LAPIN AMK
Lapland University of Applied Sciences

VERKKOSIVUSTON SUUNNITTELU JA TOTEUTUS LINUX-PALVELIMELLE

George Launoila

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2024

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	George Launoila	**Vuosi**	2024
Ohjaaja	Aku Kesti		
Toimeksiantaja	Heat By Nature Sweden AB		
Työn nimi	Verkkosivuston suunnittelu ja toteutus Linux-palvelimelle		
Sivumäärä	31		

Työn tavoitteena oli rakentaa modernit, saavutettavat, responsiiviset ja tietoturvalliset verkkosivut Linux-palvelimelle. Toimeksiantajana toimii Heat By Nature AB Sweden.

Ensimmäisessä osiossa käydään läpi verkkotunnuksen ja sähköpostin konfigurointeja sekä verkkosivun rakentamista. Vaihe sisälsi alustavan ulkonäön ja responsiivuuden suunnittelun ja niiden implementaatiot.

Toisessa osiossa tutustutaan Linux-ympäristöön ja yleisiin tietoturvakäsitteisiin sekä niiden käytännön sovelluksiin. Tässä vaiheessa tarkastellaan Apache HTTPD -palvelimen käyttöönottoa, haittaohjelmia, TSL/SSL-protokollaa ja palomuurin konfigurointia.

Projektin tuloksena on verkkosivusto, joka on rakennettu asiakkaan toiveiden mukaisesti. Verkkosivuston isännöinti Linux-palvelimella tarjoaa vapauden kolmansien osapuolten palveluista ja takaa nopeuden, turvallisuuden sekä vakauden.

Avainsanat Linux, palomuuri, palvelin, tietoturva, verkkotunnus, palvelin, WWW-sivut

LAPIN AMK
Lapland University of Applied Sciences

Abstract of the thesis

Information and Communication Technology
Bachelor of Engineering

Author	George Launoila	**Year**	2024
Supervisor(s)	Aku Kesti		
Commissioned by	Heat By Nature Sweden AB		
Title	Design and implementation of a website on a Linux server.		
Number of pages	31		

The objective of this thesis study was to create a modern, accessible, responsive and secure website on Linux server. The commissioner for this project was Heat By Nature AB Sweden.

First, the configuration of the domain and email, as well as the construction of the website were studied. This phase included the initial design and implementation of the appearance and responsiveness. After that, the Linux environment and general cybersecurity concepts and their practical applications were studied. The implementation of the Apache HTTPD server, malware, TSL/SSL protocols, and firewall configuration were explored.

The outcome of the thesis study is a website built according to the commissioner's specifications. Hosting the website on a Linux server provides freedom from third-party services and ensures speed, security and stability.

Keywords cyber security, firewall, Linux, server, web page

SISÄLLYS

KÄYTETYT LYHENTEET

DE	Desktop Environment, työpöytäympäristö
IDE	Integrated Development Environment, ohjelmointiympäristö
API	Application Programming Interface, ohjelmointirajapinta
px	Pixel, kuvapiste
MX record	Mail exchanger record, MX-tietue
DNS	Domain Name System, nimipalvelujärjestelmä
SSL/TLS	Secure Sockets Layer / Transport Layer Security, kryptografisia protokollia, jotka tarjoavat turvallisen tiedonsiirron internetissä.
HTTP/HTTPS	Hypertext Transfer Protocol / Secure, hypertekstin siirtoprotokolla
CA	Certification Authority, sertifikaattiviranomainen
IP address	Internet Protocol address, internetin protokollaosoite

1 JOHDANTO

Opinnäytetyön toimeksiantajana toimii Heat By Nature AB Sweden. Yritys myy ekologisia ja savuttomia lämmitysjärjestelmiä.

Tämä opinnäytetyö käsittelee sitä, miten voi rakentaa verkkosivuja omalla palvelimella. Opinnäytetyö selvittää, mikä GNU/Linux-käyttöjärjestelmä on ja miksi sitä käytetään palvelimissa. Lisäksi tarkastellaan palomuurin toimintaa ja sitä, miten verkkosivusto voidaan tehdä turvalliseksi.

Tämä opinnäytetyö on kaksiosainen. Ensimmäisen osion tavoitteena on suunnitella ja toteuttaa asiakkaalle verkkosivusto, joka on responsiivinen ja helppokäyttöinen. Toisessa opinnäytetyön osiossa otetaan käyttöön Linux-palvelin ja määritellään sen palomuuri.

Verkkosivuston tarkoituksena on esitellä asiakkaan yritystä ja sen palveluita. Verkkosivuston on oltava responsiivinen eli mukautuva eri laitteiden näyttöihin, kuten tietokoneisiin, tableteihin ja puhelimiin. Verkkosivuston on myös oltava helppokäyttöinen, eli sen on tarjottava selkeä ja intuitiivinen käyttöliittymä.

Linux-palvelimen käyttöönotto ja palomuurin määrittely on toinen osa opinnäytetyötä. Linux-palvelimen tarkoituksena on tarjota verkkosivustolle luotettava ja turvallinen isäntä. Palomuurin avulla voin hallita verkkoliikennettä ja suojata palvelinta ulkopuolisilta hyökkäyksiltä.

Tämä opinnäytetyö osoittaa osaamistani verkkosivustojen suunnittelussa ja toteutuksessa sekä Linux-palvelimien käyttöönotossa ja palomuurin määrittelyssä. Verkkosivustoni vastaa asiakkaan yrityksen tarpeita ja odotuksia.

2 VERKKOTUNNUS JA SÄHKÖPOSTIPALVELU

Verkkosivun rakentamisessa on oleellista saada yritykselle domain eli verkkotunnus. Paras mahdollinen verkkotunnus on luonnollisesti yrityksen oma nimi. Tämä ei tuottanut ongelmia, sillä sain varattua yritykselle .com-, .eu-, .org-, se-, .net-päätteiset verkkotunnukset.

Varaamiseen käytin Squarespace-palvelua. Ruotsalaista tunnusta varten käytin Godaddy-palvelua, sillä Squarespacella ei voi varata ruotsalaisia verkkotunnuksia. Määrittelin myös, että kaikki muut tunnukset välittävät .com-tunnukselle, sillä asiakas ei halua erikseen lokalisoituja sivuja.

2.1 Yrityksen sähköposti ja toiminta-ohjelmisto/ympäristö

Seuraava askel on perustaa yritykselle sähköpostit @heatbynature.com-päätteellä ja ottaa käyttöön mahdolliset toimisto-ohjelmat. Vaihtoehdot olivat Google Workspace, Microsoft Office ja Zoho Suite.

Päätökseni oli kompromissi, sillä otin Zoho Suiten käyttöön sähköposteja varten ja tarpeen vaatiessa toimisto-ohjelmiksi otetaan käyttöön LibreOffice. Zoho Suite on huomattavasti edullisempi, kuin kilpailijat. LibreOffice puolestaan on täysin ilmainen, sillä se on avoimeen lähdekoodiin perustuva ohjelmisto.

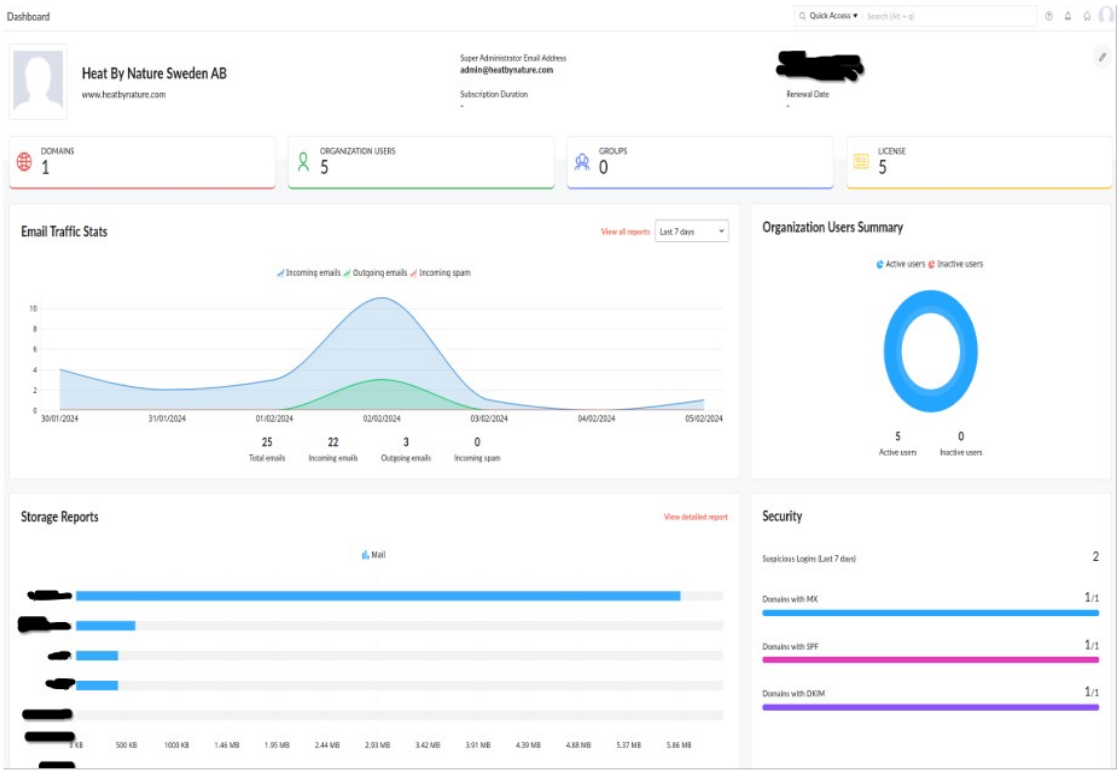
2.2 Sähköpostin yhdistäminen verkkotunnukseen

Sähköpostin yhdistäminen verkkotunnukseen on melko yksinkertaista. Yhdistäminen tapahtuu lisäämällä Zoho Suiten MX-tietueet verkkosivun DNS-asetuksiin ja määrittelemällä autentikaatiotietue, joka on piilotettu seuraavassa taulukossa tietoturvan vuoksi (taulukko 1).

