jamk

Kustomoidun Linux-käyttöjärjestelmän koventaminen

Juho Vähämaa

Opinnäytetyö, AMK
Huhtikuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Vähämaa, Juho

Kustomoidun Linux käyttöjärjestelmän koventaminen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Huhtikuu 2024, 68 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: Kyllä

Tiivistelmä

Opinnäytetyö keskittyy Debian 11 Linux-käyttöjärjestelmän järjestelmäkovennusten suunnitteluun ja toteutukseen. Kovennusprosessissa hyödynnetään Center for Internet Securityn (CIS) viitekehyksiä, jotka ovat maailmanlaajuisesti tunnustettuja. Opinnäytetyön tavoitteena on nostaa järjestelmän turvallisuutta pienentämällä sen haavoittuvuuspinta-alaa.

Järjestelmäkovennukset toteutettiin peilaamalla viitekehysten kovennuksia käyttöönotettavaan järjestelmään ja automatisoimalla kovennukset bash-skriptin avulla. Skriptin toimintatapa on tarkastaa järjestelmän tila kovennus kerrallaan ja toteuttaa mahdolliset muutokset vastaamaan käyttöönotettujen CIS viitekehysten suosituksia.

Opinnäytetyön tuloksena syntyi Debian 11 käyttöjärjestelmälle soveltuva bash-skripti, joka automaattisesti ajettaessa koventaa järjestelmän niihin CIS suosituksiin, jotka koettiin toimeksiantajan järjestelmään tarpeellisiksi. Opinnäytetyön saavutuksena syntyi myös suomennettu versio Debian 11:n viitekehyksistä, joka ei alun perin kuulunut työsuunnitelmaan.

Opinnäytetyö korostaa järjestelmäkovennusten ylläpidon tärkeyttä päivitysten yhteydessä. Tällä varmistetaan, että järjestelmän tietoturva säilyy korkeana pitkällä aikavälillä. Opinnäytetyö tarjoaa arvokasta tietoa ja menetelmiä tietoturva-asiantuntijoille sekä IT-ammattilaisille Linux-pohjaisten järjestelmien kanssa työskentelyyn.

Kaikki kehitetyt kovennukset on julkaistu julkiseen käyttöön, mikä mahdollistaa niiden laajan hyödyntämisen ja soveltamisen eri ympäristöissä. Tämän avoin lähestymistapa edistää yhteisön yhteistyötä ja tietoturvan jatkuvaa parantamista.

Avainsanat (asiasanat)

Linux, käyttöjärjestelmä, kovennus, tietoturva, viitekehykset, auditointi, hyökkäyspinta-ala, automaatio

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Vähämaa, Juho

Hardening a custom Linux OS

Jyväskylä: JAMK University of Applied Sciences, April 2024, 68 pages.

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: finnish

Abstract

The thesis is about setting up and applying security enhancements for the Debian 11 Linux operating system. It uses guidelines from the Center for Internet Security (CIS), which are well-known worldwide. The goal is to make the system safer by reducing the chances for security breaches.

The security enhancements were put in place by following the CIS guidelines and making them work automatically with a bash script. This script checks the system's security, one step at a time, and makes needed changes to meet the CIS standards.

The outcome of the thesis was a bash script that automatically strengthens the Debian 11 system according to the CIS recommendations that were important for the client's system. There was also a Finnish version of the Debian 11 guidelines created, which wasn't planned initially.

The thesis underlines the importance of keeping the security enhancements up-to-date, especially when the system gets updated. This helps to keep the system secure over time. The thesis offers useful information and techniques for people who work with Linux-based systems in cybersecurity and IT.

All the security enhancements that were developed have been made available for everyone, which lets them be widely used and adapted in different settings. This open way of doing things helps the community work together and keeps improving security.

Keywords/tags (subjects)

Linux, operating system, hardening, cybersecurity, benchmarks, auditing, attack surface, automation

Miscellaneous (Confidential information)

Sisältö

Kuviot

1 Johdanto

Tietoturva nousi keskeiseen rooliin nykyaikaisen digitaalisen maailman rakenteissa. Nyky-yhteiskunta on osoittautunut yhä enenevässä määrin riippuvaiseksi teknologiasta, mikä teki tietoturvasta olennaisen osan päivittäistä elämäämme. Tietoturvahyökkäykset ja -rikollisuus eivät ole ainoastaan lisääntyneet määrällisesti, vaan myös monimutkaistuneet ja moninaistuneet. Tämän vuoksi vastatoimenpiteiden on oltava entistä kattavampia ja edistyneempiä. Yksi näistä vastatoimenpiteistä on käyttöjärjestelmien kovennus, millä tarkoitetaan prosessia, jossa kyberturvallisuuden asiantuntijat tekevät jatkuvia ponnistuksia tunnistaakseen, ennakoidakseen ja korjatakseen turvallisuusaukkoja koko IT-infrastruktuurissaan (What is System Hardening, n.d). Hyökkäyspinnan minimointi ei ainoastaan vähentänyt mahdollisuuksia hyökkääjille, vaan se myös kasvatti järjestelmän yleistä kestävyyttä ja vakautta (What is System Hardening, n.d).

Tässä opinnäytetyössä syvennyttiin erityisesti Debian 11 Linux-käyttöjärjestelmän kovennukseen, joka on olennainen osa monen organisaation IT-ympäristöä. Toimeksiantajana toimi innovatiivinen IT-palvelutalo Netum Oy, joka on omaksunut edistyksellisen lähestymistavan tietoturvaan. Toimeksiantaja käyttää räätälöityä Debian 11 -versiota, joka on suunniteltu erityisesti teknisiin tietoturva-arviointeihin, kuten penetraatiotestauksiin. Netum Oy:n kyberturvallisuuspalveluilla oli tarve entistä tehokkaammalle ja suojatummalle auditointiympäristölle. Tämä opinnäytetyö ei ole pelkästään osa tätä pyrkimystä, vaan myös näyttö modernin tietoturvatutkimuksen merkityksestä ja arvosta.

Työssä otettiin huomioon CIS (Center for Internet Security) viitekehyksen ensimmäisen ja toisen tason suosituksia, jotka edustavat laajalti tunnustettua ja arvostettua lähestymistapaa käyttöjärjestelmän turvallisuuden parantamiseen (About Us, n.d). Käyttöjärjestelmän kovennus ei ole pelkästään tekninen toimenpide, vaan se vaatii syvällistä ymmärrystä laitteistosta, laiteohjelmistoista, sovelluksista, ohjelmistoista, salasanoista ja monimutkaisista prosesseista (What is System Hardening, n.d).

Tämän opinnäytetyön merkittävin osa oli Debian 11 -käyttöjärjestelmän kovennuksen automatisointiin keskittyvä skripti. Se ei ole vain työkalu, vaan se edustaa Netum Oy:n kyberturvallisuustiimin jatkuvaa pyrkimystä huippuosaamiseen, nopeuttaen ja tehostaen heidän tietoturva-auditointikykyään.

1.1 Kehittämisongelma

Nykyisessä digitaalisessa maailmassa tietoturva on keskeinen huolenaihe. Linux-pohjaisia käyttöjärjestelmiä, kuten Debian, käytetään laajasti palvelimissa, työasemissa ja IoT-laitteissa. Yli 96 prosenttia maailman miljoonasta suurimmasta verkkopalvelimesta käyttää Linuxia alustanaan. (Linux Statistics, 2023.) Vaikka Linux on tunnettu vakautensa ja turvallisuutensa ansiosta, oletusasennukset voivat sisältää turvallisuusriskien muodostavia asetuksia ja palveluita.

Toimeksiantajalla oli käyttöönottovaiheessa Debian pohjainen käyttöjärjestelmä, jota käytetään tietoturva-arviointien suorittamiseen. Järjestelmään ei ole tehty järjestelmäkovennuksia, joka voi altistaa sen potentiaalisille haavoittuvuuksille. Vaikka järjestelmä toimii moitteettomasti normaaleissa olosuhteissa, sen tietoturva-asema voi olla puutteellinen silloin, kun se joutuu kohdennetun hyökkäyksen kohteeksi. Toimeksiantajan tietoturva-arviointitarpeet korostivat tarvetta kovennetulle järjestelmälle.

Opinnäytetyön tavoitteena oli vahvistaa toimeksiantajan järjestelmän tietoturvaa. Järjestelmään ajettujen järjestelmäkovennusten avulla pyrittiin vähentämään järjestelmän haavoittuvuuspinta-alaa, joka mahdollistaa luotettavampien tietoturva-arviointien suorittamisen. Kehittämistyön tulokset voivat toimia myös oppaana ja inspiraationa muille organisaatioille ja yksittäisille käyttäjille.

1.2 Tavoitteet ja kehittämistehtävät

Tämän projektin keskeisin ja kaikkein merkittävin tavoite oli kustomoidun Debian 11 -käyttöjärjestelmän kovennus. Tässä prosessissa keskityttiin erityisesti tietoturvan huomattavaan optimointiin ja järjestelmän haavoittuvien hyökkäyspintojen minimoimiseen. Tämä on erityisen tärkeää nykypäivän digitaalisessa ympäristössä, jossa tietoturvauhat ja hyökkäykset kehittyvät jatkuvasti.

Työn ytimessä oli järjestelmän suunnittelu ja räätälöinti erityisesti toimeksiantajan tietoturva-arviointitarpeisiin. Toimenpide paransi toimeksiantajan kykyä tunnistaa ja korjata potentiaalisia tietoturvauhkia sekä varmistaa järjestelmän vastetta toimeksiantajan spesifeihin vaatimuksiin ja toimintaympäristön erityispiirteisiin.

Lisäksi projektissa asetettiin laajempi tavoite: edistää tietoturva-alaa tarjoamalla konkreettinen ja perusteellinen esimerkki tehokkaasta Linux-käyttöjärjestelmän kovennuksesta. Tämän mallin toivotaan toimivan inspiraationa ja oppaana monille toimialan toimijoille, jotka pyrkivät nostamaan oman infrastruktuurinsa turvallisuustasoa.

