oikeudet, hyökkääjän on mahdollista hyödyntää tätä saadakseen enemmän oikeuksia palveluun.

Tällaiselta hyökkäykseltä puolustautumiseen on monia tapoja, joista jotkut ovat vieläpä helppoja toteuttaa. Kaksivaiheinen vahvistus kaikilla tunnuksilla vaikeuttaa salasanojen arvaamista ja tietojen kalastelun toimivuutta. Myös palvelun oikeudet pitää miettiä huolella, eikä antaa perustason käyttäjille minkäänlaisia korkeampia oikeuksia ilman kunnon syitä.

5.6 SQL-injektio

SQL-Injektiot ovat hyökkäys, jota käytetään verkkosivujen tietokantoja vastaan. Verkkosivut ovat alttiit hyökkäyksille, jos sivuilta löytyy palsta johon käyttäjä voi itse syöttää tekstiä. Jos palstaa ei ole eristetty, hyökkääjä voi antaa palstan kautta suoraan komentoja sivuston SQL-palvelimelle, jonka kautta hyökkääjä voi esimerkiksi saada takaoven järjestelmään, saada henkilökohtaisia tietoja hallintaansa tai tyhjentää koko tietokannan. (W3schools n.d.)

SQL-injektion mahdollisuus voidaan poistaa validoimalla syötteet ja muuttamalla sivuston koodia, jotta käyttäjän syötettä ei ikinä käytetä suoraan. On myös suositeltavaa piilottaa tietokantavirheet käyttäjiltä, jotta hyökkääjät eivät saa hyökkäystä helpottavaa tietoa esimerkiksi tietokannan rakenteesta. (Acunetix n.d.)

5.7 Wordpressin lisäosat

Wordpressin lisäosakaupasta saa ladattua kaikenlaisia lisäosia laajentamaan järjestelmän ominaisuuksia. Monet lisäosat ovat hyödyllisiä ja kannattavia käyttää, mutta lisäosien mukana tulee myös turvallisuushaasteita. Syyskuussa 2022 WPGateway-lisäosassa havaittiin haavoittuvuus, jonka kautta hyökkääjä voi lisätä uuden järjestelmänvalvojan sivulle ja ottaa sivuston hallintaansa. Tämä haavoittuvuus on johtanut yli 280 000 hyökkäykseen verkkosivuja vastaan (Rees 2022).

Wordpressiä käytettäessä ei koskaan kannata pitää asennettuna lisäosia, jotka eivät ole aktiivisessa käytössä. Ylimääräiset lisäosat johtavat laajempiin haavoittumismahdollisuuksiin ja voivat jopa hidastaa sivuston toimintaa. Talalaevin (2021) mukaan uusia lisäosia asentaessa kannattaa olla varuillaan ja tarkistaa lisäosan tiedot ja päivityshistoria. Myös arvioista voi olla apua lisäosan turvallisuuden kartoituksessa. Asennetut lisäosat kannattaa pitää päivitettyinä, jotta mahdolliset bugit ja haavoittuvuudet eivät johdu vanhentuneesta lisäosaversiosta. (Talalaev 2021.)

6 Ohjeistuksen luonti

Tämän ohjeistuksen valmistelu aloitettiin tutkimustyöllä, jolla voitiin perustella tehtävät asiat ja niiden sisällytys ohjeistuksessa. Ohjeistus kirjoitettiin ensin erillisessä Word-tekstitiedostossa, joka löytyy liitteistä. Ensin tehtiin sisällysluettelosta alustava versio, jonka perusteella alettiin asentamaan ja konfiguroimaan palvelinta ja ohjelmistoja. Asennuksen ja konfiguroinnin eri vaiheista otettiin kuvakaappauksia, jotka liitettiin oppaaseen. Kuvankaappausten yhteydessä oppaassa kirjoitettiin jokaisessa vaiheessa tehtävät toimet.

Oppaassa edetään loogisessa järjestyksessä, jossa ensin tehdään laajemmat yleisasiat, kuten Wordpressin asennus ja peruskonfigurointi ja myöhemmin mennään spesifimpiin tehtäviin, kuten eri hyökkäysten vastatoimien konfigurointiin.

7 Läpäisytestaus ja validointi

Jotta voidaan todeta, oliko ohjeistuksessa kerrotuista ohjeista mitään hyötyä tietoturvan kannalta, täytyy sivusto auditoida eli tarkastaa. Sharman (2022) mukaan läpäisytestauksessa on kolme vaihetta: kartoitus, skannaus ja hyväksikäyttö. Kartoitusvaiheessa tarkoituksena on saada kohteesta mahdollisimman paljon tietoa, jotta tulevia toimia varten järjestelmästä on tarpeeksi tietoa. Skannausvaiheessa jo tiedetään jotain järjestelmästä ja voidaan käyttää tarkempia tiettyihin järjestelmiin tarkoitettuja työkaluja. Tässä vaiheessa tarkoituksena on skannata kohdejärjestelmää ja löytää heikkouksia hyödynnettäväksi. Viimeisessä vaiheessa voidaan hyödyntää opittuja heikkouksia ja käyttää kyseisiä heikkouksia lisätiedon hankkimiseen. (Sharma, 2022.) Tällä kertaa keskityttiin kahteen ensimmäiseen vaiheeseen, sillä tarkoituksena oli vain saada tietoa siitä, miten tietoturvaa voi vielä parantaa ja mikä ei ole onnistunut.

Läpäisytestauksessa käytettiin Kali Linux-virtuaalikonetta. Kyseiseen käyttöjärjestelmään päädyttiin sen tarjoaman laajan työkaluvalikoiman ansiosta. Kali Linux sisältää vakiona yli 600 läpäisytestaustyökalua ja lisävaihtoehtoja on saatavilla laajalti (What is Kali Linux? 2022). Itse testaukseen käytettiin nmap-, WPScan-, sqlmap- ja XSSer-työkaluja.

Ensin sivusto skannattiin nmap-työkalulla. Nmap (network mapper) on ilmainen tietoturvaskanneri, joka on vakiona asennettu Kali Linuxissa. Työkalulla löydettiin ensimmäiseksi palvelimen avoimet portit. Avoimista porteista ei ole varsinaisesti haittaa, jos ne ovat toiminnassa olevien palveluiden aktiivisessa käytössä. Löytyi kuitenkin yksi avoin portti, joka on SSH-palvelun käytössä. Se, kannattaako portti sulkea, riippuu täysin omasta käyttötavasta. Tämän työn tekemiseen SSH-etäyhteyttä ei tarvittu, mutta oikeassa käyttöympäristössä se voi olla hyödyksi. Avointen porttien lisäksi nmap löysi myös NGINX-palvelinohjemiston ja Wordpressin versionumerot. Näistä voisi olla hyötyä hyökkääjille, varsinkin jos versiot ovat vanhentuneita. Muutamalla lisäkomennolla löytyivät myös Wordpress-sivustolla käytetyt lisäosat ja niiden versionumerot. Myös tästä voi olla hyötyä hyökkääjälle, sillä vanhentuneet ja muut epämääräiset lisäosat voivat lisätä palvelimen hyökkäyspintaa.

Seuraavaksi voitiin siirtyä skannaamaan sivusto WPScan-työkalulla. Tämäkin työkalu oli jo asennettu, joten sen käyttöönotto onnistui helposti komentoriviltä. Skanneri sai nopeasti selville useita asioita sivustosta. Koska hakemiston selaus oli otettu aiemmin pois käytöstä, skanneri ei pystynyt näkemään Wordpress-asennuksen rakennetta. Ongelmiakin kuitenkin löytyi. XML-RPC protokolla oli käytössä sivustolla, joka saattaa olla kyseenalaista tietoturvaa ajatellen. Protokollassa on ollut useita tietoturvaongelmia aiemmin ja sen käyttö ei ole pakollista sivustolla, jos mikään palvelu ei tarvitse sitä. Skanneri löysi myös sivustolla olevan käyttäjätunnuksen. Käyttäjän tunnus ja nimimerkki ovat samat, joka ei ole hyväksi tietoturvan kannalta. Jos käyttäjätunnus löytyy helposti, sitä voi käyttää brute force-hyökkäyksissä hyväksi. Skanneri huomasi myös oikean heikkouden Wordpressissä, joka oli huomattu kuukausi sitten. Haavoittuvuus on kuitenkin pieni ja sellainen, johon ei ole tullut vielä päivitystä.

SQLmap-työkalulla voidaan testata sivuston turvallisuutta SQL-injektiohyökkäyksiä vastaan. Työkalu tunnisti, että sivustokartta on piilossa, eikä löytänyt muitakaan heikkouksia sivustossa. Yksi syy tulokseen on siinä, että tutkittu sivusto on hyvin yksinkertainen, eikä sisällä monimutkaisia elementtejä, jotka saattaisivat olla riskialttiita. Sivusto skannattiin myös XSSer-työkalulla, joka ei havainnut sivustolla XSS-heikkouksia.