Host	Type	Priority	Data
@	MX	50	mx3.zoho.eu
@	MX	10	mx.zoho.eu
@	MX	20	mx2.zoho.eu
@	TXT	N/A	zoho-verification=[redacted]

Taulukko 1. Verkkosivun DNS-asetukset Squarespace-palvelussa

Admin-paneelin kautta voin seurata liikennettä ja käyttäjiä. Seuraamalla varmistan, etteivät käyttäjätilit ole vaarantuneet. Käyttäjien nimet on piilotettu kuviosta (kuvio 1).



Kuvio 1. Näkymä Admin-paneelista

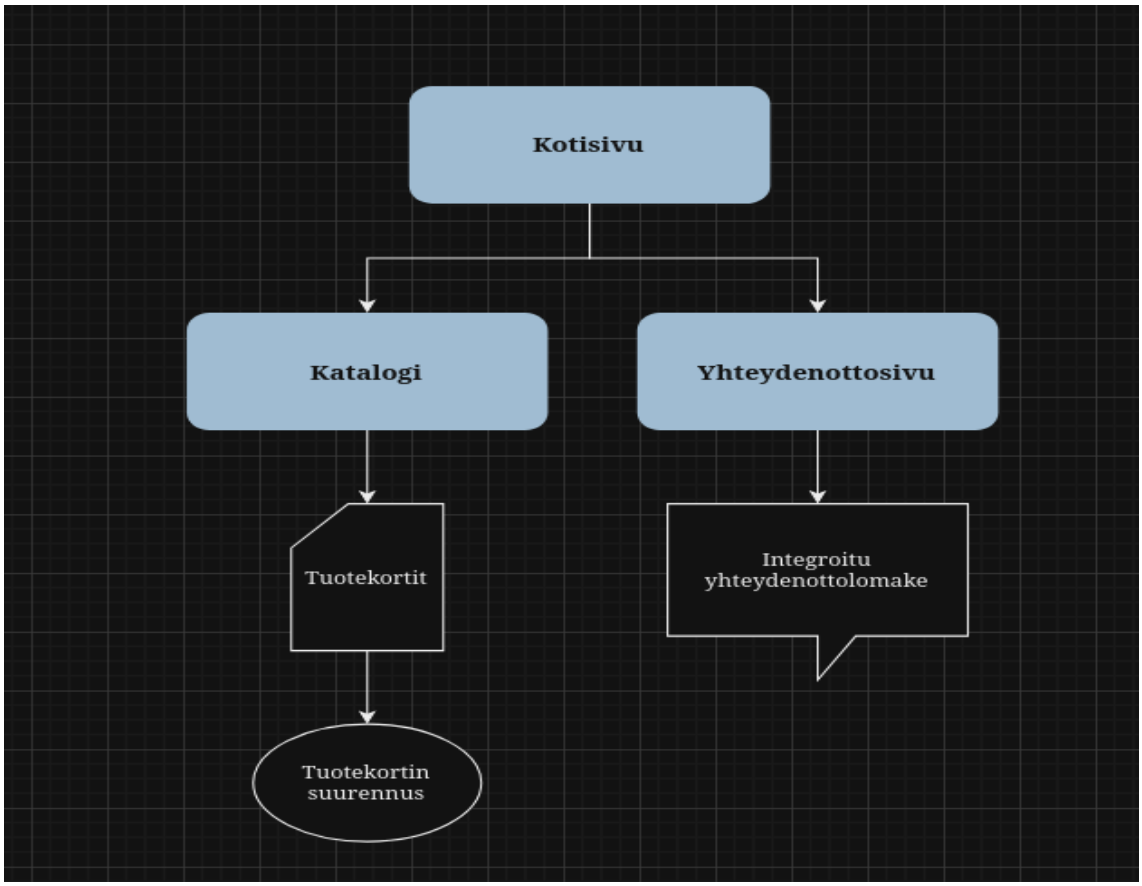
3 VERKKOSIVUSTON SUUNNITTELU

3.1 Verkkosivuston vaatimukset

Asiakas haluaa, että sivusto sisältäisi kolme sivua. Ensimmäinen on kotisivu, joka sisältää yrityksen iskulauseen sekä muut esittelytiedot.

Toinen sivu on katalogi, johon tulee näkyviin yrityksen myymät bioetanolitakat ja niiden tiedot. Katalogi on rakennettava niin, että tuotekortit voi helposti lisätä ja poistaa myynnistä.

Viimeinen sivu on varattu yhteydenottoa varten. Se tulee sisältää yhteydenotto-lomakkeen, jonka avulla käyttäjä voi helposti lähettää sähköpostia yrityksen myyntitilille kirjautumatta sisään mihinkään. (kuvio 2).



Kuvio 2. Verkkosivuston sivut ja ominaisuudet

3.2 Sivuston saavutettavuus

WCAG eli Verkkosisällön saavutettavuusohjeet ovat World Wide Web -konsortion kehittämiä ja ylläpitämiä ohjeistuksia, joita noudatan tässä projektissa. Ohjeistus jaetaan laajasti neljään periaatteeseen.

Havaittavuus eli käyttäjien on voitava havaita verkkosisältö jollain tavalla käyttäen yhtä tai useampaa aistiaan. **Hallittavuus** eli käyttäjien on voitava hallita käyttöliittymäelementtejä (esim. painikkeiden on oltava jollain tavalla klikattavissa - hiiri, näppäimistö, äänikomento jne.). **Ymmärrettävyys** eli verkkosisällön on oltava ymmärrettävää käyttäjilleen. **Toimintavarmuus** eli verkkosisällön on oltava kehitetty käyttämällä hyvin omaksuttuja verkkostandardeja, jotka toimivat eri selaimissa, nyt ja tulevaisuudessa. (World Wide Web Consortium 2021.)

3.3 Sivuston responsiivisuus

Keskeistä on varmistaa, että työpöytä- sekä mobiiliversioilla verkkosivustosta näytetään täysin identtiset tiedot. Tämän toteuttamiseksi on olennaista käyttää yhtä ja samaa HTML-koodia, jolloin erillisiä mobiiliversioita ei tarvita.

Tällainen lähestymistapa tunnetaan responsiivisena suunnitteluna, joka mahdollistaa sivuston automaattisen sopeutumisen eri laitteiden näyttökokoihin. Näin varmistetaan yhtenäinen ja saumaton käyttäjäkokemus riippumatta siitä, käyttääkö käyttäjä tietokonetta vai mobiililaitetta. Responsiivinen suunnittelu tekee myös sivuston ylläpidosta ja päivityksistä helpompaa, koska kaikki muutokset näkyvät kaikilla laitteilla samanaikaisesti. (Google for Developers 2023.)

3.4 Sivuston turvallisuus

HTTPS-protokolla on salausta käyttävä tietojensiirtoprotokolla, joka kehitettiin HTTP:n pohjalta. HTTPS lisää tunnistautumisen ja eheyden muuten turvattomaan protokollaan.

HTTPS mahdollistaa verkkosivustojen käyttäjille arkaluonteisen tiedon, kuten luottokorttinumeroiden, pankkitietojen ja kirjautumistunnusten turvallisen siirtämisen internetin yli. Tästä syystä HTTPS on erityisen tärkeä verkkotoimintojen,

kuten ostosten, pankkitoiminnan ja etätyön turvaamisessa. HTTPS on nopeasti muuttumassa standardiprotokollaksi kaikille verkkosivustoille, riippumatta siitä vaihdetaanko niiden välityksellä arkaluonteista tietoa käyttäjien kanssa vai ei. (SSL 2021.)

Tunnistautuminen toimii SSL/TLS-protokollan avulla. Verkkosivuston SSL/TLS-sertifikaatissa on julkinen avain, jota verkkoselain käyttää varmistaakseen, että palvelimelta lähetetyt asiakirjat (kuten HTML-sivut) on digitaalisesti allekirjoitettu vastaavan yksityisen avaimen kanssa. Jos palvelimen sertifikaatin on allekirjoittanut julkisesti luotettu sertifikaattiviranomainen (CA), selain hyväksyy sertifikaatin. Tämä tarkoittaa, että suurin osa selaimista ei enää hyväksy itse allekirjoitettuja sertifikaatteja. (SSL 2021.)

4 VERKKOSIVUSTON TOTEUTUS

4.1 Kotisivu ja teema

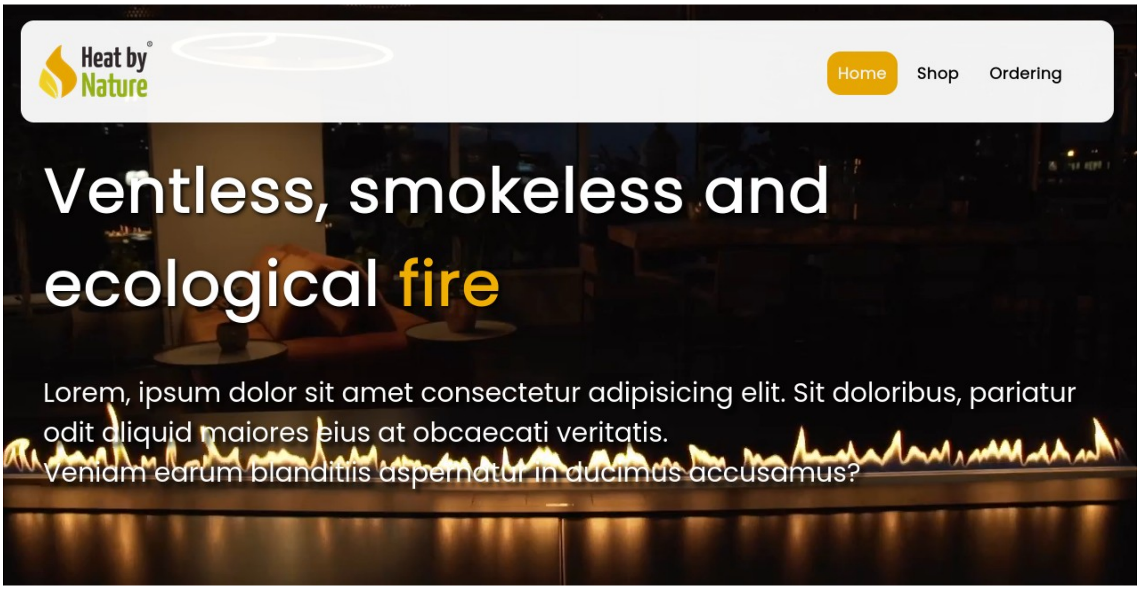
Ensimmäisenä loin Canva-palvelulla mallin tulevan sivuston kotisivusta (kuvio 3). Sivuston päävärin valitsin yrityksen logon liekistä. Käyttäen tätä väriä luon asiakkaalle tervetulleen olon ja samalla väri myös kuvastaa ekologisella tavalla tuotettua lämpöä, joka taas luo lisää tunnelmaa.