1.3 Menetelmät

Opinnäytetyössä analysoitiin Center for Internet Securityn (CIS) tarjoamia parhaita käytänteitä Debian pohjaiselle käyttöjärjestelmälle. Kovennuksia peilattiin käyttöönotettavaan järjestelmään niin, että järjestelmästä saataisiin mahdollisimman kovennettu, kuitenkaan heikentämättä sen toimintakykyä tietoturva-arvioinneissa. Tämän lisäksi opinnäytetyössä kehitettiin kovennusskriptit Debian 11 -käyttöjärjestelmälle, joiden tehtävänä on tarkastaa järjestelmän asetukset valittujen parhaiden käytänteiden mukaisesti ja muokata asetuksia vastaamaan niitä, mikäli ne eivät täsmää.

1.4 Esiolettamukset

Opinnäytetyön painopisteen ollessa digitaalisen ympäristön tietoturvahaasteissa, oli ensisijaisena tavoitteena luoda huolellisesti kustomoitu ja kovennettu Debian 11-käyttöjärjestelmä. Tämä käyttöjärjestelmä on räätälöity vastaamaan erityisesti toimeksiantajan turvallisuuteen liittyviä tarpeita, jotka korostuvat tietoturva-arvioinnin kontekstissa. Työn tuloksena saadaan paitsi vankempi järjestelmä, myös syvällinen ja analyyttinen raportti kovennusprosessista. Tässä opinnäytetyössä keskityttiin kuvailemaan järjestelmän turvallisuudessa tapahtuneita muutoksia, tunnistettuja haavoittuvuuksia ja niiden huolellisia korjaustoimenpiteitä sekä antamaan perusteellinen kuva tehdystä työstä ja sen pitkäaikaisista vaikutuksista.

Sujuvan ja tehokkaan käyttökokemuksen varmistamiseksi laadittiin kattavat ja selkeästi muotoillut käyttöohjeet järjestelmän asennukseen, käyttöön ja ylläpitoon. Nämä ohjeet on erityisesti suunniteltu palvelemaan paitsi toimeksiantajaa, myös muita Linux-käyttäjiä ja organisaatioita, jotka ovat kiinnostuneita soveltamaan samankaltaisia kovennustoimenpiteitä omiin infrastruktuureihinsa. Ohjeet tarjoavat ratkaisumalleja yleisimpiin ongelmatilanteisiin, jotta voidaan varmistaa häiriötön ja turvallinen järjestelmän käyttökokemus.

2 Teoreettiset ja käsitteelliset lähtökohdat

2.1 Linux-käyttöjärjestelmä

Linux-käyttöjärjestelmä nousi esille vuonna 1991, kun suomalainen ohjelmistosuunnittelija Linus Torvalds esitteli maailmalle Linux-ytimen ensimmäisen version. Tämä oli merkittävä virstanpylväs, ja sen jälkeen, useiden yhteisöjen ja Free Software Foundationin panostuksen myötä, Linuxista on kasvanut yksi johtavista avoimen lähdekoodin käyttöjärjestelmistä, joka on laajasti adoptoitu eri laitteistoissa globaalisti. (Linux, 2023.) Avoimen lähdekoodin periaatteella tarkoitetaan koodin julkista saatavuutta sekä yhteisön mahdollisuutta muokata ja kehittää koodia edelleen. Tämä demokraattinen lähestymistapa ohjelmistokehitykseen mahdollistaa turvallisuusongelmien ja haavoittuvuuksien nopean havaitsemisen, ja ne voidaan näin korjata tehokkaammin kuin suljetun lähdekoodin järjestelmissä. (What is open source, 2019.) Perustasolla käyttöjärjestelmä on ohjelmistojen kokoelma, joka hallinnoi tietokoneen laitteistoa ja antaa resursseja sovelluksille. (Negus 2015, 5.) Linux-ydin on tärkeä osa käyttöjärjestelmää, ja se toimii sillanrakentajana tietokoneen laitteiston ja sovellusten välillä. (What is the Linux Kernel, 2019.)

Erottautuen monista kilpailevista käyttöjärjestelmistä, kuten Microsoftin Windowsista tai Applen Mac OS:stä, Linux tarjoaa useita eri jakeluversioita. Nämä Linux-jakelut ovat kehitetty erilaisiin tarpeisiin ja ympäristöihin. Jakelun kehittäminen ja mukauttaminen on mahdollista Linuxin avoimen lähdekoodin luonteen ansiosta. Yksi tunnetuimmista Linux-jakeluista on Ubuntu Linux, joka on suunniteltu käyttäjäystävälliseksi ja graafisen käyttöliittymän kautta helposti lähestyttäväksi. (Linux distributions, n.d) Graafisella käyttöliittymällä (GUI) tarkoitetaan visuaalista käyttöliittymää, joka mahdollistaa vuorovaikutuksen laitteen kanssa graafisten elementtien, kuten ikonien ja painikkeiden kautta. Muita merkittäviä Linux-jakeluita ovat esimerkiksi Debian, joka tunnetaan sen vakauden ja luotettavuuden ansiosta, Fedora, joka on tunnettu teknologian edelläkävijyydestään, sekä Kali Linux, joka keskittyy erityisesti tietoturvaan ja penetraatiotestaukseen. (Linux distributions, n.d; Kali Linux Tutorial, n.d.)

Kun tarkastellaan Linux-jakeluiden valintaa, on tärkeää huomioida monia seikkoja, kuten jakelun perusta ja historiallinen kehitys. Slackware, Debian ja Red Hat edustavat Linux-jakeluiden kehityksen kulmakiviä, joista on johdettu useita muita versioita ja jotka ovat olennaisia ymmärtää nykyisten jakeluiden kontekstissa.

Slackware on yksi GNU/Linux-jakeluiden pioneereista, joka on tunnettu minimalistisuudestaan ja manuaalisesta hallinnastaan. Sen periaatteet ja rakenteellinen yksinkertaisuus ovat vaikuttaneet monien muiden jakeluiden, kuten Salixin ja Zenwalkin, suunnitteluun. Slackwaren vaikutus Linux-maailmassa on merkittävä, tarjoten pohjan, jolle muut jakelut voivat rakentaa. (What is Slackware Linux, n.d.)

Debian seuraa Slackwarea vanhimpien jakeluiden joukossa ja on tunnettu vakauden, turvallisuuden ja luotettavuuden perintönä. Sen kehitysmalli ja tiukka testausprosessi ovat luoneet vankan perustan monille muille jakeluille, kuten Ubuntu ja Linux Mint. Debianin joustavuus ja laaja ohjelmistovalikoima tarjoavat ihanteellisen ympäristön erilaisten tietoturvatoimien, kuten kovennusten, toteuttamiseen. Debianin rooli on keskeinen, sillä se tarjoaa perustan, jolle monet muut jakelut ovat kehittyneet. (King, 2020.)

Red Hat, toinen merkittävä nimi Linux-maailmassa, on avoimen lähdekoodin ohjelmistoyritys, jonka tuotteet perustuvat Red Hat Enterprise Linuxiin (RHEL). RHEL ja sen yhteisöpohjainen versio Fedora ovat olleet alustana lukuisille johdannaisille, kuten CentOSille (nykyisin Rocky Linux ja AlmaLinux). Red Hatin innovaatiot ja sen ylläpitämä ekosysteemi ovat olleet tärkeitä avoimen lähdekoodin kehitykselle ja yrityskäytölle. (Terrell, 2021.)

Ymmärtämällä näiden kolmen jakelun – Slackwaren, Debianin ja Red Hatin – kehityshistorian ja niiden vaikutuksen muihin jakeluihin, saamme kattavan kuvan Linux-jakeluiden evoluutiosta ja siitä, miten ne ovat muovanneet nykyistä Linux-ekosysteemiä. Tämä historiallinen konteksti on arvokas, kun pohditaan sopivan ympäristön valintaa tietoturvatoimien toteuttamiseen, ja se auttaa ymmärtämään, miksi tietyt jakelut, kuten Debian, ovat ihanteellisia vakaiden ja turvallisten tietojärjestelmien rakentamiseen.

2.1.1 Turvallisuus

Linux-käyttöjärjestelmä on suunniteltu olemaan paitsi tehokas ja mukautuva, myös perustavanlaatuisesti turvallinen. Linux-yhteisössä yksityisyys ja tietoturva eivät ole pelkästään etusijalla, vaan ne ovat integroitu syvälle kehitysfilosofiaan. Käyttöjärjestelmän avoin kehitysmalli merkitsee, että laajennettu joukko kehittäjiä ja tietoturva-asiantuntijoita voi aktiivisesti tarkastella, tarkentaa ja

vahvistaa sen turvallisuusominaisuuksia. Tämä kollektiivinen valvonta ja kehitys on erityisen arvokasta ajassa, jolloin tietoturvaloukkaukset voivat aiheuttaa merkittäviä vahinkoja laajassa mittakaavassa. Vaikka Linux itsessään tarjoaa useita turvallisuusominaisuuksia, käyttöjärjestelmän loppukäyttäjien ja ylläpitäjien rooli on korvaamaton sen turvallisuuden ylläpidossa ja parantamisessa. (Kili, 2022.)

2.1.2 Kustomoitu Linux-käyttöjärjestelmä

Linux-käyttöjärjestelmän mukauttamisen ytimessä on kyky räätälöidä järjestelmää vastaamaan tarkasti käyttäjän tai organisaation spesifisiä tarpeita. Tässä prosessissa käyttäjä voi päättää, mitkä ohjelmistokomponentit sisällytetään järjestelmään, eliminoiden näin kaikki tarpeettomat elementit, jotka saattavat lisätä turvallisuusriskejä. Tämä ennakoiva ohjelmistojen valinta kustomoinnin aikana on keskeistä, sillä se mahdollistaa järjestelmän optimoinnin sekä toiminnallisuuden, että turvallisuuden kannalta, sisällyttäen vain välttämättömät ohjelmistot.