8 Pohdinta

8.1 Tulokset ja johtopäätökset

Opinnäytetyössä tarkasteltiin itse isännöidyn Wordpress-palvelimen tietoturva ja hyödyllisimpiä toteutettavia toimia. Selvitystyössä otettiin huomioon käyttöjärjestelmän ja palvelinohjelmiston valinta, Wordpressin konfigurointi sekä otettiin selvää yleisimmistä hyökkäyksistä, joita verkkosivuille kohdistuu. Tutkimustyön tulokset toteutettiin oikeassa palvelinympäristössä, jonka vaiheista kirjoitettiin kirjallinen ohjeistus. Ohjeistuksen validiteettia testattiin yleisillä läpäisytestauksen työkaluilla, joilla voitiin havainnoida, oliko tehdyillä asioilla ollut positiivista vaikutusta palvelimen tietoturvan kannalta.

Tutkimuksen aikana tuli selväksi se, miten monisäikeinen aihe tietoturva on, ja miten monimutkaista on tehdä palvelimesta mahdollisimman tietoturvallinen. Tässä opinnäytetyössä otettiin selvää hyvistä toteutettavista käytänteistä, mutta aiheesta kiinnostuneille ja mahdollisimman hyvää turvaa hakeville on tekemistä loputtomasti enemmän eri osa-alueilta. Positiivisella puolella selvisi myös, että työkaluja ongelmien ratkaisemiseen on runsaasti eri taitotasoille aloittelijasta ammattilaistasoon asti ja tiettyynkin ongelmaan voi olla useita ratkaisuja. Selvisi että harvoin millekään vaiheelle on vain yksi oikea ratkaisu, vaan ratkaisuja on monia ja niiden tärkeystaso vaihtelee.

Työn validointivaiheessa havainnoitiin, että tehdyillä muutoksilla ja oli ollut positiivinen vaikutus palvelimen tietoturvatasoon. Selväksi tuli kuitenkin myös se, että parannettavaa riittäisi edelleen. Työssä tehdyt muutokset tehtiin todella yksinkertaiselle perusverkkosivulle, jossa ei ole laajaa hyökkäyspintaa. Läpäisytestauksen ja validoinnin tulos saattaisi olla siis erilainen oikeassa käytössä olevalla sivustolla, jossa on elementtejä ja osia perussivuun verrattuna moninkertaisesti. Se ei tarkoita, että tehdyt toimet olisivat olleet turhia, vaan että oikealle sivulle kannattaisi tehdä vieläkin enemmän varmistuakseen sen turvallisuudesta. Käyttäjän kannattaa myös miettiä, mikä on omalla kohdalla kannattavin isännöintivaihtoehto verkkosivulle. Monet verkossa toimivat isännöintipalvelut tarjoavat helppokäyttöisiä ominaisuuksia sivujen turvallisuuden hallintaan ja palveluissa on yleensä jo vakiona hyvä tietoturvataso. Tällaisissa palveluissa vähenee myös riski siitä, että omien toimien seurauksena koko palvelin tai kotiverkko muuttuu alttiiksi avoimen internetin vaaroille. Itse isännöinti on kuitenkin toimiva vaihtoehto niille, joilla on kiinnostusta aiheeseen ja kärsivällisyyttä ongelmanratkaisuun.

8.2 Luotettavuus

Työn ja etenkin kirjoitetun oppaan luotettavuuteen vaikuttaa se, että kirjoittaja on tietoturva-aiheessa vasta aloittelija, eikä omaa alalta laajaa kokemusta ja tietämystä. Siksi ohjeistusta ei kannata pitää täysin luotettavana, vaan mieluummin suuntaa antavana oppaana aiheisiin, joihin kannattaa kiinnittää huomiota. Oppaan paikkansapitävyys tulee myös todennäköisesti heikentymään sitä myöten, mitä pidempi aika sen kirjoittamisesta on kulunut jatkuvien päivitysten ja ohjelmistomuutosten takia. Opinnäytetyön luotettavuudessa täytyy myös ottaa huomioon se, että läpäisytestauksessa testattu ympäristö oli toiminnaltaan hyvin rajallinen eikä se täten kuvaa todellista oikean elämän tilannetta. Näin ollen on oletettavissa, että mikäli samat toimet tehtäisiin oikealla, tuotannossa olevalla palvelimella, olisivat tulokset huonommat kuin tässä työssä.

8.3 Eettisyys

Tutkimuseettisiä periaatteita pyrittiin noudattamaan koko työprosessin ajan. Lähteiden luotettavuutta pyrittiin arvioimaan kriittisesti ja työssä olevat lähdeviitteet on merkattu Jyväskylän ammattikorkeakoulun ohjeistuksen mukaisesti. Kaikki tekstissä käytetyt lähteet on listattu lähdeluetteloon. Työssä ei käsitelty ollenkaan henkilötietoja, eikä työhön kuulu salassa pidettävää aineistoa. Työllä ei ollut myöskään toimeksiantajaa, joten tutkimuslupaa tai eettistä ennakkoarviointia ei tarvittu työlle.

8.4 Jatkokehitys

Opinnäytetyössä kirjoitettua opasta on mahdollista jatkokehittää lisäämällä uusia osioita ja ottamalla käsittelyyn alueita ja aiheita, jotka siitä oli tässä vaiheessa rajattu pois. Oppaan ulkoasuun kannattaisi myös panostaa enemmän, mikäli sitä haluaisi jatkokehittää. Oppaan voisi esimerkiksi siirtää verkkoon, jossa siitä voisi tehdä visuaalisemman ja selkeämmin seurattavan kokonaisuuden. Tämä helpottaisi myös komentorivin tekstinpätkien käyttöä ja asetustiedostojen luontia, sillä tekstipätkät voitaisiin kopioida suoraan omaan toteutukseen.

Lähteet

Apache HTTP Server Project. N.d. Apache-palvelinohjelmiston kotisivu. Viitattu 30.10.2022. https://httpd.apache.org/

Apache Security Vulnerabilities. N.d. Apache-palvelinohjelmiston haavoittuvuuksia. Viitattu 18.11.2022. https://www.cvedetails.com/vulnerability-list.php?vendor_id=45&product_id=66&version_id=&

Base Image Servicing Lifecycles 2022. Tietoa Windows-palvelimien tuesta. Julkaistu 27.4.2022. Viitattu 11.11.2022. https://learn.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/base-image-lifecycle

Bister, T. 2019. Tietojenkäsittelyn opinnäytetyö: viittoja ja karttoja tutkimisen ja kehittämisen teille. Jyväskylä: Jyväskylän ammattikorkeakoulu. Jyväskylän ammattikorkeakoulun julkaisuja 272. Viitattu 11.10.2022. https://janet.finna.fi/Record/jamk.993577594806251

Brute Force Attack: A Definition. 2021. Selitys brute force-hyökkäyksistä. Julkaistu 1.12.2021. Viitattu 10.12.2022. https://us.norton.com/blog/emerging-threats/brute-force-attack

Brute Force Attacks. N.d. Tietoa brute force-hyökkäyksiltä suojautumisesta. Viitattu 1.12.2022. https://wordpress.org/support/article/brute-force-attacks/

Changing File Permissions. N.d. Wordpress-käyttöoikeuksien suositukset. Viitattu 16.11.2022. https://wordpress.org/support/article/changing-file-permissions/

diSessa, A. A. & Cobb, P. (2004). Ontological innovation and the role of theory in design experiments. The Journal of the Learning Sciences. Viitattu 12.10.2022. https://www.cs.uic.edu/~i523/edelson.pdf.

Dumont, S. N.d. What Salting Has to Do with Password Security. Viitattu 6.12.2022. https://voleer.com/blog/what-salting-has-to-do-with-password-security

Edelson, D. C. 2002. Design research: What we learn when we engage in design. The Journal of the Learning Sciences. Viitattu 12.10.2022. https://www.cs.uic.edu/~i523/edelson.pdf

FreeBSD Security Information. N.d. FreeBSD:n tietoturvaominaisuuksia. Viitattu 11.11.2022. https://www.freebsd.org/security/

Gall, R. 2023. The Wordfence 2022 State of Wordpress Security Report. Julkaistu 24.1.2023. Viitattu 24.1.2023. https://www.wordfence.com/wp-content/uploads/2023/01/The-Wordfence-2022-State-of-WordPress-Security-Report.pdf

Grima, M. 2022. Hacking WordPress websites & stealing WordPress passwords. Julkaistu 15.6.2022. Viitattu 12.12.2022. https://www.wpwhitesecurity.com/hacking-wordpress-websites-passwords/

Groeneveld, R. 2022. The password problem. Julkaistu 17.10.2022. Viitattu 28.10.2022. https://www.nomios.com/news-blog/password-problem/

IBM Security Services 2014 Cyber Security Intelligence Index. 2014. Analyysiä IBM:n keräämästä hyökkäysdatasta. Viitattu 19.11.2022. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

Jackson, B. 2022. Wordpress Security – 19 Steps to Lock Down Your Site. Julkaistu 12.12.2022. Viitattu 18.12.2022. https://kinsta.com/blog/wordpress-security/

Linux Statistics. 2022. Linux-käyttöjärjestelmäperheen käyttötilastoja. Viitattu 12.11.2022 https://truelist.co/blog/linux-statistics/

NGINX Security Vulnerabilities. N.d. NGINX-palvelinohjelmiston haavoittuvuuksia. Viitattu 18.11.2022. https://www.cvedetails.com/vulnerability-list/vendor_id-10048/product_id-17956/Nginx-Nginx.htmlhttps://www.cloudflare.com/learning/bots/what-is-rate-limiting/

NGINX. N.d. NGINX-palvelinohjelmiston etusivu. Viitattu 30.10.2022. https://nginx.org/en/

Ojasalo, K., Moilanen, T., Ritalahti, J. 2015. Kehittämistyön menetelmät – uudenlaista osaamista liiketoimintaan. Neljäs painos. Helsinki: Sanoma Pro.