Kuvio 3. Canvalla tehty malli sivustosta

Asiakas piti visiostani ja hyväksyi mallin. Hyväksynnän jälkeen aloin toteuttaa sivustoa käyttäen Visual Studio Code IDE:ta ja Git-työkalua.

Verkkosivuston luomisprosessissa huomasin, että sivuston tausta teki tekstin lukemisesta hankalaa ja vaikeutti sivuston responsiivisuutta. Päätin luopua kuvasta ja otin käyttöön videon palavasta bioetanolitakasta. Muutos paransi responsiivisutta ja teki sivustosta nykyaikaisemman näköisen.

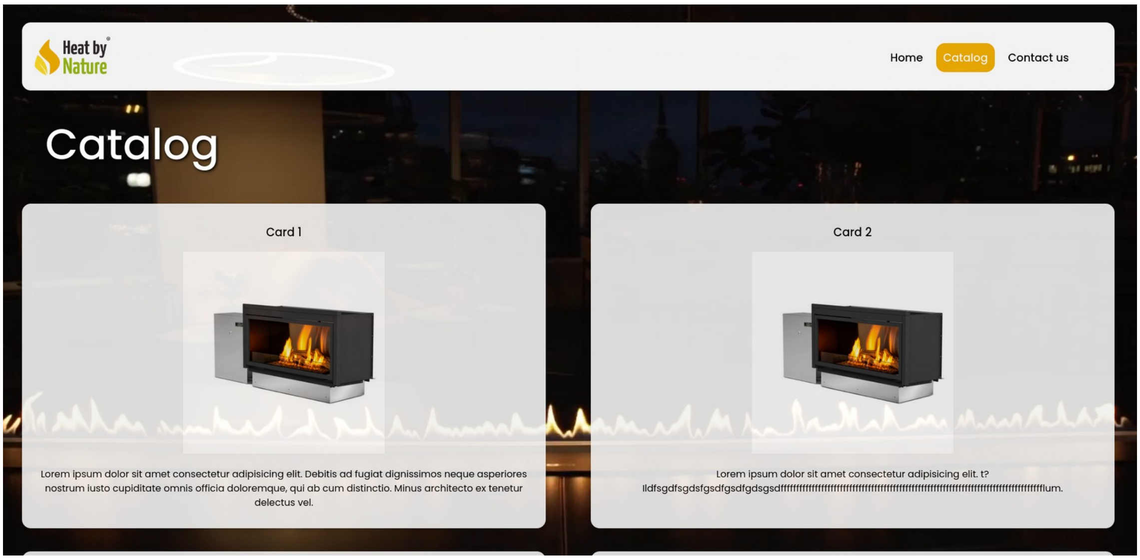
Helppolukuisuuden vuoksi muutin ylävalikon väriä näkyvämmäksi ja muutin navigointipainikkeiden väriä mustiksi. Painikkeet muuttavat väriä vasta aktiivisina (kuvio 4).



Kuvio 4. Lopullinen ulkonäkö

4.2 Katalogi

Katalogi-sivu seuraa kotisivun asettamaa teemaa. Sivun sisältö ovat tuotekortit, jotka sisältävät tuotteen. Jokaisessa kortissa on tuotteen nimi, kuva ja kuvaus (kuvio 5).



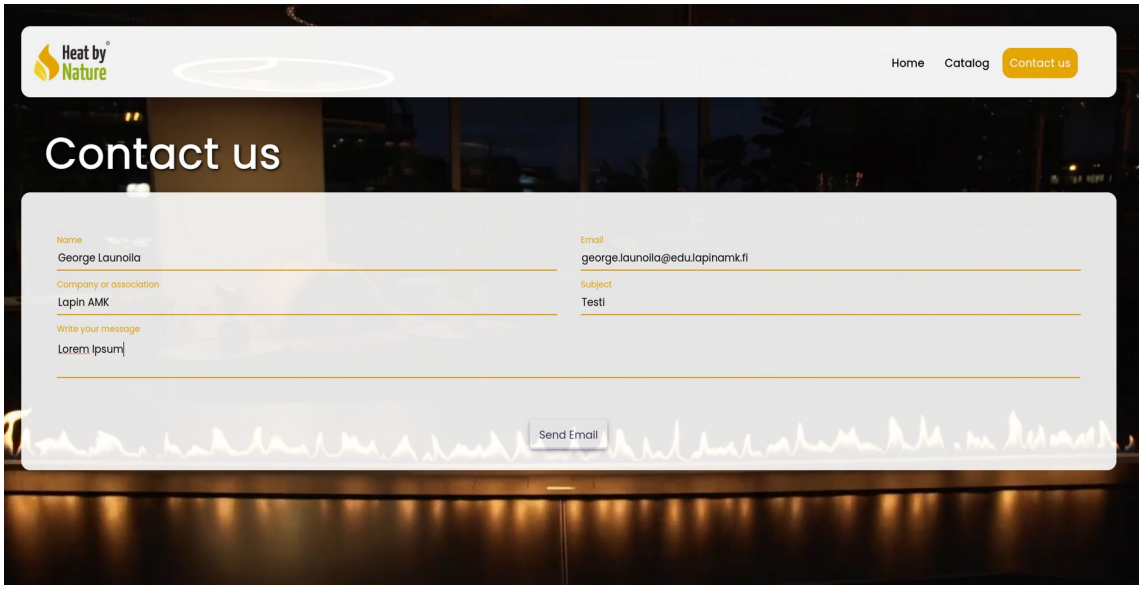
Kuvio 5. Näkymä katalogista

Jokaisen kuvan voi avata isoon näkymään. Tämän ominaisuuden rakentamiseen käytin JavaScriptin Fancybox-kirjastoa (kuvio 6).

Kuvio 6. Fancybox:illa tehty kuvan suurennus

4.3 Yhteydenottosivu

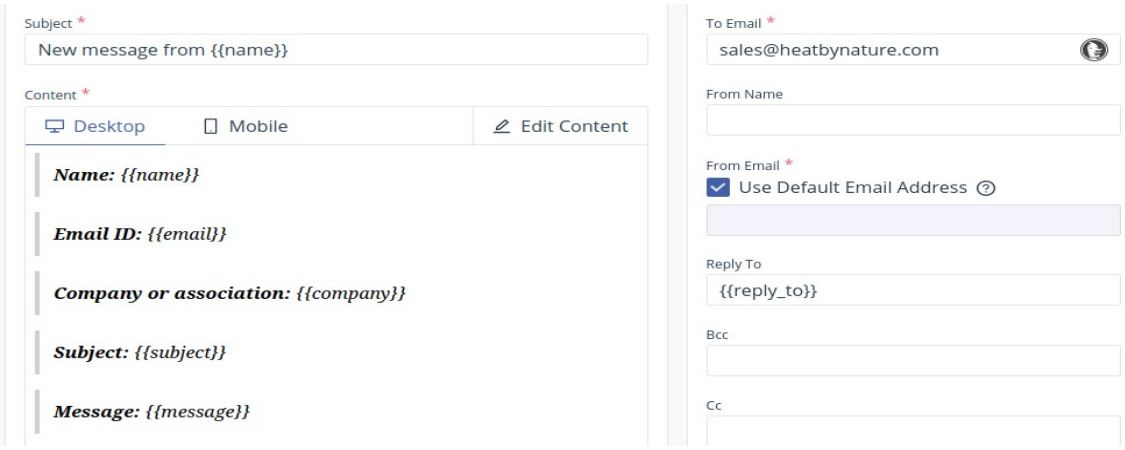
Yhteydenotto-sivu seuraa myös kotisivun asettamaa teemaa ja ylävalikkoa. Sivun yhteydenottolomake sisältää kohdat ”Name”, ”Email”, ”Company or Association”, ”Subject” ja ”Write your message”. Asiakas täyttää kaikki kohdat ja painaa ”Send Email”-painiketta ja sähköposti lähtee automaattisesti yrityksen myyntitilille. Kohdat muuttuvat oranssiksi täytettyinä ja painikkeeseen tulee oranssi korostus aktiivisena (kuvio 7).



Kuvio 7. Esimerkki täytetystä lomakkeesta

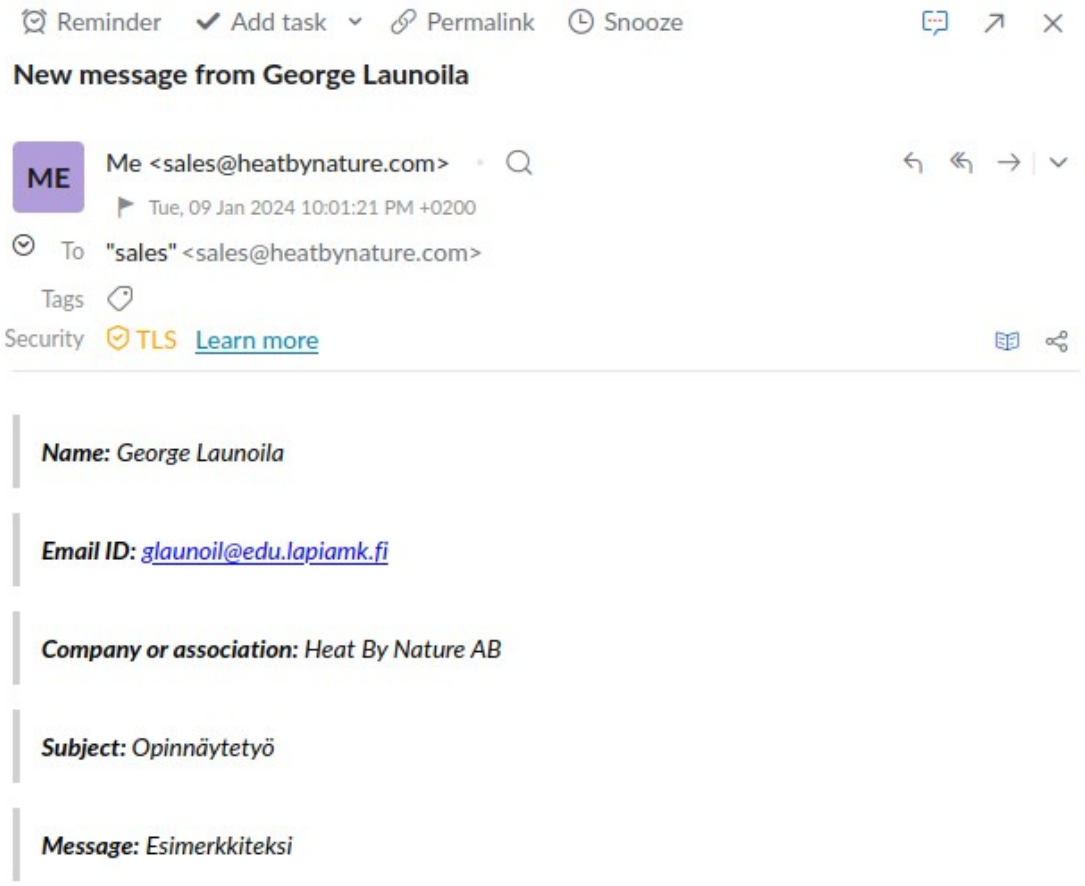
Sähköpostin lähettämiseen käytössä on Email.js API. Email.js on työkalu, jolla voi lähettää sähköposteja helposti. Käyttöön ei vaadita palvelinta, vaan pitää vain valita sähköpostipalvelu, malli ja kirjasto. (Email.js Docs 2023.)