Tässä kustomoidussa ympäristössä ohjelmistojen valinnat on tehty huolellisesti jo kustomointivaiheessa, mikä tarkoittaa, että mahdolliset turvallisuusriskit on minimoitu jo ennen järjestelmän käyttöönottoa. Tämän seurauksena opinnäytetyö keskittyy muihin näkökohtiin, jättäen ohjelmistojen tarkastelun tietoisesti pois. Tämä valinta perustuu tunnistamiseen, että ohjelmistovalintojen kattava analyysi ja niiden turvallisuusvaikutusten arviointi olisi itsessään laaja tutkimus, mahdollisesti toisen opinnäytetyön mittainen projekti. Näin ollen, työssä keskitytään kustomoidun järjestelmän muihin kriittisiin aspekteihin, jotka tukevat toimeksiantajan tietoturvatavoitteita, samalla tunnustaen, että ohjelmistovalintojen syvällinen tarkastelu ylittäisi nykyisen opinnäytetyön laajuuden ja tavoitteet.

Tiedon saavutettavuuden riskien osalta on implementoitu useita turvatoimenpiteitä arkaluonteisen tiedon suojaamiseksi luvattomalta pääsyltä. Kehitetty järjestelmä hyödyntää eristyksen ja verkkoyhteydettömyyden periaatteita, jotka yhdessä fyysisen pääsyn vaatimuksen kanssa muodostavat tehokkaan suojan. Nämä toimenpiteet vähentävät merkittävästi ulkopuolisten pääsyn riskejä, turvaten näin arkaluonteisen tiedon. Jatkuva valppaus potentiaalisten haavoittuvuuksien tunnistamisessa ja korjaamisessa on välttämätöntä, erityisesti kun otetaan huomioon jatkuvasti muuttuva tietoturvauhkien maisema.

2.2 Käyttöjärjestelmien kovennus

Käyttöjärjestelmien kovennus tarkoittaa joukkoa strategisia toimenpiteitä, joiden avulla pyritään vähentämään IT-järjestelmien haavoittuvuutta ja parantamaan niiden kykyä vastustaa mahdollisia hyökkäyksiä. Kovennus ei ole pelkästään tekninen prosessi; se on myös strateginen lähestymistapa, jossa arvioidaan ja mukautetaan järjestelmän toimintaa ja konfiguraatiota vähentääkseen riskejä ja varmistaa, että parhaat mahdolliset turvallisuuskäytännöt ovat käytössä. (What is Systems Hardening, n.d.)

Käyttöjärjestelmän kovennuksen ensisijainen tavoite on pienentää järjestelmän hyökkäyspintaa, jolloin haavoittuvuuksien hyväksikäyttö tai ei-toivottujen toimijoiden pääsy järjestelmään estetään tai vaikeutetaan. Järjestelmässä voi aina olla sisäänrakennettuja heikkouksia tai haavoittuvuuksia, jotka ovat syntyneet suunnittelu- tai toteutusvaiheessa. Tämän vuoksi kovennuksen prosessi vaatii kriittistä tarkastelua ja jatkuvaa mukauttamista kunkin organisaation erityistarpeiden ja riskiprofiilin mukaan. (Stavrakas, 2022.)

Vaikka kovennuksen tavoitteena on vahvistaa tietoturvaa, on tärkeää muistaa, että täydellistä turvallisuutta ei ole olemassa. Kovennuksen tarkoituksena on vähentää riskejä, ei poistaa niitä kokonaan, ja on tärkeää olla tietoinen mahdollisista seurauksista, jotka voivat syntyä kovennustoimenpiteiden seurauksena. Näihin voi kuulua käyttömukavuuden heikkeneminen, ylläpidon vaativuuden kasvu ja potentiaaliset kustannukset, jotka liittyvät kovennuksen toteuttamiseen ja ylläpitoon. (Stavrakas, 2022.)

2.3 Olemassa olevat työkalut

Olemassa olevat työkalut tarjoavat vankan perustan ymmärtää nykyisiä käytäntöjä ja teknologiota, jotka on suunniteltu parantamaan järjestelmien turvallisuutta. Tässä kappaleessa käydään läpi joukon tunnettuja kovennustyökaluja, jotka toimivat vertailukohtana kehittämälleni työkalulle.

Lynis on korkeatasoinen turvallisuusauditointityökalu, joka on suunniteltu Linux-, macOS- ja Unix-pohjaisten alustojen tietoturvan vahvistamiseen. Sen pääasiallinen käyttötarkoitus kattaa laajan spektrin tietoturvaan liittyviä toimenpiteitä, kuten järjestelmän kovennuksen, vaatimustenmukai-

suuden testaamisen ja turvallisuusauditoinnin. Vuodesta 2007 lähtien saatavilla ollut tämä avoimen lähdekoodin projekti, lisensoitu GPL:n alaisuudessa, on erinomainen valinta organisaatioille, jotka haluavat suorittaa perusteellisia tarkastuksia ja parantaa järjestelmiensä tietoturvaa. (Lynis, an introduction, n.d.) Kun vertaillaan Lynistä itsetehtyyn työkaluun, joka noudattaa CIS viitekehyksiä, on tärkeää huomioida, miksi räätälöity ratkaisu voi olla parempi joissain tilanteissa. Itse tehty työkalu voidaan täysin räätälöidä organisaation tarpeisiin, ottaen huomioon erityiset vaatimukset ja ympäristön.

CIS Build Kitit ovat Center for Internet Securityn (CIS) tarjoamia työkaluja, jotka on suunniteltu auttamaan järjestelmien kovennusprosessin automatisoinnissa. Ne perustuvat kunkin CIS Benchmarkin "Remediation" -osioon, tarjoten skriptejä tai malleja, jotka kattavat valtaosan benchmark-asetuksista. (CIS Build Kits FAQ, n.d.) Itse tehty kovennustyökalu käyttää CIS:n viitekehyksiä kovennuksissa. CIS Build Kit olisi hyvä ratkaisu järjestelmäkovennuksien ylläpitoon, mutta CIS SecureSuite membership on melko kallis, jos sitä ei pystytä hyödyntämään tarpeeksi laajalla alueella.

OpenSCAP on avoimen lähdekoodin työkalu, joka tarjoaa kattavan ratkaisun tietoturvan vaatimustenmukaisuuden ja haavoittuvuusanalyysin hallintaan. Sen keskeinen komponentti, oscap-komentorivityökalu, mahdollistaa monipuoliset toiminnot, kuten paikallisten järjestelmien konfiguraatio- ja haavoittuvuusskannaukset, turvallisuusvaatimustenmukaisuussisällön validoinnin sekä näiden skannausten ja arviointien perusteella raporttien ja ohjeiden generoinnin. (Compliance and Vulnerability Scanning with OpenSCAP, n.d.) OpenSCAP ei suoranaisesti kovenna järjestelmiä. Tämä ratkaisu voisi olla hyvä lisä itse tehdyn kovennustyökalun rinnalle, mutta sitä ei oteta käyttöön järjestelmään, koska sen skannausten intensiivisyys saattaa hidastaa järjestelmän toimintakykyä.

2.4 Kyberturvallisuuden viitekehykset

Viitekehys kyberturvallisuuden näkökulmasta tarkoittaa standardoitua tai laajasti hyväksyttyä ohjeistusta, joka sisältää parhaita käytäntöjä, suosituksia, politiikkoja, menetelmiä ja ohjeita tietoturvan hallintaan ja ylläpitoon organisaatioissa. Kyberturvallisuuden viitekehykset on suunniteltu auttamaan organisaatioita suojaamaan tietojärjestelmiänsä, verkkojaan ja dataansa erilaisilta

tietoturvariskeiltä, parantamaan reagointivalmiutta tietoturvaloukkauksiin ja hallitsemaan tietoturvauhkia tehokkaammin.

Esimerkkejä tunnetuista kyberturvallisuuden viitekehyksistä ovat mm. NIST:n kyberturvallisuuden viitekehys (Cybersecurity Framework), jonka on kehittänyt Yhdysvaltain kansallinen standardi- ja teknologiainstituutti (NIST), ja se tarjoaa yleismaailmallisia ohjeita tietoturvauhkien hallintaan liittyen. (Gillis, 2024.) ISO/IEC 27001, kansainvälinen standardi, joka määrittelee vaatimukset tietoturvan hallintajärjestelmälle (ISMS), tarjoten kehyksen tietoturvariskien hallintaan. (Kosutic, n.d.) Sekä tässä opinnäytetyössä hyödynnetyt CIS viitekehykset, jotka ovat Center for Internet Securityn (CIS) kehittämiä maailmanlaajuisesti tunnustettuja parhaita käytäntöjä, jotka auttavat tietoturvallisuuden ammattilaisia toteuttamaan ja hallinnoimaan kyberturvallisuuden puolustusta. Ne on kehitetty globaalissa yhteisössä turvallisuusasiantuntijoiden kanssa, ja ne tarjoavat ohjeita organisaatioille suojaamaan itseään proaktiivisesti uusilta riskeiltä. CIS Viitekehykset tarjoaa suosituksia yli 25 eri toimittajan tuotteiden turvalliseen käyttöönottoon, ja niitä käytetään muun muassa käyttöoikeuksien rajoittamiseen, tarpeettomien porttien sulkemiseen ja ylimääräisten sovellusoikeuksien poistamiseen. (What are CIS Benchmarks, n.d.)

2.4.1 Parhaat käytänteet Debianin kovennukseen

CIS viitekehysten Debian järjestelmäkovennukset on jaettuna kuuteen eri osa-alueeseen, jotka ovat 1. alustava asennus, 2. palvelut, 3. verkko, 4. lokitus ja auditointi, 5. pääsy, tunnistus ja valtuutus sekä 6. ylläpito. Tässä kappaleessa käydään läpi jokainen osio ja niiden sisältävät suositukset sekä suositusten koventamisen vaikutus järjestelmän toimivuuteen ja turvallisuuteen.