Pedamkar, P. N.d. What is FreeBSD? Viitattu 10.11.2022. https://www.educba.com/what-is-freebsd/

Protect yourself from phishing. N.d. Viitattu 3.11.2022. https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing

Rees, K. 2022. Wordpress Plugin Vulnerability Abused in Zero-Day Exploit. Julkaistu 14.9.2022. Viitattu 7.12.2022. https://www.makeuseof.com/wordpress-plugin-abused-in-zero-day-exploit/

Sharma, S. How to Perform Wordpress Vulnerability Assessment & Penetration Testing. Julkaistu 17.1.2022. Viitattu 15.1.2022. https://www.getastra.com/blog/security-audit/wordpress-penetration-testing/

SQL Injection. N.d. Tietoa SQL-injektioista. Viitattu 21.11.2022. https://www.w3schools.com/sql/sql_injection.asp

Supply chain attacks. 2022. Tietoa supply chain-hyökkäyksistä. Julkaistu 14.12.2022. Viitattu 9.12.2022. https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide

Talalaev, A. 2021. Test WordPress Plugin Security. Tietoa lisäosien turvallisuuden testauksesta. Julkaistu 14.6.2021. Viitattu 8.12.2022. https://patchstack.com/articles/test-wordpress-plugin-security/

The CentOS Project. N.d. CentOS-käyttöjärjestelmän kotisivut. Viitattu 5.11.2022. https://www.centos.org/

The FreeBSD Project. 2022. FreeBSD-käyttöjärjestelmän kotisivut. Viitattu 10.11.2022. https://www.freebsd.org/

Tietoturva. 2020. Yleistä tietoa tietoturvasta. Julkaistu 9.7.2020. Viitattu 26.10.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Tietoturvan inhimilliset ja fyysiset tekijät. N.d. Viitattu 2.11.2022. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-inhimilliset-ja-fyysiset-tekijat/

Tucakov, D. 2021. Linux vs. Windows Server: The Ultimate Comparison. Julkaistu 9.12.2021. Viitattu 11.11.2022. https://phoenixnap.com/blog/linux-vs-microsoft-windows-servers

Ubuntu user statistics. N.d. Ubuntu-käyttöjärjestelmän käyttötilastoja. Viitattu 30.10.2022. https://ubuntu.com/desktop/statistics#desktop-specs

Understanding Privilege Escalation. N.d. Tietoa privilege escalation-hyökkäyksistä. Viitattu 8.12.2022. https://www.cynet.com/network-attacks/privilege-escalation/#heading-1

Usage statistics and market share of Wordpress. 2022. Wordpressin käyttötilastoja. Viitattu 15.10.2022. https://w3techs.com/technologies/details/cm-wordpress

Usage statistics of web servers. 2022. Verkkopalvelimien käyttötilastoja. Viitattu 15.10.2022. https://w3techs.com/technologies/overview/web_server

Using UNIX Permissions to Protect Files. N.d. UNIX-käyttöoikeuksien selitys. Viitattu 28.10.2022. https://docs.oracle.com/cd/E19120-01/open.solaris/819-3321/secfile-60/index.html

Virustotal Ransomware Activity Report 2021. Julkaistu 4.10.2021. Viitattu 10.12.2022. https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf

What is HTTPS? N.d. Tietoa HTTPS-protokollasta. Viitattu 22.11.2022. https://www.cloudflare.com/learning/ssl/what-is-https/

What is Kali Linux? 2022. Tietoa Kali-käyttöjärjestelmästä. Julkaistu 9.9.2022. Viitattu 17.1.2023. https://www.kali.org/docs/introduction/what-is-kali-linux/

What is Linux? N.d. Perustietoa Linux-käyttöjärjestelmäperheestä. Viitattu 1.11.2022. https://www.linux.com/what-is-linux/

What is rate limiting? N.d. Tietoa pyyntöjen rajoittamisesta. Viitattu 6.12.2022. https://www.cloudflare.com/learning/bots/what-is-rate-limiting/

What is SQL Injection and How to Prevent It? N.d. Tietoa SQL-injektioista. Viitattu 7.12.2022. https://www.acunetix.com/websitesecurity/sql-injection/

What is the best Windows Server for security? 2021. Windows-palvelinversioiden vertailua. Julkaistu 25.2.2021. Viitattu 11.11.2022. https://blog.avast.com/best-windows-server-security-avast

What is TLS? N.d. Tietoa SSL- ja TLS-protokollista. Viitattu 22.11.2022. https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

What is Two-Factor Authentication? N.d. Viitattu 27.10.2022. https://authy.com/what-is-2fa/

Windows Server. N.d. Windows Server-palvelimen kotisivu. Viitattu 10.11.2022. https://www.microsoft.com/fi-fi/windows-server

Wordpress Salts: What They Are, How They Work, and How to Use Them. 2022. Selitys salasanojen suolaamisesta. Julkaistu 28.11.2022. Viitattu 1.12.2022. https://kinsta.com/knowledge-base/wordpress-salts/

Wordpress Statistics. N.d. Wordpressin käyttötilastoja. Viitattu 13.11.2022. https://wordpress.org/about/stats/

Wordpress XSS Attack. 2018. Tietoa XSS-hyökkäyksistä. Julkaistu 14.11.2018. Viitattu 10.12.2022. https://secure.wphackedhelp.com/blog/wordpress-xss-attack/

X-Force Threat Intelligence Index 2022. Analyysiä IBM:n keräämästä hyökkäysdatasta. Viitattu 19.11.2022. https://www.ibm.com/reports/threat-intelligence/

Liitteet

Liite 1. Opas itse isännöidyn Wordpress-palvelimen tietoturvatoimiin

Opas itse isännöidyn Wordpress-palvelimen tietoturvatoimiin

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

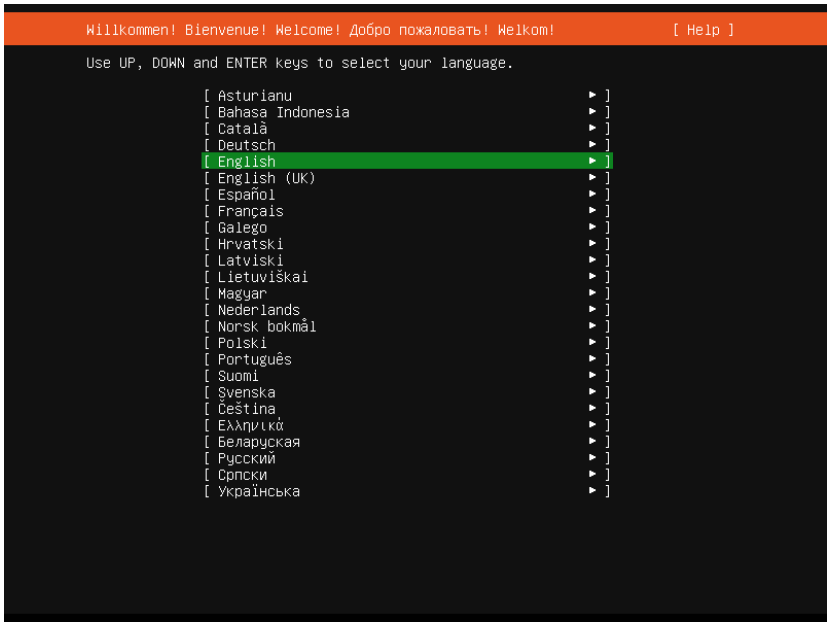
1 Johdanto

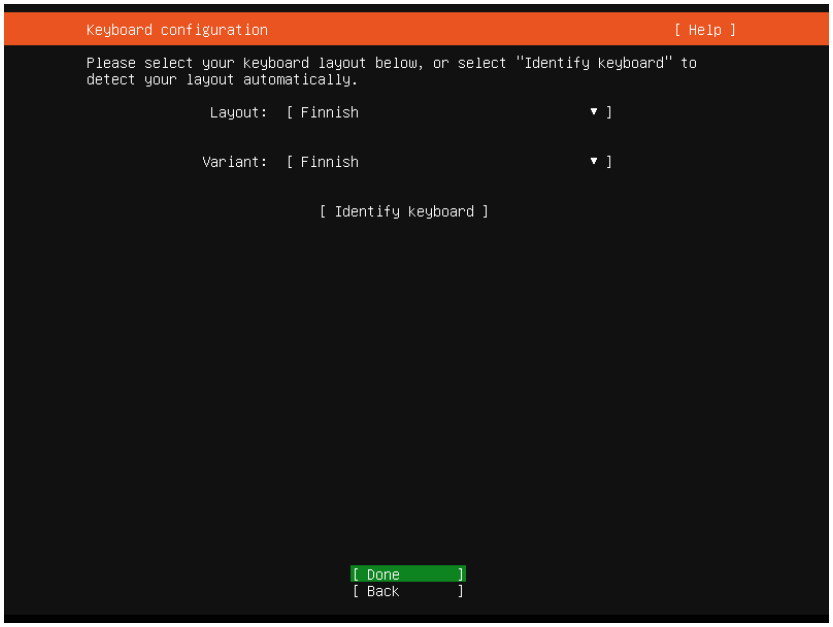
Tässä oppaassa on tavoitteena selventää itse isännöidyn Wordpress-palvelimen tietoturvaan liittyviä asennusvaiheita. Oppaan ei ole tarkoitus olla kaiken kattava, vaan se toimii hyvänä aloituspintana oman palvelimen tietoturvatoimiin. Tämä opas on tehty käyttäen Virtualbox-ohjelmistoa käyttöjärjestelmän virtualisointiin, joka helpottaa oppaan tekoa. Komentorivillä tehtävät komennot on aina laitettu omalle rivilleen ja niitä edeltää #-merkki selkeyttämään vaiheita.