Email.js:n käyttöliittymän avulla asetetaan sähköpostin muotoilu ja käytettävät muuttujat. Kuviossa näkyvät muuttujat tulevat yhteydenottolomakkeesta (kuvio 8.)



Kuvio 8. Näkymä Email.js:n käyttöliittymässä

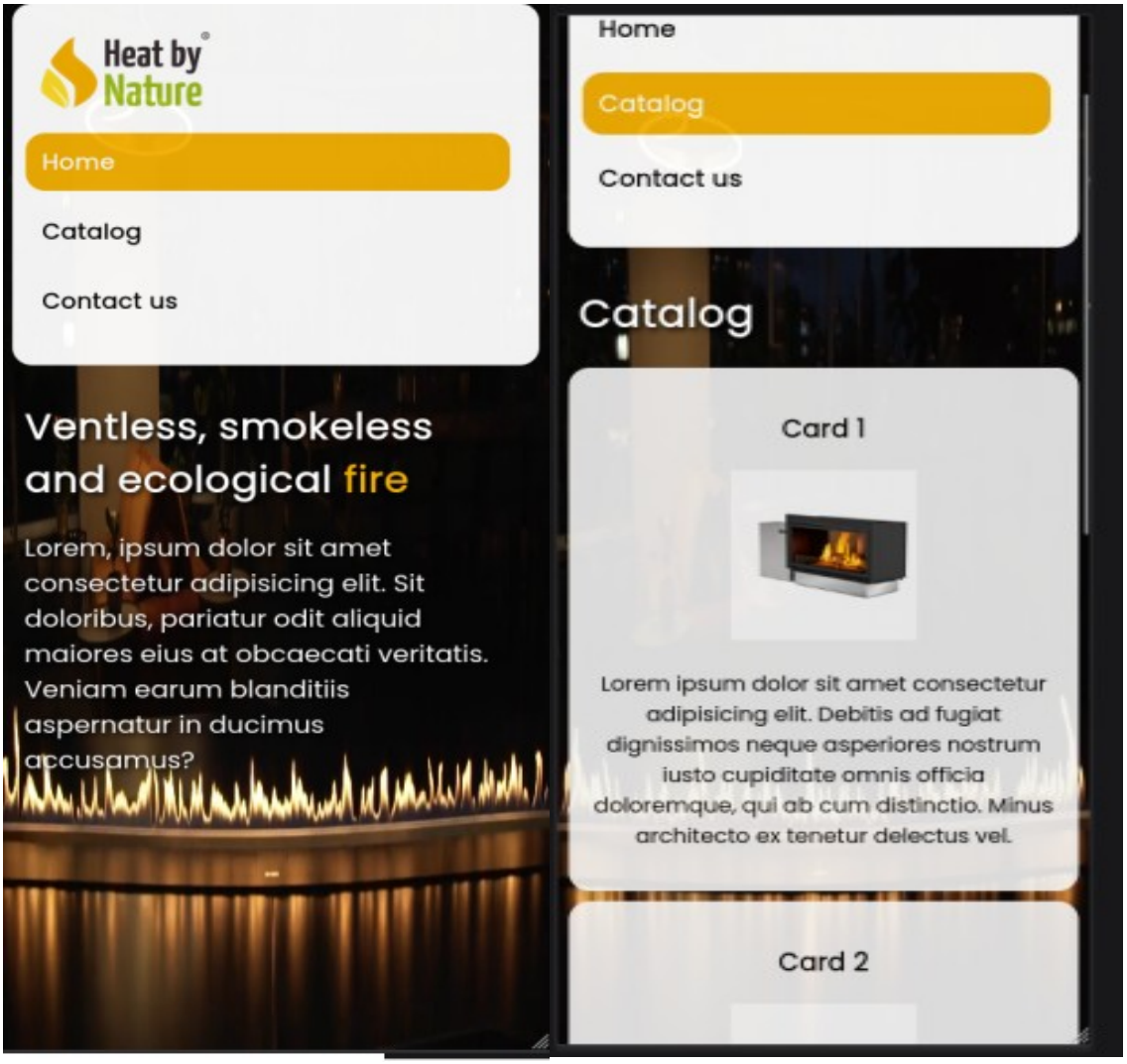
Onnistuneen viestin lähettämisen jälkeen selain antaa ilmoituksen ”200 OK” ja viesti lähtee onnistuneesti yrityksen sähköpostiin. Sähköpostiviestin lähettämiseen ja vastaanottamiseen käytetään yhtä ja samaa sähköpostiosoitetta. (kuvio 9.)



Kuvio 9. Sähköpostin vastaanotto

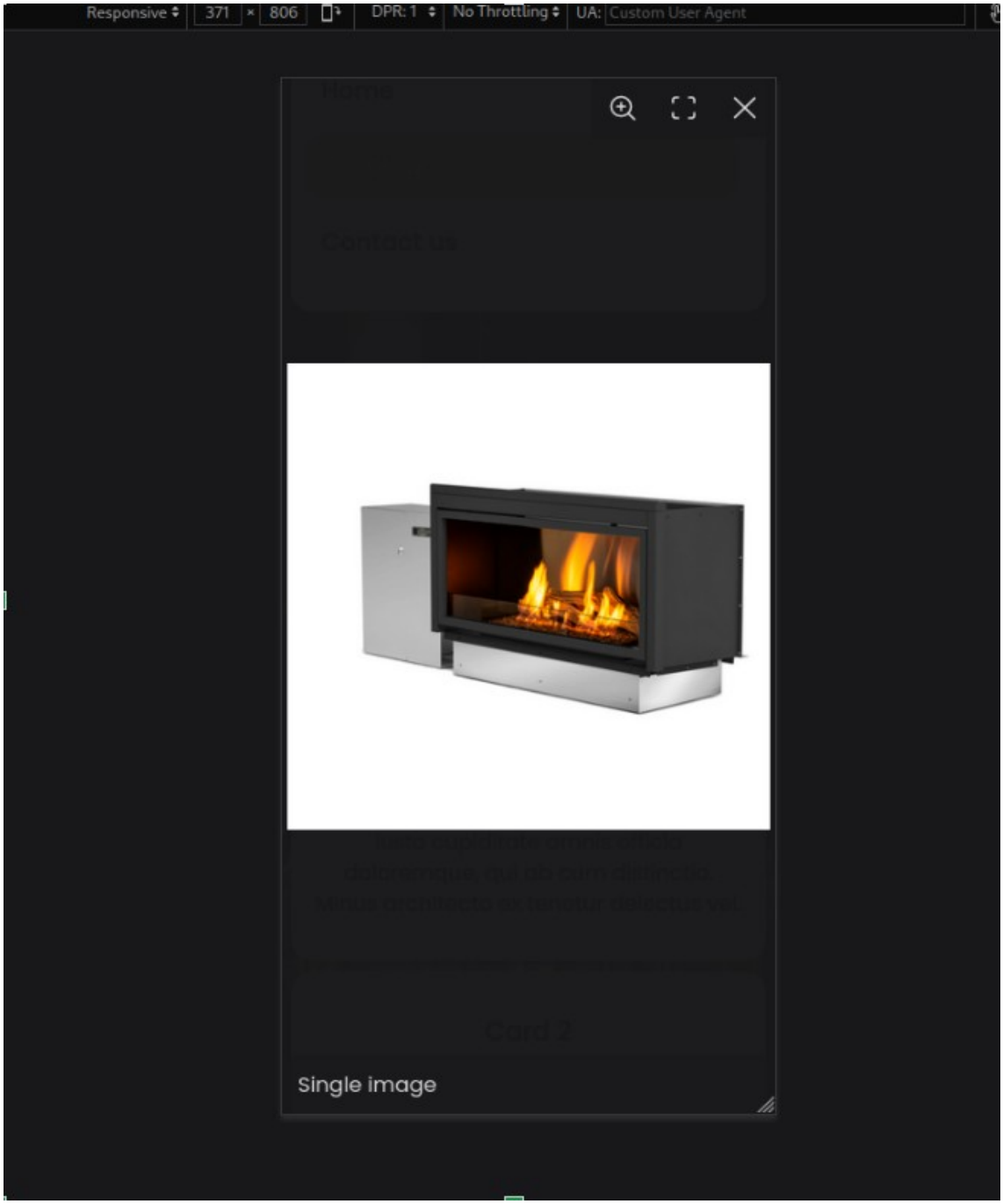
4.4 Verkkosivuston responsiivisuus

Määrittelemäni responsiivisuudella on kolme tilaa. Oletustila on suunniteltu näytöille, joiden leveys on yli tuhat pikseliä. Tablettitila on tarkoitettu näytöille, joiden leveys on alle tuhat pikseliä, mutta yli 700 pikseliä. Puhelintila on tarkoitettu näytöille, joiden leveys on alle 700 pikseliä. Tämä mahdollistaa elementtien helpon sopeutumisen tarvittaessa. Tapauksessa, kun px määrä alittaa määritetyn 700, sivuston elementit kutistuvat ja menevät allekkain (kuvio 10).