Alustava asennus osion -alle sijoitetut kovennukset on otettava huomioon jo manuaalisessa asennusvaiheessa tai välittömästi sen jälkeen. Nämä suositukset voivat olla haastavia tai jopa mahdottomia toteuttaa myöhemmin järjestelmän käyttöönoton jälkeen. Alustavan asennuksen piiriin kuuluvat toimenpiteet kattavat tiedostojärjestelmän konfiguroinnin, ohjelmistopäivitysten määrittämisen, tiedostojärjestelmän eheyden varmistamisen, turvallisen käynnistyksen, pakollisen pääsynvalvonnan, komentorivin varoitusviestit, GNOME-näyttöhallinnan sekä erilaiset päivitykset, korjaukset ja lisäsuojaussovellukset. (CIS Debian Linux 11 Benchmark, 2022.)

Palvelut osiossa käsitellään kolmea keskeistä aluetta: ajan synkronointia, järjestelmäpalveluita ja asiakasohjelmistoja. Nämä alueet ovat olennaisia järjestelmän asianmukaisen toiminnan ja ylläpidon kannalta, tarjoten perustan, jonka varaan muut järjestelmän osat rakentuvat. Ajan synkronointi varmistaa, että kaikki järjestelmän kellot ovat yhdenmukaisia, järjestelmäpalvelut huolehtivat järjestelmän perustoiminnoista ja asiakasohjelmistot tarjoavat käyttäjille tarvittavat työkalut ja toiminnot järjestelmän tehokkaaseen käyttöön. (CIS Debian Linux 11 Benchmark, 2022.)

Verkko osiossa käsitellään kolmea tärkeää verkkoaiheista aluetta: käyttämättömien verkkoprotokollien ja -laitteiden hallintaa, verkon parametrien säätöä sekä palomuurin käyttöä. Käyttämättömien verkkoprotokollien ja -laitteiden hallinta auttaa vähentämään turhia riskejä, parantamaan järjestelmän turvallisuutta ja optimoimaan suorituskykyä. Verkon parametrien säätäminen on keskeistä verkkoyhteyksien luotettavuuden ja tehokkuuden kannalta. Palomuuri puolestaan on välttämätön työkalu järjestelmän suojaamiseksi ulkoisilta uhilta, tarjoten ensilinjan puolustuksen haitallisia verkkoaktiviteetteja vastaan. (CIS Debian Linux 11 Benchmark, 2022.)

Lokitus ja auditointi -osiossa keskitytään kahteen kriittiseen osa-alueeseen: järjestelmän auditointiin ja lokitukseen. Järjestelmän auditointi on keskeinen prosessi, jossa valvotaan ja tarkastetaan järjestelmän toimintaa ja turvallisuutta, varmistetaan säädösten noudattaminen ja tunnistetaan mahdolliset turvallisuuspoikkeamat. Lokitus puolestaan on tärkeä työkalu tapahtumien kirjaamiseen, joka mahdollistaa tehokkaan seurannan, ongelmien diagnosoinnin ja turvallisuustapahtumien analysoinnin. Yhdessä nämä toiminnot muodostavat perustan järjestelmän valvonnalle ja turvallisuuden ylläpidolle. (CIS Debian Linux 11 Benchmark, 2022.)

Pääsy ja valtuutus -osiossa käsitellään viittä avaintekijää, jotka liittyvät pääsyn, tunnistuksen ja valtuutuksen hallintaan: aikaan perustuvia tehtäväajoittimia, SSH-palvelinta, käyttöoikeuksien kohottamista, autentikointimoduuleja sekä käyttäjätilejä ja niiden ympäristöjä. Aikaan perustuvat tehtäväajoittimet mahdollistavat automaattiset toiminnot määriteltyinä aikoina, mikä tehostaa järjestelmän hallintaa. SSH-palvelin tarjoaa turvallisen tavan etäyhteyksien hallintaan. Käyttöoikeuksien kohottaminen on keskeinen osa käyttöoikeuksien hallintaa, varmistaen oikeat käyttöoikeudet tarvittaessa. Autentikointimoduulit ovat olennaisia järjestelmän käyttäjien tunnistamisessa ja valtuuttamisessa. Käyttäjätilit ja niiden ympäristöt ovat perusta käyttäjien toiminnalle ja heidän oikeuksiensa hallinnalle järjestelmässä. (CIS Debian Linux 11 Benchmark, 2022.)

Ylläpito -osiossa keskitytään kahteen olennaiseen ylläpitotoimenpiteeseen: järjestelmän tiedostojen oikeuksiin ja paikallisten käyttäjien sekä ryhmien asetuksiin. Järjestelmän tiedostojen oikeudet ovat kriittisiä järjestelmän turvallisuuden ja eheyden kannalta, ja niiden asianmukainen määrittely varmistaa tietoturvan säilymisen. Toisaalta paikallisten käyttäjien ja ryhmien asetukset ovat keskeisiä hallittaessa käyttöoikeuksia ja käyttäjien toimintaa järjestelmässä. Näiden asetusten avulla voidaan määritellä käyttäjien roolit, oikeudet ja rajoitukset, joka on tärkeää järjestelmän hallinnoidun ja turvallisen käytön varmistamiseksi. (CIS Debian Linux 11 Benchmark, 2022.)

3 Toteutus

Järjestelmäkovennuksia varten luotiin bash-skripti, jonka tehtävänä on tarkastaa järjestelmän tila tiettyjen suositusten osalta ja tämän jälkeen tehdä tarvittavat toimenpiteet järjestelmään, jotta asetukset täsmäävät valittuihin parhaisiin käytäntöihin. Skriptit on luotu CIS viitekehysten pohjalta, ja ne ovat olleet testauksen kohteena useita kymmeniä kertoja.

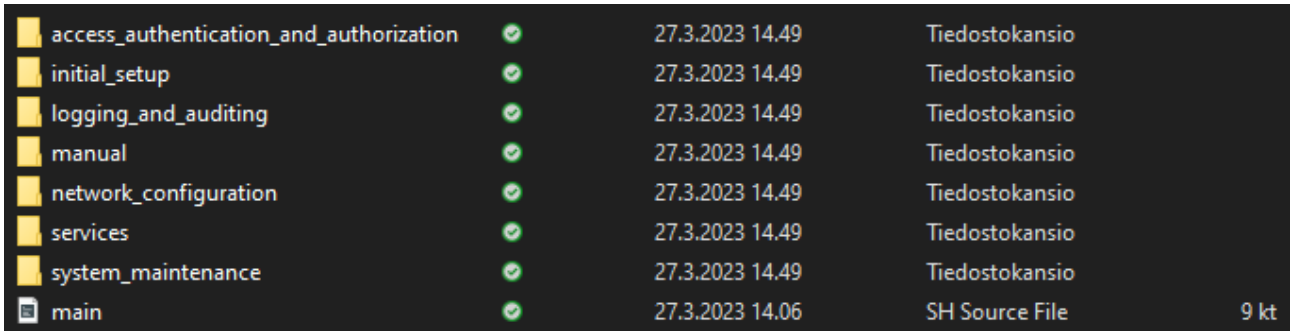
Projektin lähdekoodi on saatavilla julkisesti GitHub-repositoriossa, joka on lisensoitu Creative Commons -lisenssillä. Lisenssi mahdollistaa teoksen vapaan käytön, muokkauksen ja levittämisen niin kauan kuin alkuperäinen tekijä (tässä tapauksessa minä) mainitaan ja uudelleenjaot noudattavat samaa lisenssiä. (Vähämaa, 2024)

Järjestelmän koventaminen vaatii tasapainottelua turvallisuuden ja käytettävyyden välillä. Kovennusprosessi aloitettiin analysoimalla kaikki Debian 11 työpöytäympäristöön tarkoitetut tason 1 sekä 2 suositukset. Tässä hyödynnettiin tietoa siitä, mitä työkaluja järjestelmässä tullaan käyttämään ja miten. Järjestelmää kovennettaessa on tärkeää tuntea kyseisen järjestelmän toiminnot, jotta järjestelmäkovennukset pienentävät haavoittuvuuspinta-alaa, kuitenkin ottaen huomioon sen, että järjestelmän käytettävyys ei heikenny.

Liitteessä 1. on lueteltuna kaikki CIS viitekehyksissä olevat, työpöytäympäristöön tarkoitetut suositukset molemmilta tasoilta. Suositukset ovat käännettyinä suomen kielelle ja jokaisessa suosituksessa on suomennettu yhteenveto suosituksen kuvauksesta ja vaikutuksesta.

3.1 Skriptin kirjoittaminen

Skripti on kirjoitettu Visual Studio Codessa bash-skriptinä. Erilaisia skriptejä työssä on 42 kappaletta mukaan lukien pääskripti, josta kutsutaan luokitellut skriptit tietyssä järjestyksessä. Kuviossa 1. näkyvä ”main” tiedosto on pääskripti. Järjestelmäkovennuksessa käytettävä skripti on kokonaan opinnäytetyön kirjoittajan kirjoittama, johon on käytetty apuna CIS viitekehysten julkisen dokumentin aineistoa.