2 Käyttöjärjestelmän asennus ja konfigurointi

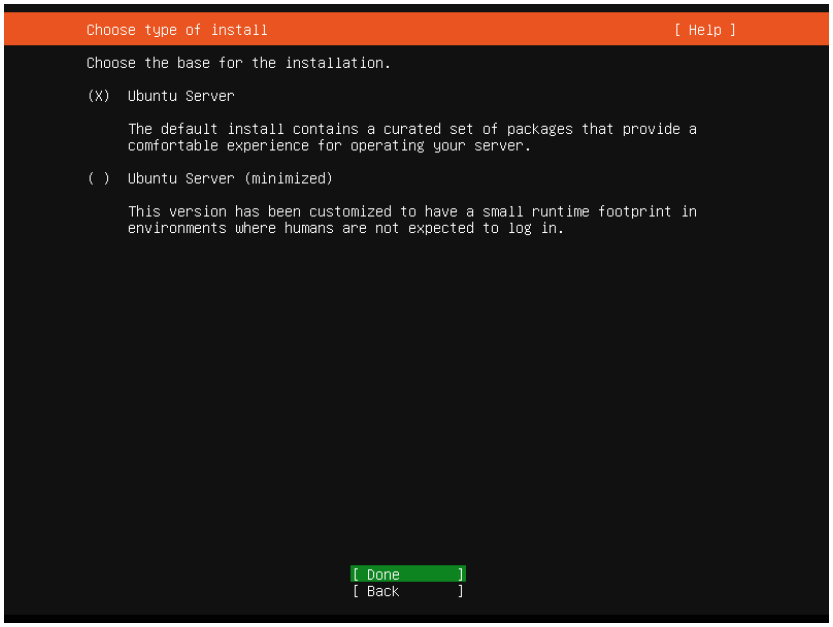
Valittu käyttöjärjestelmä, jonka päälle tässä oppaassa asennetaan kaikki muut ohjelmistot on Ubuntu Serverin 22.04.1 LTS-versio. Ubuntu valikoitui Linux-distribuutioiden joukosta sen vakiona olevan tietoturvatason, helppokäyttöisyyden, laajan tuen ja hyvien oletusominaisuuksien ansiosta. Ubuntun palvelinversiossa ei ole visuaalista käyttöliittymää, joten kaikki toiminnot tehdään komentorivin kautta. Se saattaa vaikuttaa alussa haastavammalta, mutta palvelinkäytössä visuaalinen käyttöliittymä on usein ylimääräinen ja tarpeeton lisäys.

Kun pääset aloittamaan asennuksen, joudut heti tekemään valintoja. Valitse haluttu kieli ja näppäimistön asettelu.

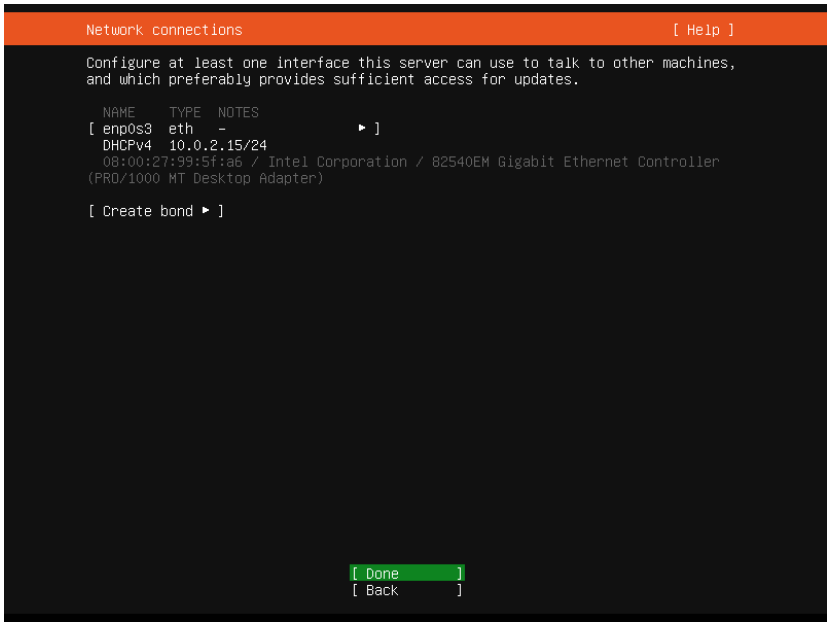




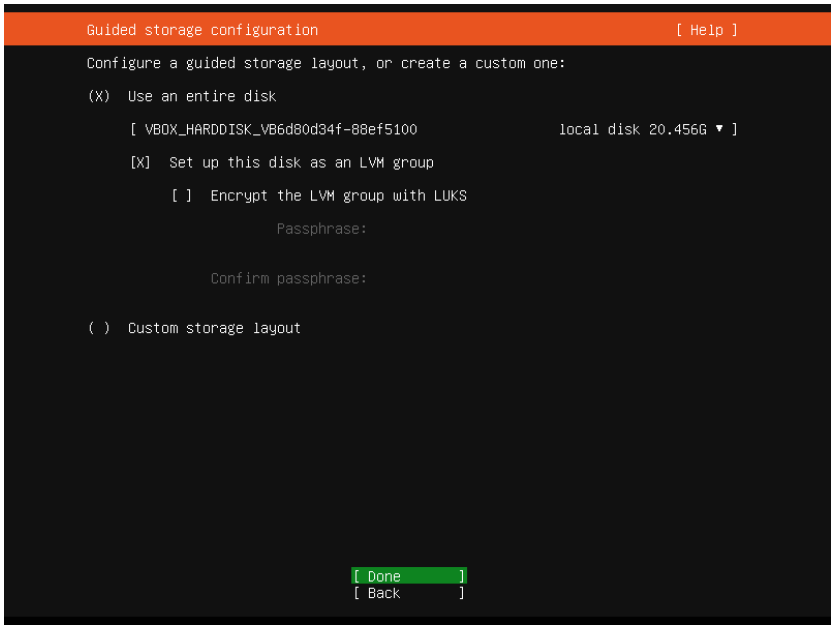
Seuraavassa osassa valitaan asennustyyppi. Valitaan tällä kertaa Ubuntu Server, sillä haluamme koko version minimoidun version sijaan, sillä minimoitu versio on tarkoitettu erityisesti automatisoitua laajan skaalan käyttöönottoa varten.



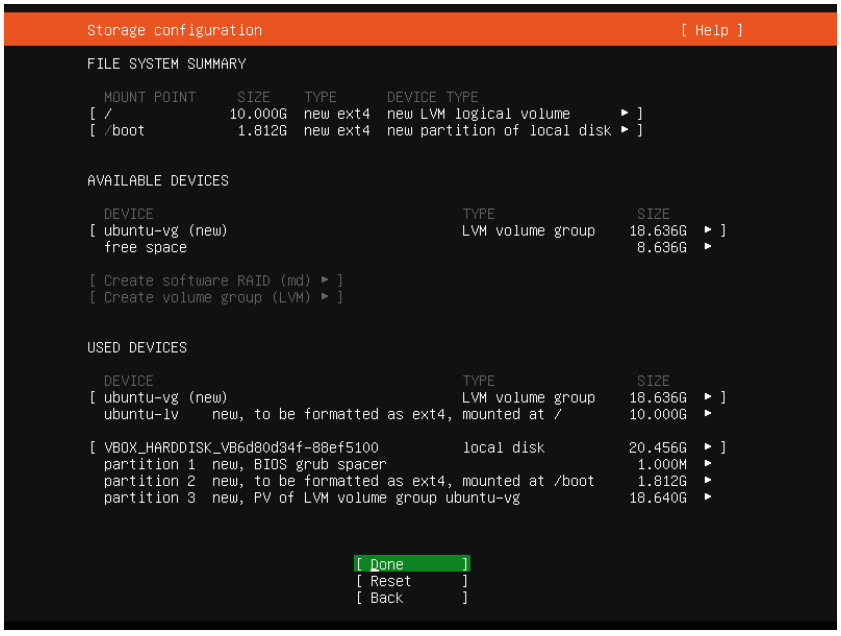
Kannattaa myös valita kohta ”Search for third-party drivers” jonka avulla asennusohjelma yrittää etsiä ajureita järjestelmälle, johon käyttöjärjestelmä asennetaan. Seuraavassa ruudussa valitaan verkkoyhteys, valitse siis se yhteys mitä haluat käyttää. Palvelinympäristössä on suositeltavaa käyttää langallista yhteyttä sen kestävyyden vuoksi.