Kuvio 10. iPhone 11 Pron näkymä kotisivusta ja katalogista

Fancyboxilla tehty kuvan suurennus myös sopeutuu automaattisesti näytön koon mukaan. Se helpottaa käyttökokemuksen optimointia eri laitteilla, kuten puhelimilla ja tableteilla (kuvio 11).



Kuvio 11. iPhone 11 Pron näkymä kuvan suurennuksesta

5 LINUX JA PALVELIN

5.1 GNU/Linux historia

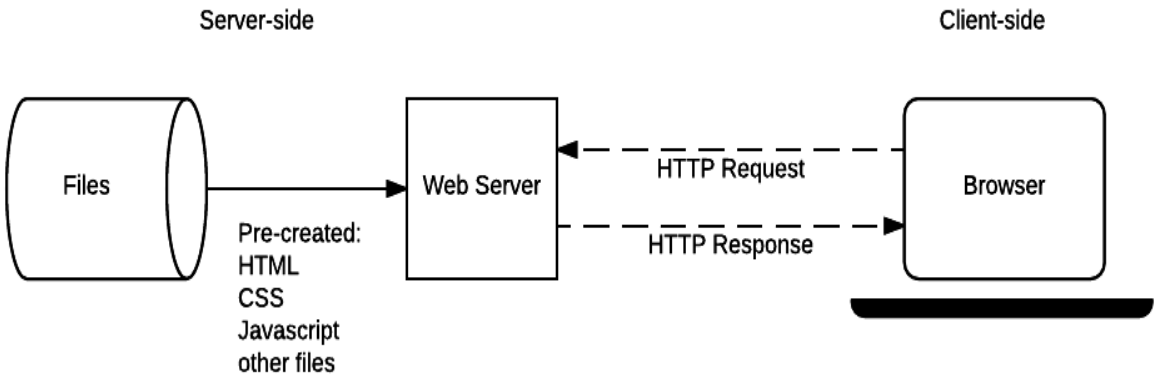
Richard Stallman kirjoitti GNU-manifestin vuonna 1985 pyytääkseen tukea GNU-käyttöjärjestelmän kehittämiseen. GNU eli GNU’s Not Unix! -käyttöjärjestelmä on kehitetty, jotta käyttäjillä olisi vapaus tietokoneen käytössä. Tarkemmin sanottuna vapaa ohjelmisto tarkoittaa, että käyttäjillä on neljä olennaista vapautta: (0) ohjelman käyttöoikeus, (1) ohjelman tutkimis- ja muokkausoikeus lähdekoodimuodossa, (2) tarkan kopion jakamisoikeus ja (3) muokattujen versioiden jakamisoikeus. (Stallman 2023.)

Käyttöjärjestelmä sisältää ytimen, kääntäjiä, tekstieditoreita, tekstimuotoilijoita, sähköpostiohjelmistoja, graafisia käyttöliittymiä, kirjastoja, pelejä ja monia muita asioita. Näin ollen koko käyttöjärjestelmän kirjoittaminen on erittäin suuri tehtävä. Vuoteen 1990 mennessä GNU oli lähes valmis, mutta siitä puuttui yksi osa — ydin. (Stallman 2023.)

Vuonna 1991 Helsingin yliopistossa opiskeleva Linus Torvalds alkoi kehittämään Linux-ydintä, koska hän ei ollut tyytyväinen Microsoft MS-DOS -käyttöjärjestelmään. Hän oli tottunut UNIX-käyttöjärjestelmään, jota Helsingin Yliopiston tietokoneet tuohon aikaan käyttivät. Linux versio 1.0 julkaistiin vuonna 1994 ja ytimen yhdistäminen GNU:n ohjelmistoihin johti täyteen käyttöjärjestelmään. (Gregersen 2023.)

5.2 Palvelimen toimintaperiaate

Yksinkertaisesti palvelin on tietokone, joka varastoi verkkosivun tiedostot ja muun datan. Internetin avulla muut käyttäjät yhdistyvät palvelimeen saadakseen tiedostot. Aina kun selain tarvitsee tiedoston, joka on tallennettu verkkopalvelimelle, selain pyytää tiedostoa HTTP:n avulla. Kun pyyntö saapuu (laitteisto) palvelimelle, (ohjelmisto) HTTP-palvelin hyväksyy pyynnön, etsii pyydetyt tiedostot ja lähettää ne takaisin selaimelle myös HTTP:n kautta (kuvio 12). (MDN Web Docs 2023.)



Kuvio 12. Serverin toiminta. (MDN Web Docs 2023.)

Staattinen verkkopalvelin koostuu tietokoneesta (laitteisto) ja HTTP-palvelimesta (ohjelmisto). Sitä kutsutaan staattiseksi, koska palvelin lähettää isännöimänsä tiedostot sellaisinaan selaimelle. Dynaaminen verkkopalvelin koostuu staattisesta verkkopalvelimesta sekä tietokannasta. Sitä kutsutaan dynaamiseksi, koska sovelluspalvelin päivittää isännöidyt tiedostot ennen kuin ne lähetetään selaimelle HTTP-palvelimen kautta. (MDN Web Docs 2023.)

5.3 Linux palvelimena

Palvelimen tärkein työ on olla päällä lähes koko ajan. Tämän vuoksi GNU/Linux on täydellinen käyttöjärjestelmä tähän tarkoitukseen, sillä se on äärimmäisen vakaa, luotettava ja turvallinen.

Linux tarjoaa ihanteellisen alustan modernille, innovatiiviselle tietotekniikalle, minkä vuoksi se on laajasti käytössä eri toimialoilla ja uusissa teknologiaan liittyvissä käyttötapauksissa. Se on vakiintunut standardi korkean käytettävyyden, luotettavuuden ja kriittisten työkuormien kehittämisessä ja suorittamisessa datakeskuksissa ja pilvipalveluympäristöissä. Linux tukee monenlaisia käyttötapauksia, kohdejärjestelmiä ja laitteita. (Red Hat 2023.)

5.4 Hieman tietoturvasta

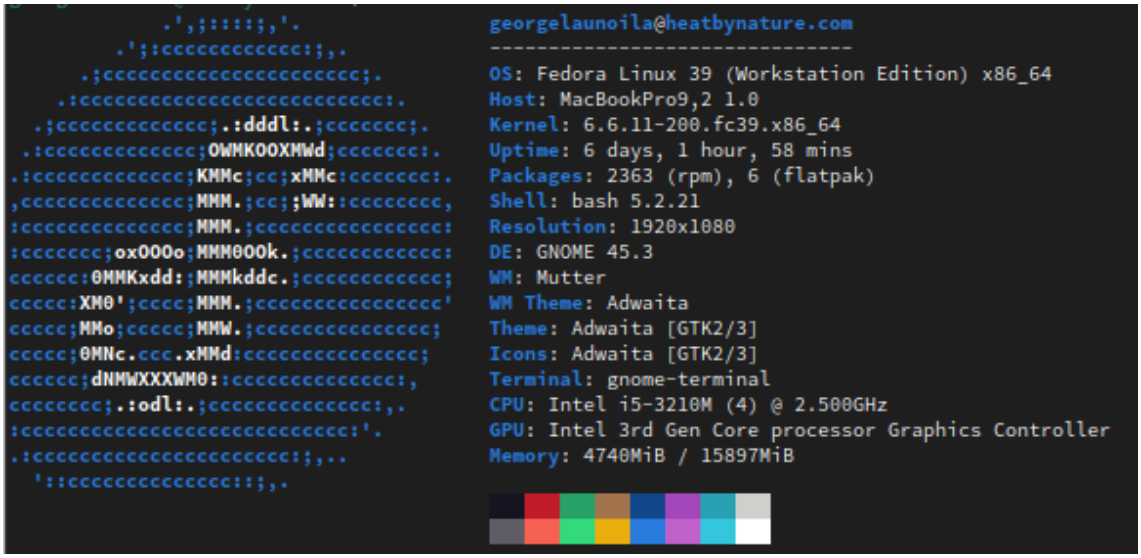
Tietoturva on tietokonejärjestelmien ja tietojen suojaamista vahingoittumiselta, varkaudelta ja luvattomalta käytöltä. Staattiset verkkosivustot saattavat vaikuttaa vähemmän haavoittuvilta verrattuna dynaamisiin verkkosivustoihin, joissa on tietokantoja, mutta ovat silti alttiita tietyille hyökkäyksille.

Yleisimpiä hyökkäyksiä ovat SQL-injektiot ja Cross-Site Scripting (XSS), jotka kohdistuvat tietokantoihin ja lisäävät haitallisia skriptejä verkkosivuille. Cross-Site Request Forgery (CSRF) houkuttelee käyttäjiä suorittamaan tahattomia toimia, kun taas palveluestohyökkäys eli DDoS ylikuormittaa palvelimet liikenteellä ja tekee sivustoista saavuttamattomia. Brute force -hyökkäykset yrittävät jatkuvasti murtaa salasanoja, kun taas Man in the Middle kaappaa viestinnän pahantahtoisiin tarkoituksiin.

Tietokannan tai kirjautumisjärjestelmän puuttuminen vähentää joitain riskitekijöitä, staattiset verkkosivustot ovat edelleen alttiita palvelunestohyökkäyksille. Lisäksi luvaton etäkäyttö voi tapahtua esimerkiksi hyödyntämällä heikkoutta palvelimen tai verkkoyhteyden suojausasetuksissa, mikä mahdollistaa ulkopuolisten pääsyn verkkosivustolle ja sen sisältöön.

6 PALVELIMEN JA TIETOTURVAN IMPLEMENTAATIO

Alun perin suunnittelin käyttäväni Arch Linux -jakelua palvelimellani. Kuitenkin työtietokoneeni emolevyn rikkoutumisen seurauksena päätin valita Fedora-jakelun palvelimelleni, sillä käytin palvelintietokonetta myös verkkosivun rakentamisessa ja tämän opinnäytetyön kirjoittamisessa (kuvio 13).