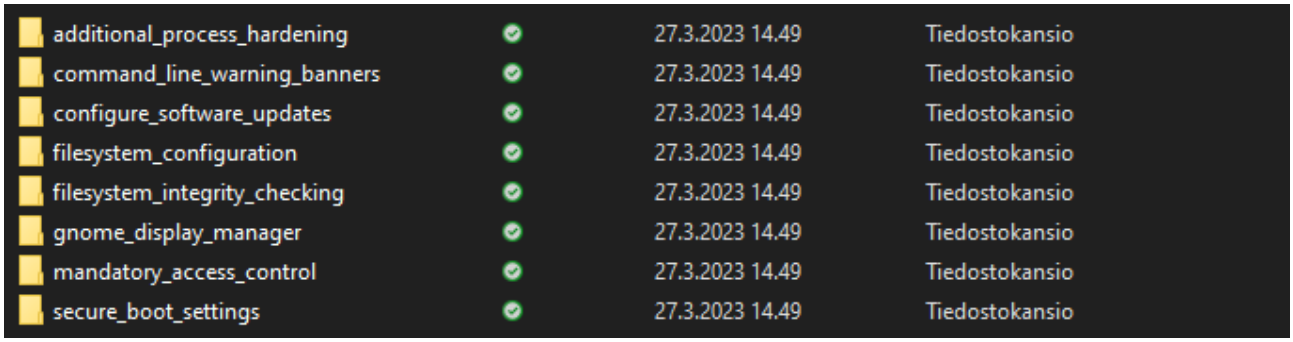
Kuvio 1. Kovennus -kansion sisältö

Kuviossa 2. on kuvakaappaus osittaisesta pääskriptin sisällöstä. Alussa luodaan kovennukset hakemisto käyttäjän kotihakemiston sisälle ja luodun hakemiston sisälle luodaan tekstitiedostot, johon kovennuksissa ilmenevät virheet, onnistumiset ja korjaukset kirjataan jälkitarkastelua varten.

```
#!/bin/bash

# Create a directory for the output files
mkdir /home/lab/kovennukset

# Initialize the pass and fail output files
touch "/home/lab/kovennukset/security_check_pass.txt"
touch "/home/lab/kovennukset/security_check_fail.txt"
touch "/home/lab/kovennukset/security_check_fix.txt"

passFile="/home/lab/kovennukset/security_check_pass.txt"
failFile="/home/lab/kovennukset/security_check_fail.txt"
fixFile="/home/lab/kovennukset/security_check_fix.txt"
lyellow='\e[33m'
yellow='\e[93m'
reset='\e[0m'

pathInitial="/home/lab/Scripts/initial_setup"
pathServices="/home/lab/Scripts/services"
pathNetwork="/home/lab/Scripts/network_configuration"
pathLogging="/home/lab/Scripts/logging_and_auditing"
pathAccess="/home/lab/Scripts/access_authentication_and_authorization"
pathSystem="/home/lab/Scripts/system_maintenance"

echo -e "${yellow}\n-------------------------------------------------------
echo -e "${lyellow}\n-----------------------------------------------\n#
bash $pathInitial/filesystem_configuration/disable_unused_filesystems.sh
bash $pathInitial/filesystem_configuration/configure_tmp.sh
bash $pathInitial/filesystem_configuration/configure_var.sh
bash $pathInitial/filesystem_configuration/configure_var_tmp.sh
bash $pathInitial/filesystem_configuration/configure_var_log.sh
bash $pathInitial/filesystem_configuration/configure_var_log_audit.sh
bash $pathInitial/filesystem_configuration/configure_home.sh
```

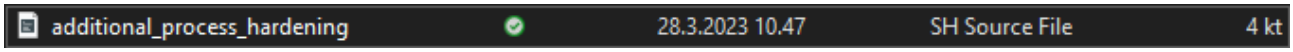
Kuvio 2. Pääskriptin sisältöä

Jokaisen kuviossa 1. näkyvän hakemiston alla on lisää alihakemistoja ja niiden hakemistojen alta löytyvät itse ajettavat skriptit, skriptit on jaoteltu hakemistoihin selvyyden vuoksi, jotta ylläpitotoimet ovat sujuvampia. Kuviossa 3. on hakemiston ”Initial Setup” sisältö.



Kuvio 3. Initial Setup -kansion sisältö

Kuviossa 4. nähdään additional process hardening -kansion sisältö, kansio sisältää yhden skriptitiedoston. Kansion skriptien lukumäärä määräytyy niiden kategorisoinnin perusteella, joissain kansioissa voi olla useampiakin skriptejä.



Kuvio 4. Additional process hardening -kansion sisältö

Skripti alkaa esimerkkikuviossa 5. merkeillä #!/bin/bash, joka on Unix-pohjaisissa järjestelmissä käytetty shebang-rivi. Rivi ilmoittaa skriptin alussa järjestelmälle, mitä komentotulkkia tulisi käyttää skriptin suorittamiseen. #!/bin/bash kertoo, että skripti tulee suorittaa Bash-komentotulkilla. Kuviossa 5. nähdään myös kyseisen skriptin ensimmäinen kovennus. Tyypillisesti kaikki skriptit ovat samanlaisia rakenteeltaan:

1. Skriptin alussa on kommenttikenttä, joka kertoo, mikä kovennus on kyseessä. Tämä auttaa ylläpitäjiä löytämään tietyn kovennuksen skriptistä, jos skripti on pitkä.
2. Seuraavaksi skripti ”echottaa” eli tulostaa käyttäjän terminaaliin tekstin, mitä kovennusta skripti ajaa.
3. Kolmanneksi skripti alkaa suorittamaan itse kovennusta, aluksi se tarkastaa kyseiseen kovennukseen liittyvän asian tilan, ja mikäli tila ei ole haluttu se tekee muutokset else lausekkeen sisällä. Muutoksien jälkeen se varmistaa tilan vielä kertaalleen, ja kirjoittaa sen perusteella pääskriptissä luotuun tiedostoon, mikäli kovennus on onnistunut tai epäonnistunut.

```
#!/bin/bash

# Check if address space layout randomization (ASLR) is enabled
echo "Ensuring 'ASLR' is enabled"
if sysctl kernel.randomize_va_space | grep -q "^kernel.randomize_va_space = 2$"; then
    echo "Address Space Layout Randomization (ASLR) is enabled" >> "/home/lab/kovennukset/security_check_pass.txt"
else
    printf "kernel.randomize_va_space = 2" >> /etc/sysctl.d/60-kernel_sysctl.conf
    sysctl -w kernel.randomize_va_space = 2
    if sysctl kernel.randomize_va_space | grep -q "^kernel.randomize_va_space = 2$"; then
        echo "Address Space Layout Randomization (ASLR) is enabled" >> "/home/lab/kovennukset/security_check_fix.txt"
    else
        echo "Address Space Layout Randomization (ASLR) is not enabled" >> "/home/lab/kovennukset/security_check_fail.txt"
    fi
fi
```

Kuvio 5. Additional process hardening -skriptin ensimmäinen kovennus

Kuviossa 6. nähdään saman skriptin seuraavia osia, jossa tarkastetaan mm. onko prelink asennettuna ja tehdään tarvittavat toimenpiteet, mikäli tulos ei ole haluttu.

```
#--------------------------------------------------------------------------------

# Check if prelink is not installed
echo "Ensuring 'prelink' is not installed"
if dpkg-query -W -f='${Status}' prelink 2>/dev/null | grep -q "install ok installed"; then
    prelink -ua
    apt purge -y prelink > /dev/null 2>&1
    if dpkg-query -W -f='${Status}' prelink 2>/dev/null | grep -q "install ok installed"; then
        echo "Prelink is installed" >> "/home/lab/kovennukset/security_check_fail.txt"
    else
        echo "Prelink is not installed" >> "/home/lab/kovennukset/security_check_fix.txt"
    fi
else
    echo "Prelink is not installed" >> "/home/lab/kovennukset/security_check_pass.txt"
fi

#--------------------------------------------------------------------------------

# Check if Automatic Error Reporting is not enabled
echo "Ensuring Automatic Error Reporting is not enabled"
if [ ! -f /etc/default/apport ]; then
    echo "Automatic Error Reporting is not enabled" >> "/home/lab/kovennukset/security_check_pass.txt"
elif grep -q "^enabled=0" /etc/default/apport; then
    echo "Automatic Error Reporting is not enabled" >> "/home/lab/kovennukset/security_check_pass.txt"
else
    apt purge -y apport > /dev/null 2>&1
    if [ ! -f /etc/default/apport ]; then
        echo "Automatic Error Reporting is not enabled" >> "/home/lab/kovennukset/security_check_fix.txt"
    elif grep -q "^enabled=0" /etc/default/apport; then
        echo "Automatic Error Reporting is not enabled" >> "/home/lab/kovennukset/security_check_fix.txt"
    else
        echo "Automatic Error Reporting is enabled" >> "/home/lab/kovennukset/security_check_fail.txt"
    fi
fi

#--------------------------------------------------------------------------------
```

Kuvio 6 Additional process hardening -skriptin sisällön jatko-osa

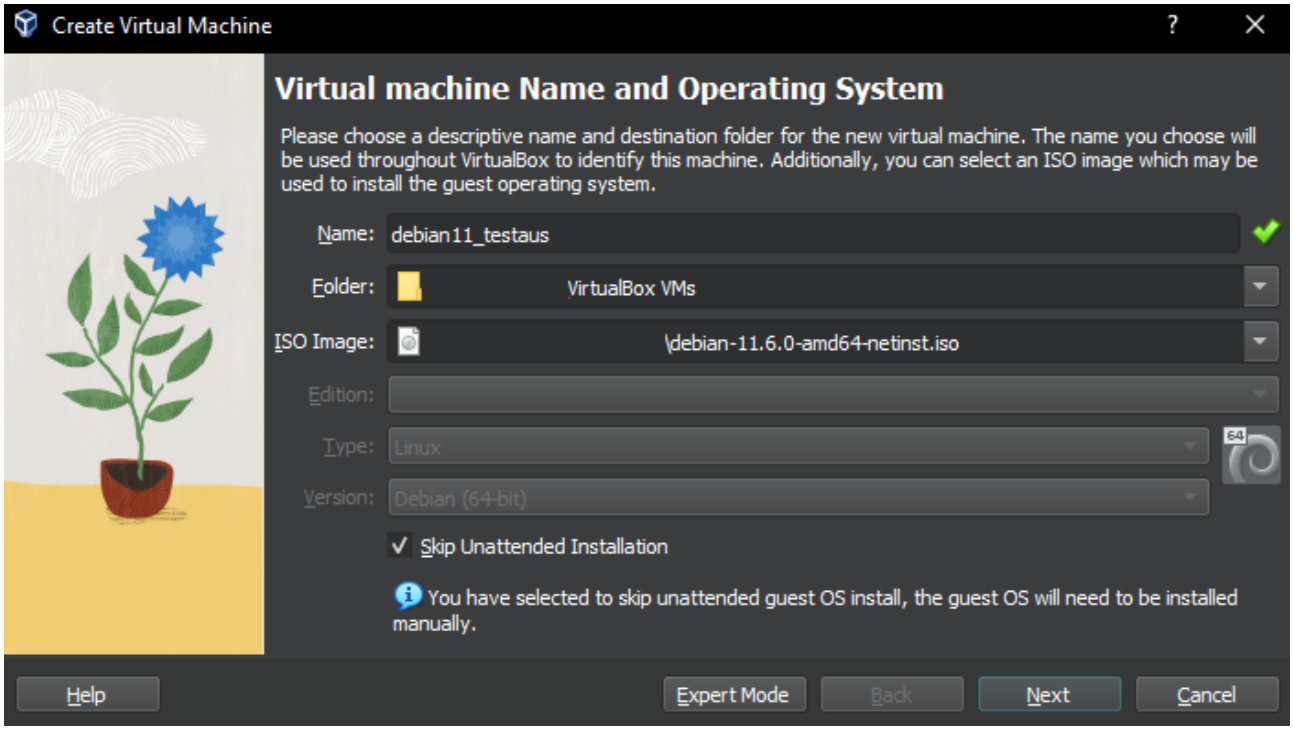
3.2 Skriptin testaaminen

Skriptiä testataan vasta-asennettua Debian 11 käyttöjärjestelmää vasten, johon ei olla vielä tehty mitään muutoksia. Tällä pyritään varmistamaan todellinen skenaario, koska skripti on tarkoitus ajaa järjestelmän asennusvaiheessa.