Seuraavaksi valitaan levy, johon käyttöjärjestelmä asennetaan. Valitse haluttu asema ja siirry seuraavalle sivulle.

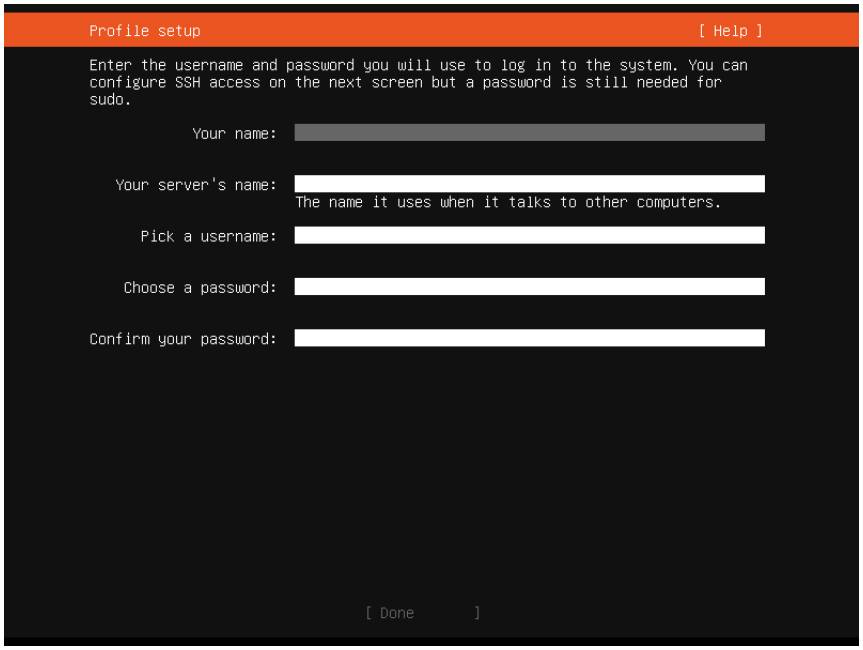


Viimeisellä sivulla voit vielä varmistaa, että olet varmasti valinnut oikean aseman käyttöjärjestelmälle.

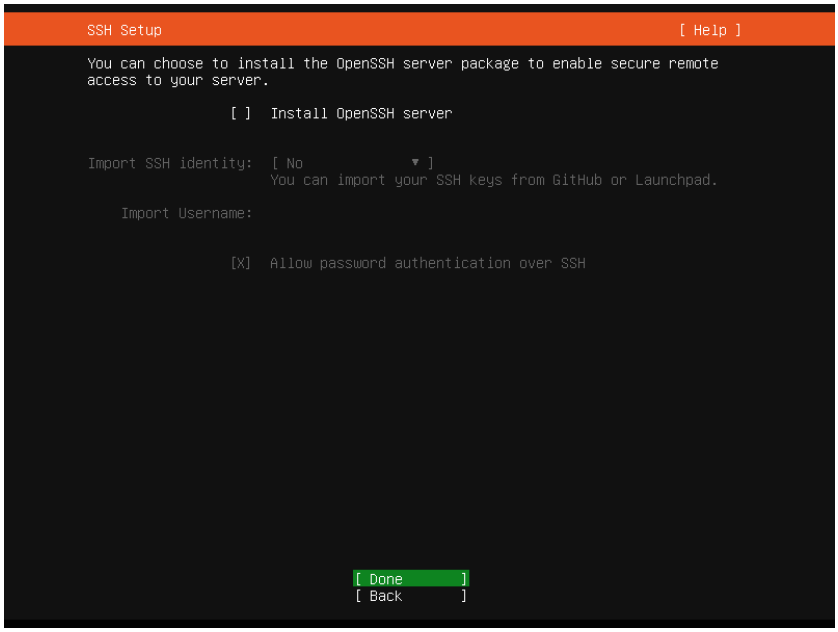


Kun olet tarkistanut, että kaikki on kunnossa, paina ”Done” ja pääset vielä tekemään profiilin itsellesi sekä nimeämään palvelimesi. Nimillä ei ole suurta väliä, mutta yleisimpiä oletusnimiä, kuten

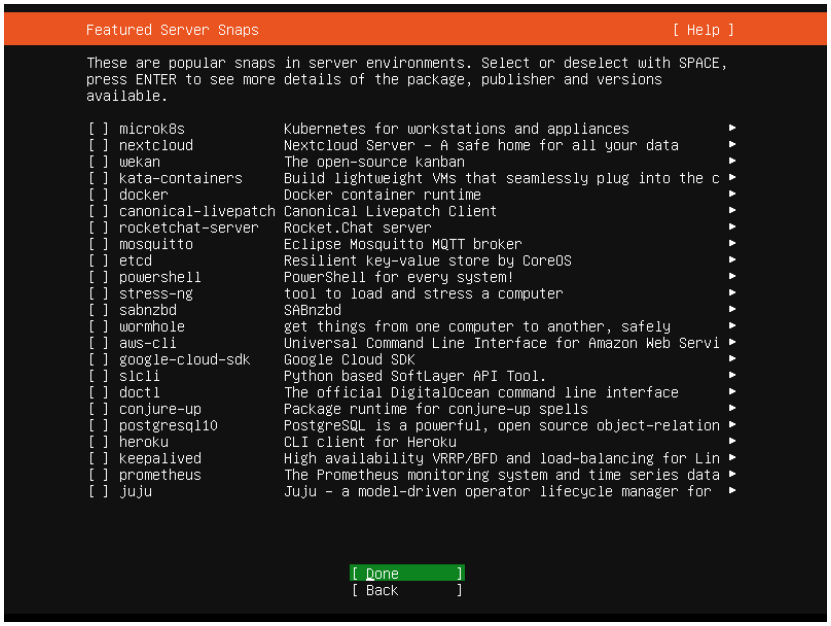
adminia ei kannata käyttää. Myöskään käyttäjäprofiilin salasanasta ei kannata tehdä helppoa eikä missään nimessä käyttää esimerkiksi qwerty-yhdistelmää salasanana. Jos haluat esimerkiksi ottaa etäyhteyden palvelimeesi, pääset kirjautumaan näillä tunnuksilla sisään. Jos käyttäjätunnus ja salasana ovat yleisiä ja helppoja arvata, helpotat tunkeutujien työtä turhaan.



Kun olet valmis, siirry seuraavaan kohtaan. Tässä vaiheessa voit valita, haluatko asentaa SSH-palvelinpaketin palvelimesi etäkäyttöä varten. Tässä tapauksessa SSH:ta ei asenneta, koska ei tarvita etäyhteyttä palvelimeen. Ylimääräisten ohjelmistojen ja varsinkin palvelinohjelmistojen asentaminen lisää mahdollisia kanavia, joiden kautta järjestelmään voidaan hyökätä.



Seuraavassa ja viimeisessä asennusruudussa listataan yleisiä asennettavia ohjelmistoja, joita voi asentaa halutessaan.



Listasta emme kuitenkaan tarvitse mitään, joten painetaan vain ”Done” ja käyttöjärjestelmän asennus alkaa. Hetken kuluttua, kun ruudulla lukee ”Install complete”, asennus on valmis ja voit

painaa ”Reboot now”. Kun palvelin on käynnistynyt uudelleen, edessä pitäisi olla komentorivi valmiina sisäänkirjautumista varten. Kirjaudu sisään aiemmin tekemilläsi tunnuksilla ja voit siirtyä seuraavaan vaiheeseen.

3 Palvelinohjelmiston asennus ja konfigurointi

Tähän oppaaseen palvelinohjelmistoksi valikoitui NGINX. Se valittiin sen tietoturvan ja modulaarisuuden vuoksi. Ennen kuin pääset asentamaan palvelinohjelmistoa, kannattaa kuitenkin ajaa seuraavat komennot:

```
# apt-get update
```

```
# apt-get upgrade
```