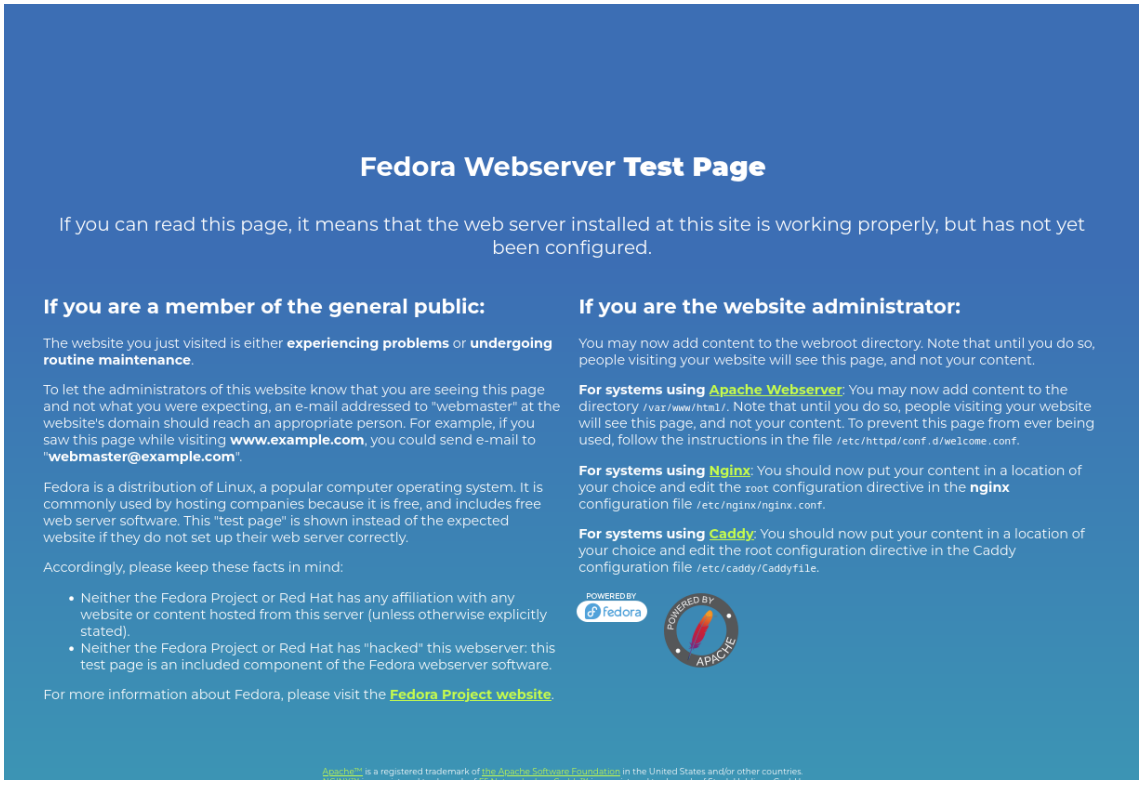


Kuvio 13. Palvelimen tekniset tiedot

6.1 Palvelimen käyttöönotto

Ensimmäinen askel on asentaa ja aktivoida Apache HTTPD. Apache HTTP Server -projekti on pyrkimys kehittää ja ylläpitää avoimen lähdekoodin HTTP-palvelinta nykyaikaisille käyttöjärjestelmille, mukaan lukien UNIX ja Windows. Apache HTTPD:n tavoitteena on tarjota turvallinen, tehokas ja laajennettava palvelin, joka tarjoaa HTTP-palveluja noudattaen voimassa olevia HTTP-standardeja. (The Apache Software Foundation 2023.)

Varmistakseen, että Apache HTTPD varmasti toimii, syötetään selaimeen ”localhost”-osoite. Aktivointi on onnistunut, jos Apachen testisivusto tulee näkyviin (kuvio 14).



Kuvio 14. Selaimen tuloste.

Aktivoinnin jälkeen on määritettävä sivuston verkkotunnus, verkkosivun sijainti ja mitä porttia sen tulisi kuunnella. Tässä tapauksessa sen on kuunneltava porttia 443, sillä HTTPS-yhteydet kulkee sen kautta. Luodaan ja määritellään verkkosivun konfigurointitiedosto Apache HTTPD -palvelimen kansioon (kuvio 15).

```
 GNU nano 7.2                          /etc/httpd/sites-available/heatbynature.com.conf
<VirtualHost *:443>
    ServerAdmin admin@heatbynature.com
    ServerName heatbynature.com
    ServerAlias www.heatbynature.com
    DocumentRoot /var/www/html/heatbynature.com
```

Kuvio 15. Valmis konfigurointitiedosto

Seuraavaksi on määritettävä 443-portin välityksen reitittimen asetuksissa. Tämä tehdään sen takia, että se mahdollistaa internetistä tulevien liikenne- ja yhteyspyyntöjen ohjautumisen Apache HTTPD -palvelimelle (kuvio 16).

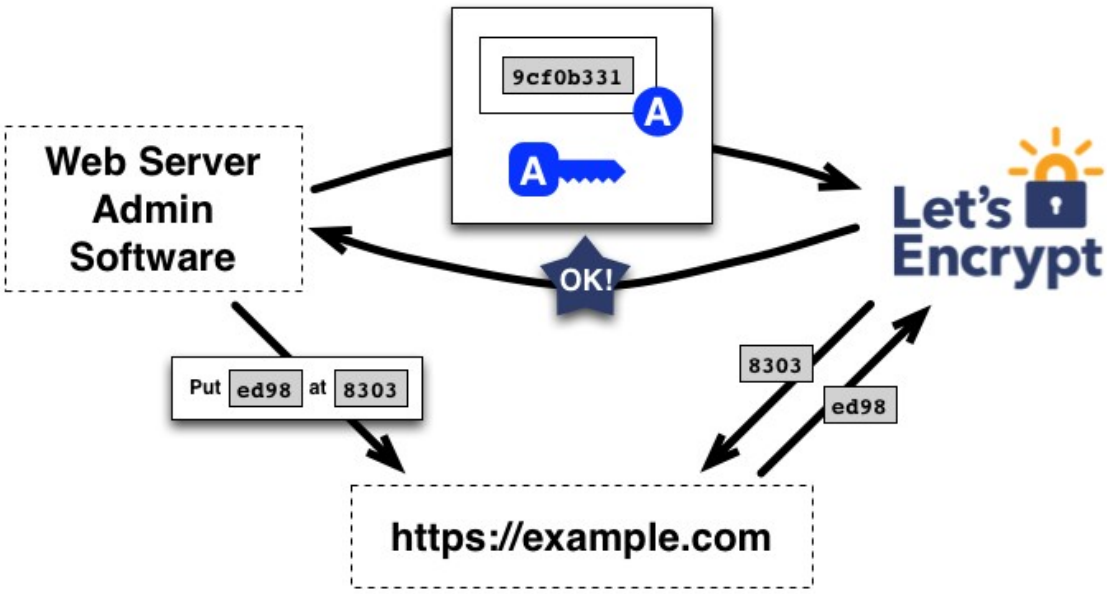
#	Service Name	External Start Port	Internal Start Port	Internal IP address
1	verkkosivusto	443	443	192.168.1.17

Kuvio 16. Reitittimen asetukset

6.2 SSL-protokolla ja HTTPS

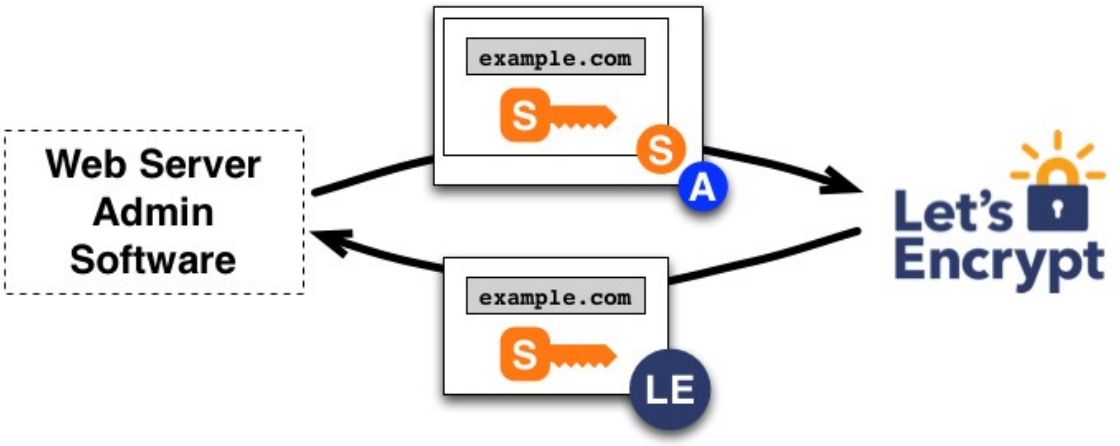
Ottaakseen käyttöön SSL-protokollan tuen, allekirjoitin sertifikaatin itse käyttämällä ”mod_ssl”-konsoliohjelmaa. Sertifikaatin allekirjoituksen jälkeen huomasin, että selain ei hyväksynyt sertifikaattia ja merkitsi sivuston ”tietoturvariskiksi”. Tämä johtui siitä, että nykyään selaimet eivät hyväksy itse allekirjoitettuja sertifikaatteja. Ratkaisu oli käyttää sertifikaattiviranomaisen (CA) myöntämää sertifikaattia. Squarespace-palvelu myöntää verkkotunnuksille sertifikaatteja Let's Encrypt -sertifikaattiviranomaisen kautta.

Let's Encrypt tunnistaa palvelimen ylläpitäjän julkisen avaimen avulla. Kun agenttisohjelmisto vuorovaikuttaa ensimmäisen kerran Let's Encryptin kanssa, se luo uuden avainparin ja osoittaa Let's Encryptille, että palvelin hallitsee yhtä tai useampaa verkkotunnusta. Tämä vastaa perinteisen CA-prosessin vaihetta, jossa luodaan käyttäjätili ja lisätään siihen verkkotunnuksia (kuvio 17). (Let’s Encrypt 2019.)



Kuvio 17. Avainparin luominen. (Let’s Encrypt 2019.)

Kun agentilla on valtuutettu avainpari, sertifikaattien pyytäminen, uusiminen ja mitätöiminen on yksinkertaista. Täytyy vain lähettää sertifikaatinhallintaviestit ja allekirjoittaa ne valtuutetulla avainparilla (kuvio 18).