3.2.1 Virtuaalikone

Tietoturva-arvioinneissa käytettyä Debian käyttöjärjestelmää käytetään virtuaalikoneessa, joten skriptin testaaminen pyritään myös testaamaan virtualisoidussa ympäristössä. Tätä varten täytyy luoda virtuaalikone testausta varten.

Kuten kuviossa 7. nähdään, virtuaalikone luodaan Oracle Virtualbox -ohjelmassa. Virtuaalikoneen asetuksilla ei ole merkitystä kovennusten toimivuuteen. Asennusvaiheessa on muutamia kohtia, jotka täytyy ottaa huomioon, kuten alkuperäisessä asennuskohdassa mainittiin.

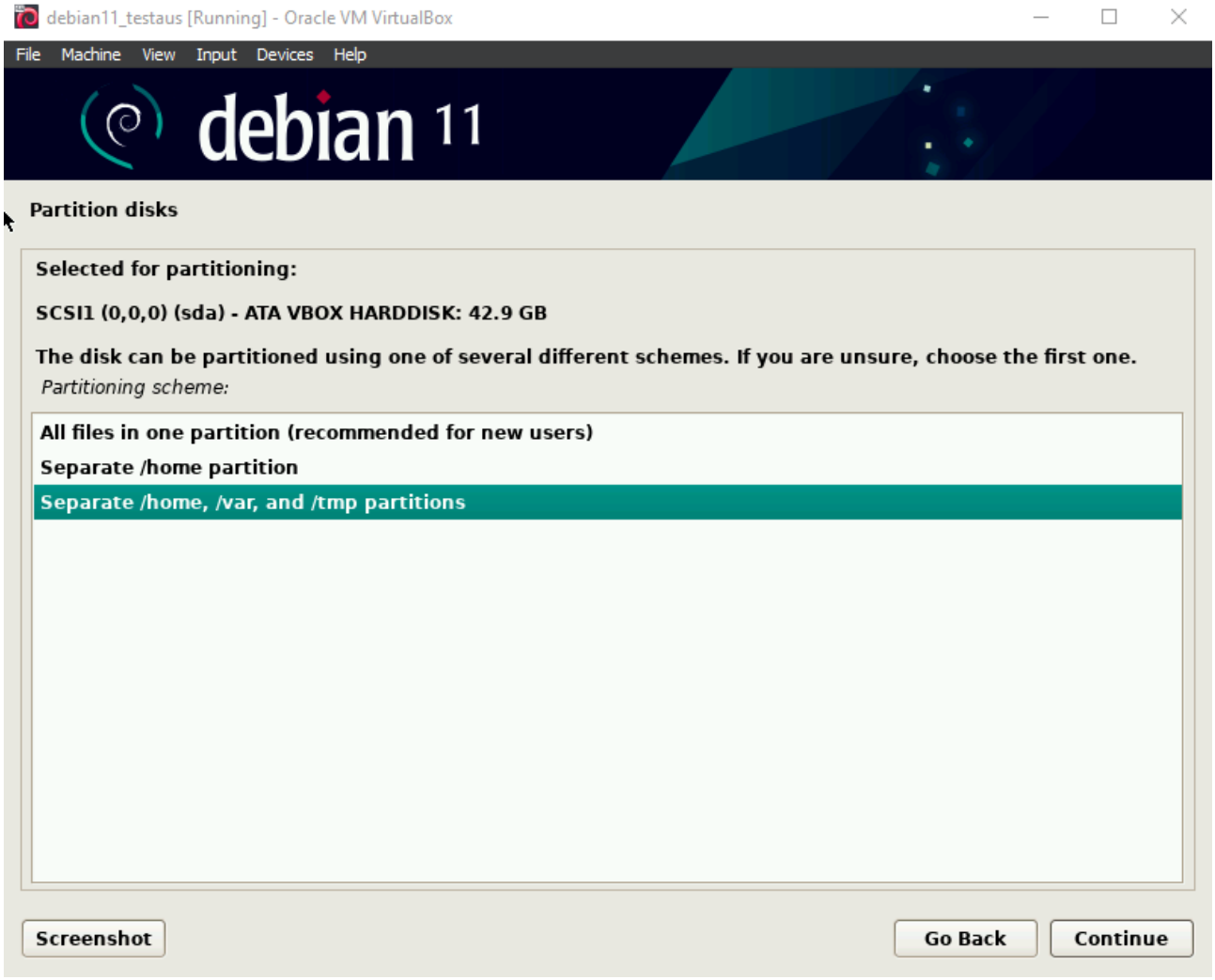


Kuvio 7. Virtuaalikoneen luonti

Asennusvaiheessa käyttäjältä kysytään osioinnin yhteydessä, kuinka osiointi halutaan tehdä ja mitä asetuksia siihen laitetaan. Tietoturva-arviointi kohdassa nämä asetukset on määritelty pre-seed -tiedostoon, joka tekee valinnat automaattisesti, mutta kovennusten testausvaiheessa pre-seed ei ole vielä valmis, joten manuaalinen konfigurointi on pakollista. Kuviossa 8. nähdään valinta ”use entire disk and set up encrypted LVM”. Tämä on tärkeää, sillä järjestelmässä tulee olla käytössä salattu levy.

Kuvio 8. Levynsalaus

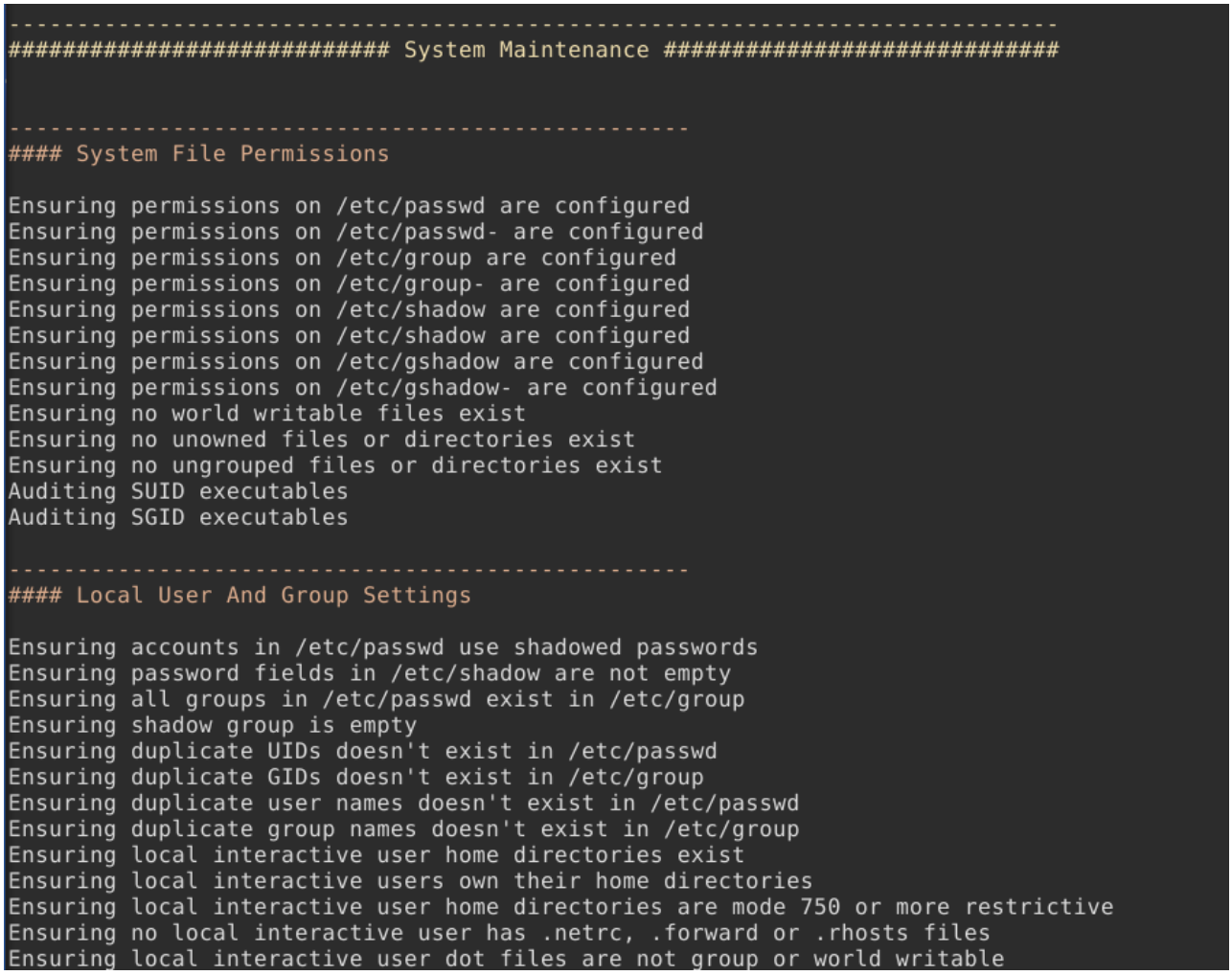
Kuviossa 9. käyttäjältä kysytään levyjaosta, järjestelmässä levyosiot jaetaan erillisiin /home, /var ja /tmp -osioihin, koska se voidaan tehdä vielä automaattisessa levynjaossa. Tämä on tärkeä valita asennusvaiheessa, koska levynjako asennetussa järjestelmässä voi olla vaikeaa.