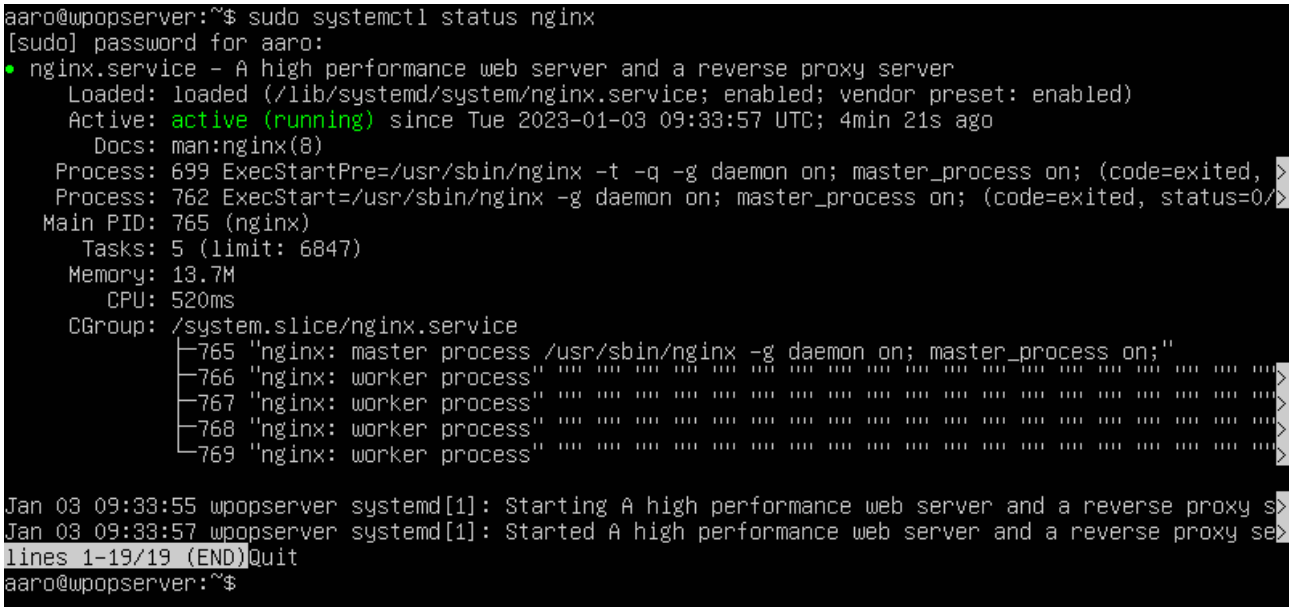
Näiden komentojen avulla voit varmistua siitä, että päivitykset ovat viimeisimmässä versiossa mahdollisimman sujuvan asennusprosessin mahdollistamiseksi. Kun päivitykset ovat valmiit, päästään itse asennukseen, joka onnistuu komennolla:

```
# apt-get install nginx
```

Asennuksen valmistuttua palvelinohjelmiston pitäisi käynnistyä automaattisesti taustalla, se voidaan varmistaa seuraavalla komennolla:

```
# systemctl status nginx
```

Komennosta tulevan syötteen pitäisi näyttää suurin piirtein samalta kuin alla olevassa kuvassa. Vihreä teksti kertoo palvelimen olevan aktiivinen ja toiminnassa.



3.1 MariaDB:n asennus

Mariadb on tietokantaohjelmisto, jota käytetään tällä kertaa Wordpressin kanssa. Sen asentaminen onnistuu seuraavalla komennolla:

apt-get install mariadb-server

Asennuksen jälkeen ajetaan seuraava komento, jonka avulla tietokantapalvelu käynnistyy:

systemctl enable mariadb.service

Viimeisenä vaiheena ajetaan vielä komento, jonka avulla voidaan parantaa tietokannan tietoturvallisuutta esimerkiksi poistamalla käyttäjiä ja lisäämällä salasanan root-käyttäjille. Komennon avulla voidaan myös poistaa testitietokanta, johon kaikki käyttäjät pääsisivät vakioasennuksessa.

mysql_secure_installation

Secure installation-komennon aloitettua tulee useita kysymyksiä, joiden pohjalta pystytään suojaamaan tietokantaa. Ensin kysytään, haluatko vaihtaa root-salasanasi. Jos palvelimesi root-salasana on jo hyvä, voit kieltäytyä ja siirtyä seuraavaan vaiheeseen. Seuraavaksi ohjelmisto kysyy, haluatko poistaa anonyymit käyttäjät. Mariadb:ssä on vakiona anonyymi käyttäjä, jonka avulla kuka tahansa voi kirjautua palveluun ilman käyttäjätiliä. Tämä omaisuus on kuitenkin vain testausta varten, joten anonyymit käyttäjät kannattaa poistaa. Seuraavaksi sinulta kysytään, poistetaanko root-käyttäjältä mahdollisuus kirjautua palveluun muualta kuin itse palvelimelta. Tähänkin kannattaa valita kyllä, joka poistaa mahdollisuuden arvata root-salasanaa muualta. Seuraavassa kysymyksessä kysytään, haluatko poistaa testitietokannan, johon kuka tahansa voi päästä. Kanta on olemassa lähinnä testausta varten, ja se kannattaa poistaa viimeistään ennen palvelimen käyttöönottoa, mutta voimme tehdä sen nyt samalla. Viimeiseenkin kysymykseen kannattaa vastata kyllä, jotta oikeudet päivitetään heti. Tämän vaiheen jälkeen olet valmis ja Mariadb on asennettu! Seuraavassa vaiheessa päästään PHP:n asennukseen.

3.2 PHP:n asennus

Asennetaan PHP seuraavalla komennolla:

```
# apt-get install php8.1 php8.1-fpm php8.1-common php8.1-mysql php8.1-xml php8.1-xmlrpc
php8.1-curl php8.1-gd php8.1-imagick php8.1-cli php8.1-dev php8.1-imap php8.1-mbstring
php8.1-soap php8.1-zip php8.1-bcmath -y
```

Komento on pitkä, sillä samalla asennetaan tiettyjä yleisiä moduuleja, joita tarvitaan Wordpressin käyttämiseen.

3.3 Wordpress-tietokannan luominen

Nyt kun MariaDB on asennettu, voidaan luoda tietokanta Wordpressin käyttöön. Jotta niin voidaan tehdä, kirjaudutaan ensin palveluun seuraavalla komennolla:

```
# mysql -u root -p
```

Kirjautumisen jälkeen voidaan siirtyä luomaan tietokanta seuraavilla komennoilla. Vaihda toiseen komentoon käyttäjänimen ja salasanan tilalle sellaiset tunnukset, mitä haluat käyttää. Pidä mielessä tietoturva äläkä käytä yleisimpiä ja helposti arvattavia salasanoja tai käyttäjätunnuksia.

```
# CREATE DATABASE tietokanta;
```

```
# GRANT ALL ON tietokanta.* TO 'käyttäjänimi'@'localhost' IDENTIFIED BY 'salasana' WITH GRANT OPTION;
```

```
# FLUSH PRIVILEGES;
```

```
# exit
```

Komennot luovat ensin tietokannan, sitten antavat oikeudet tietokantaan valitulle käyttäjälle ja päivittävät oikeudet, jotta uudet asetukset alkavat toimia heti.

3.4 NGINXin konfigurointi Wordpressiä varten

Alat vihdoin lähestyä itse Wordpressin asennusta, mutta vielä on muutama asia, jotka pitää tehdä sitä ennen. Ensin luodaan kansio Wordpress-asennukselle:

```
# mkdir -p /var/www/html/wordpress/public_html
```

Seuraavaksi luodaan NGINX-palvelinlohko Wordpressille. Siirrytään ensin oikeaan kansioon:

```
# cd /etc/nginx/sites-available
```

Kun olemme oikean kansion sisällä, luodaan palvelinlohkolle konfigurointitiedosto:

nano wordpress.conf

Kirjoita tiedostoon seuraavat tiedot:

```
  GNU nano 6.2                                  wordpress.conf
server {
        listen 80;
        root /var/www/html/wordpress/public_html;
        index index.php index.html;
        server_name SUBDOMAIN.DOMAIN.TLD;

        access_log /var/log/nginx/SUBDOMAIN.access.log;
        error_log /var/log/nginx/SUBDOMAIN.error.log;

        location / {
                        try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                        include snippets/fastcgi-php.conf;
                        fastcgi_pass unix:/run/php/php8.1-fpm.sock;
        }

        location ~ /\.ht {
                        deny all;
        }

        location = /favicon.ico {
                        log_not_found off;
                        access_log off;
        }

        location = /robots.txt {
                        allow all;
                        log_not_found off;
                        access_log off;
        }


        location ~* \.(js|css|png|jpg|jpeg|gif|ico)$ {
                        expires max;
                        log_not_found off;
        }
}
```

Palvelinlohko voidaan aktivoida yhdistämällä konfiguraatiotiedosto emokansioon. Pysytään vielä samassa sites-available-kansiossa kuin aiemmin:

ln -s ../sites-available/wordpress.conf .

Ladataan vielä NGINX uudestaan, jotta tehdyt muutokset tulevat toimintaan:

```
# systemctl reload nginx
```

Katsotaan vielä, että NGINX toimii:

```
# systemctl status nginx
```

Jos NGINXin status on aktiivinen, kaikki on kunnossa ja voidaan vihdoin siirtyä Wordpressin asennukseen.

4 Wordpressin asennus ja konfigurointi

Nyt pääsemme vihdoin itse Wordpressin asennukseen. Mennään ensin aiemmin tekemäämme asennuskansioon:

```
# cd /var/www/html/wordpress/public_html
```

Ladataan Wordpress sen virallisilta sivuilta wget-komennolla:

```
# wget https://wordpress.org/latest.tar.gz
```

Tiedostot tulevat latauksessa pakattuna tar-tiedostona. Puretaan tiedostot näin:

```
# tar -zxvf latest.tar.gz
```

Siirretään kansiota hieman:

mv wordpress/* .