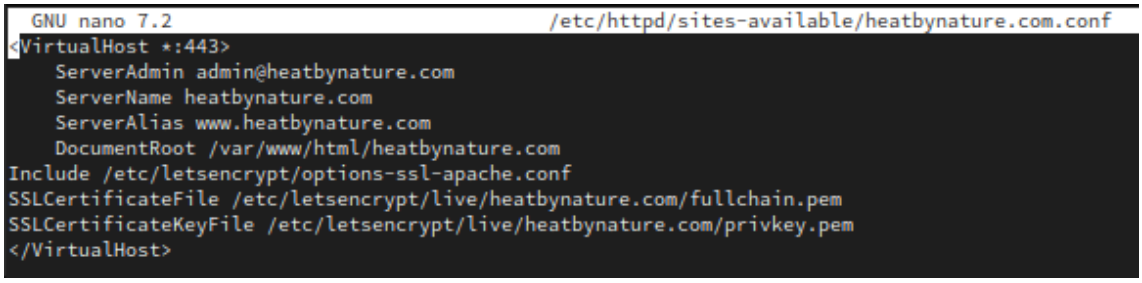
Kuvio 18. Sertifikaatin pyytäminen. (Let's Encrypt 2019.)

Sertifikaatin pyytäminen onnistuu Certbot-työkalun avulla. Certbot yksinkertaistaa ja automatisoi prosessin (kuvio 19).

```
georgelaunoila@heatbynature:~$ apachectl configtest
Syntax OK
georgelaunoila@heatbynature:~$ sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Which names would you like to activate HTTPS for?
We recommend selecting either all domains, or all domains in a VirtualHost/server block.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: heatbynature.com
2: www.heatbynature.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
Certificate not yet due for renewal

You have an existing certificate that has exactly the same domains or certificate name you requested and isn't close to ex
(ref: /etc/letsencrypt/renewal/heatbynature.com.conf)

What would you like to do?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Attempt to reinstall this existing certificate
2: Renew & replace the certificate (may be subject to CA rate limits)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Deploying certificate
Successfully deployed certificate for heatbynature.com to /etc/httpd/sites-enabled/heatbynature.com.conf
Successfully deployed certificate for www.heatbynature.com to /etc/httpd/sites-enabled/heatbynature.com.conf
Congratulations! You have successfully enabled HTTPS on https://heatbynature.com and https://www.heatbynature.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

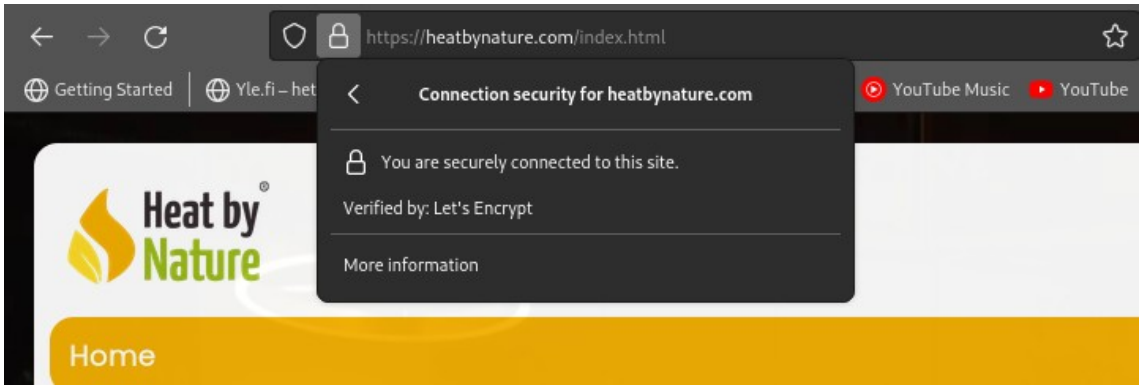
Kuvio 19. Certbotin tuloste konsolissa.

Certbot lukee sivuston konfigurointitiedoston ja sen perusteella hakee sertifikaatteja tunnukselle. Onnistuessaan ohjelma lisää avaimen ja sertifikaatin sijainnit konfigurointitiedostoon (Kuvio 20).



Kuvio 20. Verkkosivun konfigurointitiedosto

Kytketään Apache HTTPD -palvelin päälle ja varmistetaan, että sivusto toimii. Kuviossa näkyy, että selain on hyväksynyt sertifikaatin (kuvio 21).



Kuvio 21. Näkymä Firefox-selaimella

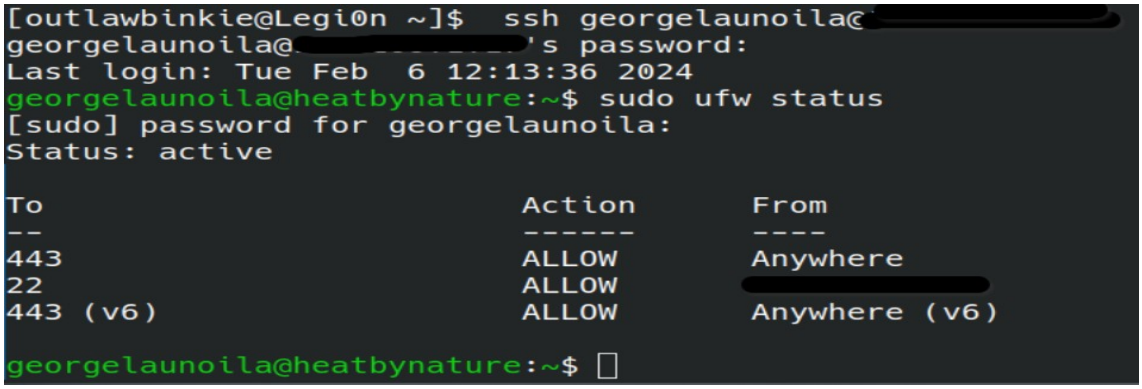
6.3 Palvelimen tietoturvallisuus ja palomuuri

Palomuuri seuraa tulevaa ja lähtevää verkkoliikennettä ja päättää sallitaanko vai estetäänkö tietty liikenne määritellyn joukon turvallisuussääntöjen perusteella. Useiden jakeluiden Linux-ytimet sisältävät pakettisuodatusjärjestelmän nimeltä Netfilter, ja perinteinen työkalu Netfilterin hallintaan on iptables-komentokokoelma. Iptables tarjoaa laajan palomuuriratkaisun, joka on helposti mukautettavissa. Iptablesin hallitseminen vaatii aikaa ja pelkästään iptablesin käyttö Netfilter-palomuurina voi olla haastava tehtävä aloittelijalle. Tämän seurauksena vuosien varrella on luotu monia käyttöliittymiä iptablesille, mistä jokainen pyrkii saavutta-

maan erilaisia tuloksia ja kohdistumaan erilaisiin käyttäjäryhmiin. (Ubuntu Server Docs 2023.)

Yksi näistä käyttöliittymistä on UFW. Uncomplicated Firewall (UFW) on käyttöliittymä Netfilterille ja soveltuu erityisen hyvin isäntäpohjaisille palomuureille. UFW tarjoaa kehyksen Netfilterin hallintaan sekä komentorivikäyttöliittymän palomuurin manipulointiin. (LibreTexts Engineering 2024.)

Aktivoidaan UFW ja avataan portit 443 eli HTTPS ja 22 eli SSH. Konfiguroidaan että, porttiin 22 voi muodostaa yhteyden vain minun tietokoneeni yksityisellä IP-osoitteella (kuvio 22).



Kuvio 22. UFW tilanne tuloste käyttäen SSH:ta.

Portti 443:n kautta HTTPS salaa tiedot tekemällä ne lukukelvottomiksi kenelle tahansa, joka saattaisi ne onnistua väärinkäyttämään. Tämä salaus on ratkaisevan tärkeää suojaamaan kyberuhkilta.

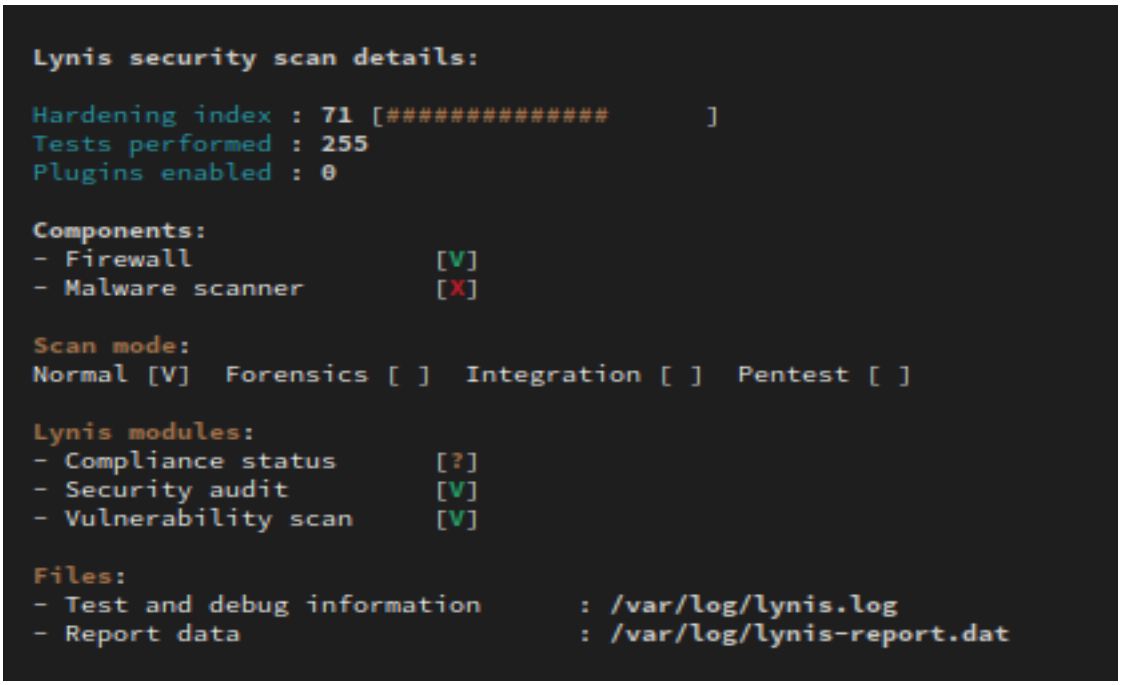
SSH (Secure Shell) on verkkoprotokolla, joka tarjoaa turvallisen pääsyn etäjärjestelmään suojaamattoman verkon yli. Se salaa kaiken datan, joka lähetetään asiakkaan ja palvelimen välillä, estäen kuuntelua, muokkausta ja muita tietoturvaan liittyviä uhkia. SSH on yleisesti käytössä etähallintaan, tiedostonsiirtoihin ja tunnelointiin. Käyttäen SSH-protokollaa pääsen muodostamaan yhteyttä palvelimeen omalla tietokoneellani etäkäyttöä varten. (OpenSSH 2023.)

DNSSEC (Domain Name System Security Extensions) on joukko laajennuksia, jotka lisäävät turvamekanismeja DNS-vastauksiin. Sen tavoitteena on todentaa DNS-tietojen alkuperä ja varmistaa niiden eheys, kun niitä välitetään DNS-palvelimilta asiakkaille. Tämä auttaa estämään erilaisia DNS-pohjaisia hyökkäyk-

siä, kuten DNS-väärentämistä, välimuistin myrkyttämistä ja välimieshyökkäyksiä. DNSSEC:in käyttö onnistuu helposti verkkotunnusvälittäjän kautta. (DNSSEC 2018.)

6.4 Tietoturvan varmistaminen ja ylläpito

Tietoturvan varmistamiseksi hyödynnän Lynis-konsoliohjelmaa. Lynis suorittaa sarjan automatisoituja testejä, jotka tarkistavat palvelimen asetuksia ja komponentteja. Työkalu lopuksi esittää kovettumisindeksin ja listan mahdollisista ehdotuksista ja varoituksista (kuvio 23).



Kuvio 23. Lopputulos testistä

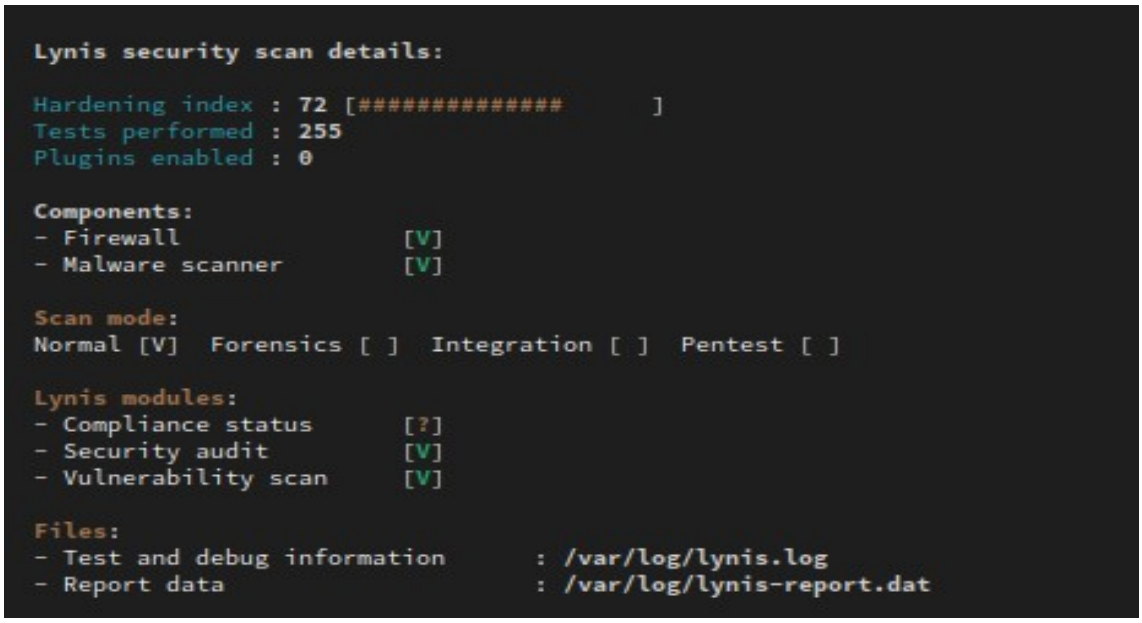
Kovettumistestin tulokset olivat hyvät, ja varoituksia ei ilmennyt. Sen sijaan Lynis antoi hälytyksen, joka osoittaa, että palvelimella ei ole haittaohjelmaskanneria.