Kuvio 9. Levynjako

3.3 Kovennusten testaus

Kovennusten testaus on keskeinen osa tietoturvan parantamisessa, jossa pyritään minimoimaan järjestelmän haavoittuvuudet tunnistamalla ja korjaamalla mahdolliset hyökkäyspinta-alat. Testausprosessi alkaa siirtämällä kirjoitetut skriptit isäntäkoneelta virtuaalialustaan. Nämä skriptit suoritetaan terminaalissa pääkäyttäjän oikeuksin. Skriptien toiminta on monivaiheista: ensin ne tarkastavat nykyiset järjestelmäasetukset, toteuttavat määritellyt kovennukset ja lopuksi varmentavat muutosten onnistumisen. Jokainen vaihe ja sen tulokset dokumentoidaan selkeästi, jolloin prosessin etenemistä voi seurata. Esimerkiksi, terminaaliin tulostuvat lokit (kuten Kuviossa 10. näkyy) antavat välitöntä palautetta kovennusten tilasta, mahdollistaen käyttäjälle yksityiskohtaisen seurannan.



Kuvio 10. Kuvakaappaus terminaalista, kun skripti ajetaan

Prosessin päätteeksi ”kovennukset”-kansioon kotihakemistossa tallentuvat tekstitiedostot tarjoavat yksityiskohtaisen yhteenvedon suoritettujen toimenpiteiden tuloksista. Nämä tiedostot, jotka sisältävät tietoa onnistuneista sekä mahdollisista epäonnistuneista kovennuksista, ovat arvokkaita sekä dokumentaation että jatkokehityksen näkökulmasta. Visuaalinen materiaali, kuten kuvakaappaukset onnistuneista ja epäonnistuneista kovennuksista (Kuviot 11 ja 12), tukevat tekstiä antamalla konkreettisen näkymän skriptien vaikutuksista.

```
lab@debian:~/kovennukset$ cat security_check_fail.txt

--------------------------------------------------------------------------------
################################ Initial Setup ################################


------------------------------------------------
#### Filesystem Configuration


------------------------------------------------
#### Configure Software Updates


------------------------------------------------
#### Filesystem Integrity Checking


------------------------------------------------
#### Secure Boot Settings
```

Kuvio 11. Kuvakaappaus epäonnistuneista kovennuksista

```
--------------------------------------------------------------------------------
################## Access Authentication And Authorization ##################


------------------------------------------------
#### Configure Time-Based Job Schedulers (cron)

cron daemon is enabled and running
permissions on /etc/crontab are configured
permissions on /etc/cron.hourly are configured
permissions on /etc/cron.daily are configured
permissions on /etc/cron.weekly are configured
permissions on /etc/cron.monthly are configured
permissions on /etc/cron.d are configured
cron is restricted to authorized users
at is restricted to authorized users

------------------------------------------------
#### Configure SSH Server

openssh-server is not installed

------------------------------------------------
#### Configure Privilege Escalation

sudo is installed
sudo commands use pty
sudo log file exists
Users must provide password for privilege escalation
re-authentication for privilege escalation is not disabled globally
sudo authentication timeout is configured correctly
Access to the su command is restricted.

------------------------------------------------
#### Configure PAM
```

Kuvio 12. Kuvakaappaus onnistuneista kovennuksista

4 Tulokset

Kehitetyssä kovennus- ja testausprosessissa saavutetut tulokset tarjoavat arvokasta tietoa kustomoidun Linux-järjestelmän turvallisuuden parantamiseksi. Prosessissa käytetty skripti, joka toimii sekä tarkastus- että korjaustyökaluna, on osoittautunut tehokkaaksi useiden tietoturvaan liittyvien puutteiden tunnistamisessa ja korjaamisessa. Kaksivaiheisessa lähestymistavassa järjestelmän asetukset ensin tarkastetaan, suoritetaan tarvittavat kovennukset ja lopuksi tarkastetaan asetukset uudelleen, mikä varmistaa, että kaikki turvatoimenpiteet on asianmukaisesti toteutettu. Tämä menettely ei ainoastaan lisää järjestelmän turvallisuutta vaan myös tuottaa arvokasta dokumentaatiota turvallisuuden kehittymisestä ajan myötä.

Vaikka kirjallista palautetta auditoijilta ei ole saatavilla, järjestelmän testaus ja arviointi ovat olleet keskeisiä osia sen kehittämisprosessissa. Epäviralliset keskustelut asiantuntijoiden kanssa ja heidän havaintonsa ovat ohjanneet kehitystyötä, korostaen turvallisuuden jatkuvan parantamisen merkitystä. Näiden vuorovaikutusten kautta saadut oivallukset ovat olleet arvokkaita tunnistettaessa alueita, joilla järjestelmää voidaan edelleen vahvistaa.

Penetraatiotestauksessa saatu tieto järjestelmän kyvystä suojautua ulkoisilta hyökkäyksiltä on ollut merkittävää, auttaen tunnistamaan ja korjaamaan mahdolliset heikkoudet. Tämä analyysi on keskeinen osa turvallisuuden kokonaisvaltaista parantamista, varmistaen, että järjestelmä on mahdollisimman suojattu nykyisiä ja tulevia uhkia vastaan.

5 Pohdinta

Opinnäytetyön tuloksena oli tietoturvan näkökulmasta parannettu käyttöjärjestelmä, jota voidaan käyttää turvallisesti niin sisäisissä kuin ulkoisissakin tietoturva-arvioinneissa. On tärkeää muistaa, että vaikka tulokset osoittavat kovennukset parantavan järjestelmän tietoturvaa, tietoturva on edelleen jatkuva prosessi. Uusia haavoittuvuuksia löytyy päivittäin ja myös viitekehykset saattavat niiden takia muuttua. Uusimpien haavoittuvuuksien seuraaminen on tärkeässä roolissa myös kovennusten jälkeisenä aikana, jotta uusimmat tietoturvapäivitykset voidaan ajaa sisään nopealla aikataululla. Tämän projektin aikana en oppinut pelkästään kovennusten toteutuksesta, vaan myös niiden tärkeydestä ja merkityksestä kasvavassa digitaalisessa yhteiskunnassa.

Kovennustoimenpiteiden ylläpito päivitysten yhteydessä on keskeinen osa järjestelmän turvallisuuden varmistamista. Kun järjestelmä päivitetään käyttöönoton yhteydessä, on tärkeää varmistaa, että kaikki kovennukset ovat edelleen voimassa ja toimivat suunnitellusti. Tämä edellyttää säännöllistä katselmointia ja seurantaa, jossa tarkistetaan, että kovennukset pysyvät aktiivisina ja tehokkaina. Tällainen lähestymistapa varmistaa, että järjestelmä säilyy turvallisena ja päivitettynä, minimoiden uusien haavoittuvuuksien riskin ja ylläpitäen korkeaa turvallisuustasoa.

Tulosten luotettavuus on varmistettu käyttämällä kattavia CIS-viitekehyksiä, jotka tarjoavat vankat periaatteet ja menetelmät kriittisen infrastruktuurin turvallisuuden varmistamiseksi. CIS-viitekehysten soveltaminen kovennuksissa mahdollistaa monipuolisen suojausstrategian, joka kattaa laajan kirjon potentiaalisia uhkia ja haavoittuvuuksia. Tämä lähestymistapa takaa, että kaikki turvallisuusnäkökohdat otetaan huomioon ja että ratkaisut ovat linjassa alan parhaiden käytäntöjen kanssa, mikä lisää merkittävästi tulosten luotettavuutta ja tehokkuutta.

5.1 Keskeisten tulosten tarkastelu suhteessa alkuosan teoreettiseen viitekehykseen

Käytännön tulokset ovat osoittaneet alussa esitellyn teoreettisen viitekehyksen mukaisesti, että kovennukset parantavat merkittävästi järjestelmän turvallisuutta vaikuttamatta negatiivisesti sen käytettävyyteen. Tämän havainnon vahvistamiseksi on suoritettu useita testauksia, joiden tarkoituksena on ollut arvioida kovennusten vaikutuksia järjestelmään. Testausprosessi on sisältänyt sekä ennen kovennuksia että niiden jälkeen tehtyjä turvallisuusskannauksia, joilla on pyritty tunnistamaan mahdolliset haavoittuvuudet ja arvioimaan kovennusten tehokkuutta.

Turvallisuusskannaukset on toteutettu käyttäen alan standardien mukaisia työkaluja (CIS viitekehykset), jotka tarjoavat kattavan yleiskuvan järjestelmän turvallisuustilanteesta. Ennen kovennuksia suoritetussa skannauksessa tunnistettiin useita haavoittuvuuksia, jotka dokumentoitiin tarkasti. Kovennustoimenpiteiden jälkeen suoritettu uusi skannaus osoitti, että suurin osa aiemmin tunnistetuista haavoittuvuuksista oli korjattu, mikä vahvisti kovennusprosessin onnistumisen.

Testaukset ja skannaukset on suoritettu systemaattisesti minun toimestani, käyttäen hyväksi sekä teoreettista osaamista että käytännön tietoturvatyökaluja. Tämä lähestymistapa on mahdollistanut objektiivisen arvioinnin kovennusten vaikutuksista järjestelmän turvallisuuteen. Järjestelmän

käyttäjien tekemät havainnot ja ilmoitukset mahdollisista ongelmista ovat olleet arvokkaita lisätessä ymmärrystä kovennusten vaikutuksista käytännössä.