Poistetaan turhaksi jäänyt wordpress-kansio selkeyttämiseksi:

rm -rf wordpress

Vaihdetaan kansiossa olevien tiedostojen oikeuksia:

chown -R www-data:www-data *

chmod -R 755 *

Seuraavaksi nimetään uudelleen Wordpressin wp-config-tiedosto, johon sitten voidaan syöttää aiemmin luodun tietokannan ja wordpress-käyttäjän tiedot:

mv wp-config-sample.php wp-config.php

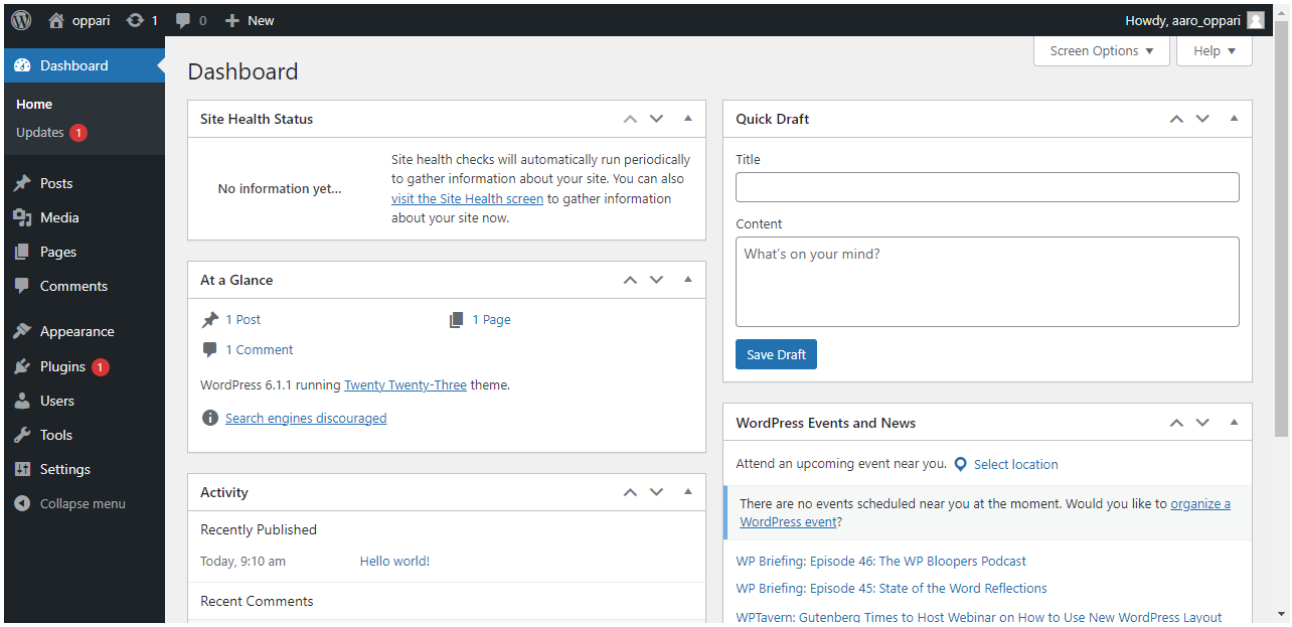
nano wp-config.php

Kohtiin DB_NAME, DB_USER ja DB_PASSWORD tulevat aiemmin luodut tiedot.

Sivuston suojaamisesi lisätään samaan tiedostoon myös suojausavain. Sen löytää seuraavalta sivustolta AUTH_KEY-kohdasta: https://api.wordpress.org/secret-key/1.1/salt/. Kun muutokset on tehty, tallenna tiedosto ja pääset asentamaan Wordpressin verkkoselaimessa.

Siirry haluamassasi verkkoselaimessa Wordpressin asennussivulle. Tässä tapauksessa se on tällainen: https://”palvelimen nimi”/wp-admin/install.php. Ensin valitset kielen, jonka jälkeen voit valita

sivuillesi nimen ja asettaa Wordpress-käyttäjänimen ja salasanan, joilla pääset myöhemmin kirjautumaan sivustolle. Kun olet syöttänyt oikeat tiedot, voit painaa asennusnäppäintä ja asennuksen pitäisi valmistua nopeasti. Asennuksen valmistuttua voit kirjautua äsken luomillasi tunnuksilla sivulle ja eteesi avautuu Wordpressin järjestelmänvalvojan etusivu.



5 Tietoturvatoimet

5.1 Varmuuskopiot

Ennen muita toimia asennetaan lisäosa, jonka avulla voidaan palauttaa sivusto siinä tilanteessa, jossa suojaustoimet eivät ole onnistuneet ja sivustolle on käynyt huonosti. Wordpressiin on saatavilla lukemattomia lisäosia, joiden avulla sivustosta voidaan tehdä ja tallentaa varmuuskopio. Nämä lisäosat tarjoavat myös usein mahdollisuuden tallentaa varmuuskopion tietyn ajan välein tai aina kun muutoksia sivustolle on tehty. Prosessi on automaattinen, joten lisäosat ovat käyttäjälle helppokäyttöisiä ja toiminnassaan melko näkymättömiä.

Helpoin tapa lisätä lisäosa on mennä Wordpressin hallintapaneelin etusivulta vasempaan sivupalkin kohtaan Plugins ja sen alta Add New. Asennetaan UpdraftPlus-lisäosa, joka on yksi suosituimmista varmuuskopiolisäosista ja jota käytetään yli 2 miljoonalla verkkosivulla. Kirjoitetaan hakupalkkiin ”UpdraftPlus” ja asennetaan lisäosa. Vaihtoehtoisesti lisäosan voi ladata osoitteesta https://wordpress.org/plugins/updraftplus/ ja asentaa manuaalisesti. Asennuksen valmistuttua siirrytään kohtaan Installed Plugins ja aktivoidaan asennettu lisäosa painamalla Activate. Nyt kun lisäosa on asennettu ja aktivoitu, siirrytään vasemmassa palkissa kohtaan Settings ja alivalikosta UpdraftPlus Backups. Näistä asetuksista voidaan hallita varmuuskopioinnin asetuksia, aseta haluamasi asetukset ja varmuuskopioille tallennussijainti ja olet valmis.

5.2 Yleinen tietoturva

Samoin kuin varmuuskopioihin, myös yleiseen tietoturvaan on saatavilla laajasti erilaisia lisäosia eri tarpeisiin. Asennetaan All in One WP Security & Firewall-lisäosa, jonka avulla voidaan tehdä monia asioita sivuston tietoturvan hyväksi. Monet näistä asioista voitaisiin myös tehdä manuaalisesti ilman lisäosia, mutta suositun ja luotetun lisäosan käyttö on helppoa kaikille käyttäjille ja mahdollisuus käyttäjävirheisiin sekä väärin tehtyihin muutoksiin pienenee. Ladataan lisäosa samalla tavalla kuin aiempikin, hakemalla sen nimi Wordpressin lisäosakaupasta. Asennuksen valmistuttua aktivoidaan lisäosa ja katsotaan tarkemmin sen asetuksia.

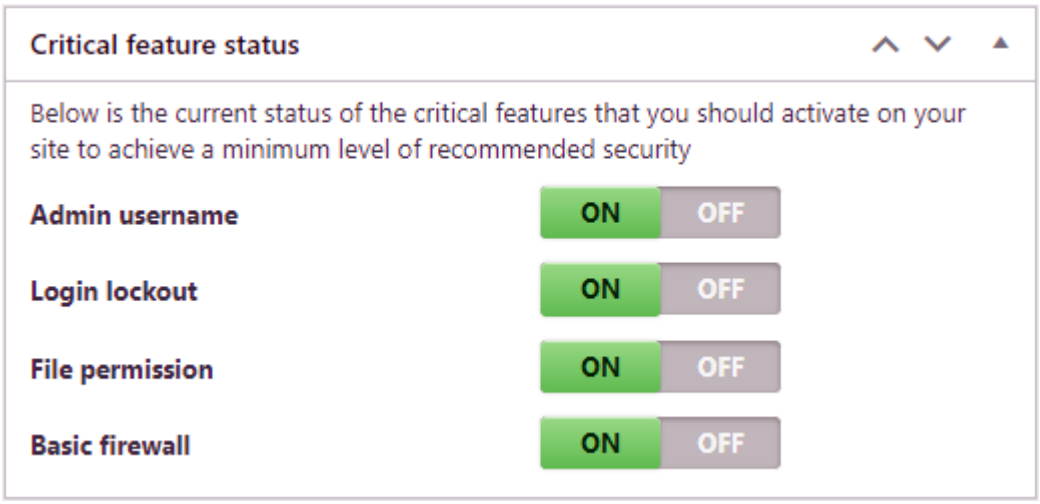
Vasempaan sivupalkkiin on ilmestynyt uusi painike, WP Security. Sen alavalikoista päästään laittamaan päälle useita tärkeitä ominaisuuksia. Siirrytään alavalikon kohtaan User Login. Sivulla on runsaasti vaihtoehtoja, joita voi valita oman tarpeen mukaan mutta laitetaan ainakin ensimmäinen niistä eli kirjautumisen esto päälle. Sen avulla kirjautuminen estetään valituksi ajaksi, kun kirjautumista on yritetty epäonnistuneesti tarpeeksi monta kertaa. Asetuksen käyttöön ottamalla voidaan kasvattaa sivuston suojaa brute force-hyökkäyksiä vastaan.