Yksi suosituimmista ja väitetysti paras haittaohjelmaskanneri on ”chkrootkit”. Työkalu etsii merkkejä siitä, että järjestelmä olisi saanut 'rootkit'-infektion tai muun haittaohjelman.

Rootkit on joukko ohjelmistotyökaluja, joita hyökkääjä käyttää peittääkseen jälkensä. Rootkitit voivat myös sisältää ohjelmistoja, jotka antavat hyökkääjälle pääsyn järjestelmän root-tasolle ja mahdollistavat tiedostojen varastamisen tai

poistamisen. Tämä tapahtuu hyödyntämällä haavoittuvaa ohjelmaa, jotta saataisiin root-käyttöoikeudet tavallisena käyttäjänä, mikä tunnetaan nimellä ”privilege escalation”. Tämä tapahtuu huijaamalla haavoittuvaa sovellusta tai sen käyttäjää tekemään jotain, mitä ei pitäisi tehdä, mikä lopulta johtaa root-käyttöoikeuksiin. (Day 2021.)

Chkrootkitin testi osoitti, että järjestelmä on täysin kunnossa. Lynis lisäsi yhden pisteen kovettumisideksiin chkrootkitin ansiosta (kuvio 24).



Kuvio 24. Päivitetty tulos

Apache Server login kautta voidaan seurata verkkosivun liikennettä. Kuviosta on peitetty kolumni, joka sisältää IP-osoitteita (kuvio 27).

Kuvio 27. Access login sisältö

7 POHDINTA

Tässä opinnäytetyössä sain mahdollisuuden tutustua siihen, miten rakentaa ja ylläpitää tietoturvallista palvelinta, suunnitella ja toteuttaa verkkosivusto asiakkaan tarpeisiin, sekä toimia yrityksessä ylläpitäjänä.

Verkkosivun rakentaminen oli melko haastavaa. Ulkoasun ja responsiivisuuden suunnittelu vaati paljon tutkimustyötä, koska ennen tätä olen tehnyt vain muutamia sivuja. Tämän myötä arvostan Front-end-kehittäjiä entistä enemmän.

SSL-protokollaan tutustuminen ja sen käyttöönotto olivat todella mielenkiintoisia ja tärkeitä vaiheita projektissa. Tietoturvan kannalta SSL on olennainen osa verkkopalveluiden turvallisuutta, ja sen käyttöönotto varmistaa, että tieto siirtyy salattuna palvelimen ja käyttäjän välillä. Palvelimen rakentaminen oli jälleen erittäin kiinnostavaa, ja aiemmat kokemukseni Linux-ympäristöstä olivat suureksi avuksi. Palomuuri on keskeinen osa tietoturvaa ja sen käyttöönotto sekä alustava varmistaminen sujuivat ongelmitta.

On tärkeää huomioida, että tietoturva vaatii jatkuvaa päivittämistä ja ylläpitoa. Vaikka alustava tietoturvan varmistaminen sujui hyvin, on tärkeää seurata tietoturvatilannetta ja tehdä tarvittavia päivityksiä ja parannuksia säännöllisesti. Tietoturvan ylläpitäminen on jatkuva prosessi, joka vaatii huolellisuutta ja tarkkaavaisuutta.

Opinnäytetyön aloitusvaiheessa kohtasin haasteen, kun työtietokoneeni emolevy hajosi. Päätin ratkaista tilanteen asentamalla Fedora-jakelun Arch Linuxin sijaan käyttämälleni palvelintietokoneelle ja suorittamalla koko projektin samalla laitteella. Tämän päätöksen ansiosta onnistuin pitämään kiinni aikataulustani, vaikka aluksi tilanne näytti hankalalta. Jälkikäteen voin rohkeasti sanoa, että tämä tilanne teki projektistani jopa mielenkiintoisemman. Ohjelmointi ja kirjoittaminen 12 vuotta vanhalla MacBookilla osoittautuivat todelliseksi "kokemukseksi". Kaiken kaikkiaan tämä opinnäytetyö tarjosi minulle mahdollisuuden kehittyä monipuolisesti eri tehtävissä. Pääsin rakentamaan verkkosivuja asiakkaan asettamien vaatimusten mukaisesti, syventymään GNU/Linux-ympäristöön ja oppimaan enemmän tietoturvasta.

LÄHTEET

Day, B 2021. What You Need to Know About Linux Rootkits. LinuxSecurity. Viitattu 26.1.2024 https://linuxsecurity.com/features/what-you-need-to-know-about-linux-rootkit

DNSSEC 2018. What is DNSSEC? Viitattu 6.2.2024 https://www.dnssec.net/

Email.js 2024. How does Emaij.js work? Viitattu 20.1.2024 https://www.emailjs.com/docs/introduction/how-does-emailjs-work/

Google for Developers 2023. Mobile site and mobile-first indexing bestpractices. Viitattu 5.1.2024 https://developers.google.com/search/docs/crawling-indexing/mobile/mobile-sites-mobile-first-indexing

Gregersen, E. 2023. Linus Torvalds. Britannica. Viitattu 31.1.2024 https://www.britannica.com/biography/Linus-Torvalds

Let’s Encypt 2019. How It Works. Viitattu 26.1.2024 https://letsencrypt.org/how-it-works/

LibreTexts Engineering 2024. UFW & firewalld. Viitattu 25.1.2024 https://eng.libretexts.org/Bookshelves/Computer_Science/Operating_Systems/Linux_-_The_Penguin_Marches_On_(McClanahan)/12%3A_Linux_Systems_Security/4.14%3A_UFW_and_firewalld

MDN Web Docs 2023. What is a web server? Viitattu 1.2.2024 https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_web_server

OpenBSD Foundation 2023. OpenSSH. Viitattu 6.2.2024 https://www.openssh.com/

Red Hat 2023. Expand innovation and operational efficiency with Linux. Viitattu 1.2.2024 https://www.redhat.com/rhdc/managed-files/li-expand-innovation-and-efficiency-with-linux-ebook-f31401-202207-en_0.pdf

SSL Support Team 2021. What is HTTPS? SSL. Viitattu 22.1.24 https://www.ssl.com/faqs/what-is-https/

Stallman, R. 2023. The GNU Project. GNU Operating System. Viitattu 24.1.2024 https://www.gnu.org/gnu/thegnuproject.html

The Apache Software Foundation 2023. What is the Apache HTTP Server Project? Viitattu 10.1.2024 https://httpd.apache.org/ABOUT_APACHE.html

Ubuntu Server Docs 2023. Security – Firewall. Viitattu 5.2.2024 https://ubuntu.com/server/docs/security-firewall

World Wide Web Consortium 2021. WCAG 101: Understanding the Web Content Accessibility Guidelines. Viitattu 5.1.2024 https://wcag.com/resource/what-is-wcag/