Siirrytään seuraavaksi alavalikon kohtaan Filesystem Security. Sivulla nähdään lista, josta voidaan tarkistaa Wordpress-palvelimen kansioiden ja tiedostojen oikeudet. Samalta sivulta voidaan myös

korjata tilanne, jos tiettyihin kansioihin tai tiedostoihin on asetettu liian laajat oikeudet. Tilanne on helppo korjata painamalla ”Set recommended permissions” jokaisen rivin kohdalta, jossa korjausta ehdotetaan. Näin oikeuksien muokkaus tapahtuu automaattisesti. Klikataan samalla sivulla olevaan toiseen valikkoon nimeltä ”PHP file editing”. Sieltä aktivoidaan ”Disable ability to edit PHP files”-kohta. PHP-tiedostojen editointioikeus kannattaa poistaa, sillä se on usein yksi ensimmäisistä työkaluista, joita hyökkääjä yrittää käyttää kirjautuakseen.

Seuraava sivu, jossa suositellaan tekemään muutoksia, on kohta ”Firewall”. Laitetaan ensin perustason palomuuri päälle kohtasta ”Enable basic firewall protection”. Tämä tekee muutaman eri asian: Se suojaa htaccess-tiedoston, rajaa ladattujen tiedostojen kokoa ja suojaa myös wp-config-tiedoston. Siirrytään seuraavksi palomuuriasetuksissa kohtaan ”Prevent hotlinks”. Ottamalla toiminnon käyttöön lisäosa estää käyttäjien muualta linkattujen kuvien käytön sivustolla.

Siirrytään kohtaan ”Brute Force”. Tältä sivulta voidaan asettaa useita asetuksia, jotka vaikeuttavat sivustolle kohdistettuja brute force-hyökkäyksiä. Kohdasta ”CAPTCHA settings” voidaan laittaa CAPTCHA-suojaus käyttöön kirjautumisvaiheessa, jonka tarkoitus on estää botteja yrittämästä kirjautumista. Tehdään sama alemmissa kohdissa myös unohdettu salasanalomakkeelle ja mukautetulle kirjautumislomakkeelle. Asetetaan CAPTCHA käyttöön myös kommenttikenttiin ”Spam Prevention”-kohdasta. Nyt olemme tehneet tärkeimmät suojausvaiheet, jotka lisäosa tarjoaa. Asetuksissa on mahdollista mennä halutessaan paljon syvemmälle, mutta nyt tehdyt toimet auttavat pääsemään minimitasolle turvassa. WP Security-lisäosan etusivulla olevan statussivun pitäisi nyt näyttää alla olevalta, joka kertoo kriittisten toimintojen olevan päällä.



6 Yleisimmiltä uhilta suojautuminen

6.1 Brute force

Brute force-hyökkäykset ovat yksi yleisimmistä tavoista hyökätä Wordpress-pohjaisille sivustoille. Olemme jo aiemmissa vaiheessa tehneet asioita, jotka lisäävät suojaa hyökkäyksiltä. Olemme asettaneet turvallisen käyttäjätunnuksen ja salasanan, rajanneet kirjautumisyrityksiä sekä olemme lisänneet CAPTCHA-suojauksen kirjautumislomakkeisiin. On olemassa muitakin nopeita toimia, joita voimme tehdä kasvattaakseme turvaa.

Lisätään ensin kaksivaiheinen vahvistus omille Wordpress-tunnuksille. Sen voit tehdä helposti aiemmin asennetulla WP Security-lisäosalla. Siirry lisäosan valikossa kohtaan ”Two Factor Auth”. Seuraavaksi skannaa sivulla oleva QR-koodi sillä tunnistautumissovelluksella, mitä haluat käyttää (Esimerkiksi Google Authenticator, Microsoft Authenticator tai Authy). Kun sovellus on tunnistanut uuden tunnuksen, voit sulkea sovelluksen. Nyt voit aktivoida kaksivaiheisen tunnistautumisen ylempänä sivulla kohdasta ”Activate two factor authentication”.

Otetaan hakemistojen selaus pois käytöstä, jotta kuka tahansa ei pääse näkemään, mitä Wordpress-kansioissa on. Hyökkääjät voivat etsiä hakemistosta haavoittuvaisia tiedostoja. Muutosta varten siirry palvelimella Wordpressin root-kansioon. Tässä tapauksessa kansioon päästään seuraavalla komennolla:

```
# cd /var/www/html/wordpress/public_html
```

Siirry muokkaamaan .htaccess-tiedostoa:

```
# sudo nano .htaccess
```

Lisätään tiedoston loppuun seuraava rivi:

```
Options -Indexes
```

Tallenna tiedosto ja olet valmis, hakemiston selaus on nyt estetty.

6.2 Man in the Middle

Tehokkain toimi man in the middle-hyökkäyksiltä suojautumiseen on TLS-sertifikaatin lisääminen sivustolle. Näin sivustolla saadaan HTTPS käyttöön ja yhteydet salattua. Tätä varten sivuston pitää olla jo verkossa toiminnassa. Verkkosivun julkaisuun ei kuitenkaan tässä oppaassa oteta kantaa, joten oletetaan että sivusto on jo julkinen.

TLS-sertifikaatteja on tarjolla useilla sivustoilla maksua vastaan, mutta saatavilla on myös ilmaisia palveluita, joilla sertifikaatti saadaan omalle sivustolle käyttöön. Käytetään tässä oppaassa certbot-nimistä työkalua, jolla saadaan muutaman komennon avulla sivustolle TLS-sertifikaatti. Certbot saadaan asennettua seuraavalla komennolla:

```
# sudo snap install –classic certbot
```

Sitten ajetaan seuraava komento, joka hankkii ja asentaa sertifikaatit:

```
# sudo certbot –nginx
```

Certbot uusii sertifikaatit automaattisesti eikä edellistä komentoa tarvitse käyttää kuin kerran. Automaattinen uusiminen voidaan kuitenkin testata seuraavalla komennolla:

```
# sudo certbot renew –dry-run
```

6.3 Cross Site Scripting (XSS)

Parhaat toimet cross site scripting-hyökkäyksiä vastaan ovat Wordpressin osien päivittäminen ja hyvän palomuurin käyttäminen. Päivittäminen on järjestelmänvalvojasta kiinni ja sivustolla on jo palomuuri toiminnassa. Voimme kuitenkin tehdä vielä lisää sivuston suojausta varten, joten katsotaan, miten sivuston syöttökentät voidaan puhdistaa. Sivustolla voi esimerkiksi olla seuraavanlainen tekstikenttä:

```
<input id="title" type="text" name="title">
```

Tällaiseen tekstikenttään käyttäjä voi kirjoittaa mitä tahansa, joka on riski sivuston turvallisuudelle. Kenttään lisättävät tiedot voidaan puhdistaa sanitize_text_field()-toiminnolla, jonka lisääminen kenttään on yksinkertaista. Muutetaan kentäsät seuraavanlainen:

```
$title = sanitize_text_field( $_POST['title'] );

update_post_meta( $post->ID, 'title', $title );
```

Puhdistusfunktio tarkistaa useita asioita kirjoitetusta tekstistä, kuten poistaa tägit ja rivin vaihdot tekstistä. Mikäli tekstikentällä on jokin tarkempi toiminnallisuus kuten sähköpostikenttä, on saatavilla tarkempia funktiota, jotka toimivat näissä tietyissä tilanteissa.

6.4 Supply Chain Attack

Supply chain attack eli toimitusketjuhyökkäys tulee yleisesti epämääräisten lisäosien ja teemojen mukana. Tämän riskin takia kannattaa tarkistaa huolellisesti kaikki lisäosat ja teemat, joita lataa sivustolle. Hyvä tapa suojautua on käyttää vain turvallisesta lähteestä, kuten Wordpressin sivustolta saatavia lisäosia. Jos haluat olla vieläkin varmempi lisäosan turvallisuudesta, vilkaise lisäosan päivityshistoriaa epämääräisten muutosten takia. Myös piraattiohjelmistoja kannattaa välttää, sillä niiden alkuperästä ja tehdyistä muutoksista ei voi olla täysin varma.

6.5 Privilege Escalation

Privilege escalation eli oikeuksien nostamishyökkäykseltä suojautuminen on hyvin käyttäjälähtöistä hyökkäyksen luonteen takia. Hyvät salasanakäytänteet ovat erittäin tärkeitä ja mikäli sivustolla on useita käyttäjiä, kannattaa heitä kouluttaa hyvistä käytänteistä ja salasanahygieniasta. Hyviä käytänteitä voi vielä voimistaa kaksivaiheisella tunnistautumisella, joka onkin jo toiminnassa sivustolla.

6.6 SQL-Injektiot

SQL-injectiot tapahtuvat sivustolla tekstinsyöttökenttien kautta. Data validation eli tiedon vahvistaminen on keino, jolla voidaan tarkistaa kenttiin syötetyn tiedon validiteetti. Kun syöttökentät on tehty oikein, ei niihin voi syöttää mitään, joka voisi tehdä haittaa sivustolle tai tietokantaan. Voidaan esimerkiksi tarkistaa, että puhelinnumerokenttään on syötetty vain numeroita eikä mitään

muita merkkejä. Validointi on liian laaja aihe, että sitä voisi tässä ohjeessa käsitellä kokonaan, mutta lisää tietoja saa Wordpressin kotisivuilta.

Kannattaa myös välttää dynaamisen SQL:n käyttöä sivustolla, sillä se toimii automaattisesti ja voi tällöin aiheuttaa tietoturvariskin. Sen sijaan suositellaan käyttämään valmiita lausuntoja ja kyselyitä.