5.2 Käytettyjen menetelmien arviointi

Menetelmä tuotti tehokkaita tuloksia lyhyelle aikavälille. Projektin edetessä selvisi, että itsetehdyn työkalun ylläpito on haastavaa, kun otetaan huomioon jatkuvasti päivittyvät järjestelmä- ja viitekehysversiot. Vaihtoehtoinen ratkaisu olisi hankkia CIS Secure Suite -jäsenyys, joka toisi käyttöön valmiiksi laaditut skriptit kovennusten toteuttamiseen. Tämä ei kuitenkaan ole suoraviivainen ratkaisu, sillä on tärkeää ymmärtää järjestelmän käyttötarkoitus ja suorittaa vain ne kovennukset, jotka sopivat kyseiseen käyttöön.

5.3 Tulevaisuuden näkymät ja kehittämisehdotukset

Opinnäytetyössä kovennettu järjestelmä on toimeksiantajan teknisten asiantuntijoiden käytössä jatkuvasti, kun toimeksiantajan omiin tai asiakkaan järjestelmiin toimeksiantajan toimesta kohdistetaan teknistä tietoturvatestausta. Tulevaisuudessa kovennettua Debian järjestelmää voi ja tulee kehittää muuttuvien järjestelmä- ja viitekehysversioiden mukaan. Aktiivinen seuranta on tärkeää, jotta mahdolliset uudet haavoittuvuudet saadaan korjattua.

Lähteet

About us. N.d. Center for Internet Security. Viitattu 7.10.2023. https://www.cisecurity.org/about-us

CIS Build Kits FAQ. N.d. Center for Internet Security. Viitattu 22.3.2024. https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content/build-kits-faq

CIS Debian Linux 11 Benchmark. 2022. CIS viitekehys PDF-dokumentti. Viitattu 20.11.2023. https://www.cisecurity.org/cis-benchmarks

Compliance and Vulnerability Scanning with OpenSCAP. N.d. Red Hat Customer Portal. Viitattu 22.3.2024. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-compliance_and_vulnerability_scanning

Gillis, A. 2024. NIST Cybersecurity Framework. Viitattu 22.3.2024. https://advisera.com/27001academy/what-is-iso-27001/

Kali Linux Tutorial, N.d. Javatpoint. Viitattu 7.9.2023. https://www.javatpoint.com/kali-linux

Kili, A. 2022. 7 Useful Linux Security Features and Tools for Beginners. Viitattu 7.9.2023. https://www.tecmint.com/linux-security-features-and-tools/

King, B. 2020. 12 Reasons Why You Should Choose Debian Linux. Viitattu 12.10.2023. https://www.makeuseof.com/tag/reasons-choose-debian-linux/

Kosutic, D. N.d. What does ISO 27001 mean? Viitattu 22.3.2024. https://advisera.com/27001academy/what-is-iso-27001/

Linux, 2023. Britannica. Viitattu 7.9.2023. https://www.britannica.com/technology/Linux

Linux Distributions. N.d. Javatpoint. Viitattu 7.9.2023. https://www.javatpoint.com/linux-distributions

Linux Statistics. 2023. Blogiteksti. Viitattu 12.10.2023. https://truelist.co/blog/linux-statistics/

Lynis, an introduction. N.d. CISOFY. Viitattu 22.3.2024. https://cisofy.com/lynis/

Negus, C. 2015. Linux Bible. The comprehensive, tutorial resource. Indianapolis: John Wiley & Sons, Inc. Viitattu 7.9.2023.

Stavrakas, H. 2022. Operating System Hardening: Benefits, Importance, & Other Considerations. Viitattu 8.9.2023. https://linfordco.com/blog/operating-system-hardening/

Terrell, H. 2021. Red Hat. Viitattu 28.12.2023. https://www.techtarget.com/searchdatacenter/definition/Red-Hat

Vähämaa, J. 2024. Debian 11 Hardening. Lähdekoodirepositorio. Viitattu 11.3.2024. https://github.com/Squidac/debian11_hardening

What are CIS Benchmarks. N.d. AWS. Viitattu 29.12.2023. https://aws.amazon.com/what-is/cis-benchmarks/

What is open source. 2019. RedHat. Viitattu 8.9.2023. https://www.redhat.com/en/topics/open-source/what-is-open-source

What is Slackware Linux. N.d. Huihoo. Viitattu 28.12.2023. https://book.huihoo.com/slackware-linux-basics/html/introduction.html

What is System Hardening. N.d. Intel. Viitattu 5.7.2023. https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/system-hardening.html

What is Systems Hardening. N.d. Beyondtrust. Viitattu 8.9.2023. https://www.beyondtrust.com/resources/glossary/systems-hardening

What is the Linux kernel. 2019. Red Hat. Viitattu 7.9.2023. https://www.redhat.com/en/topics/linux/what-is-the-linux-kernel

Liitteet

Liite 1. Järjestelmän CIS-kovennukset

Nro	Suositus	T	K	S	Kommentti
1	**Alustava asennus**				
1.1	Tiedostojärjestelmän konfigurointi				
1.1.1	Poista käytöstä tarpeettomat tiedostojärjestelmät				
1.1.1.1	Varmista, että cramfs-tiedostojärjestelmien liittäminen on poistettu käytöstä	2	K	A	Cramfs on tiedostojärjestelmä, joka on suunniteltu pienille järjestelmille. Cramfs-kuvaketta voidaan käyttää purkamatta sitä ensin. Vaikka tarpeettomien tiedostojärjestelmätyyppien poistaminen voi vähentää järjestelmän mahdollisia hyökkäyspintoja, on tärkeää arvioida, tarvitaanko kyseistä tiedostojärjestelmätyyppiä. Jos sitä ei tarvita, se tulisi poistaa käytöstä.
1.1.1.2	Varmista, että squashfs-tiedostojärjestelmien liittäminen on poistettu käytöstä	2	E	A	Squashfs on tiedostojärjestelmä, joka on suunniteltu pienille järjestelmille ja sen kuvaketta voidaan käyttää ilman purkamista. Poistamalla tukemattomia tiedostojärjestelmiä käytöstä voidaan vähentää järjestelmän mahdollisia hyökkäyspintoja. Kuitenkin, koska Snap-paketit hyödyntävät squashfs:tä pakattuna tiedostojärjestelmänä, squashfs:n poistaminen käytöstä estää Snap-pakettien käytön. Snap-ohjelmistopaketit ovat itsenäisiä ja toimivat useissa Linux-distribuutioissa ja ne eroavat perinteisistä Linux-pakettienhallintatavoista ja mahdollistavat ohjelmistojen nopeamman jakelun kehittäjiltä loppukäyttäjille ilman ulkoisen sovelluskaupan riippuvuutta.
1.1.1.3	Varmista, että udf-tiedostojärjestelmien liittäminen on poistettu käytöstä	2	E	A	UDF-tiedostojärjestelmätyyppi on yleinen levyformaatti, joka on käytössä ISO/IEC 13346:n ja ECMA-167:n mukaisesti. Se on avoimen lähdekoodin tiedostojärjestelmä, joka on suunniteltu datan tallennukseen monenlaisille medioille ja on tarpeellinen DVD:iden sekä uusimpien optisten levyformaattien kirjoittamiseen. Vaikka tarpeettomien tiedostojärjestelmätyyppien poistaminen käytöstä voi vähentää järjestelmän hyökkäyspintaa, on huomioitava, että Microsoft Azure vaatii udf:n käyttöä. Näin ollen udf:tä ei tulisi poistaa käytöstä järjestelmissä, jotka toimivat Microsoft Azure -ympäristössä.
1.1.2	Konfiguroi /tmp				
1.1.2.1	Varmista, että /tmp-hakemistolle on erillinen osio	1	K	A	"/tmp"-hakemisto on maailmanlaajuisesti kirjoitettava hakemisto, jota kaikki käyttäjät ja jotkut sovellukset käyttävät väliaikaiseen tallennukseen. Erottamalla "/tmp" omaksi tiedostojärjestelmäkseen, järjestelmänvalvoja voi asettaa lisäkiinnitysoptioita, kuten "noexec", tehden "/tmp":stä hyödyttömän hyökkääjälle suoritettavan koodin asentamiseksi. Se myös estäisi hyökkääjää luomasta kovaa linkkiä järjestelmän "setuid"-ohjelmaan ja odottamasta sen päivitystä. Erillinen osio "/tmp":lle suojaa myös resurssien liikakäytöltä, koska "/tmp" on tarkoitettu olevan maailmanlaajuisesti kirjoitettava. Jos "/tmp" tila loppuu, se on ongelma riippumatta sen alla olevasta tiedostojärjestelmästä. RAM-pohjainen "/tmp" (kuten tmpfs) on yleensä paljon pienempi, mikä voi johtaa sovelluksiin täyttämään tiedostojärjestelmän nopeammin. Toisaalta levyyn perustuva erillinen osio on hitaampi kuin RAM-pohjainen tmpfs. "/tmp":n kokoa, joka käyttää tmpfs:ää, voidaan muuttaa määrittämällä size={size} vastaavassa merkinnässä /etc/fstab:ssa.

Nro	Suositus	T	K	S	Kommentti
1.1.2.2	Varmista, että /tmp-osiossa on asetettu nodev-optio	1	K	A	"Nodev"-kiinnitysoptio määrittää, että tiedostojärjestelmä ei voi sisältää erityislaitteita. Koska "/tmp"-tiedostojärjestelmä ei ole tarkoitettu tukemaan laitteita, tämän option tulisi olla asetettuna varmistaakseen, että käyttäjät eivät voi luoda lohko- tai merkkierityislaitteita "/tmp"-hakemistoon.
1.1.2.3	Varmista, että /tmp-osiossa on asetettu noexec-optio	1	K	A	"Noexec"-kiinnitysoptio määrittää, että tiedostojärjestelmä ei voi sisältää suoritettavia binäärejä. Koska "/tmp"-tiedostojärjestelmä on tarkoitettu ainoastaan väliaikaista tiedostojen säilytystä varten, tämä optio tulisi asettaa varmistaakseen, että käyttäjät eivät voi suorittaa binäärejä "/tmp"-hakemistosta.
1.1.2.4	Varmista, että /tmp-osiossa on asetettu nosuid-optio	1	K	A	"Nosuid"-kiinnitysoptio määrittää, että tiedostojärjestelmä ei voi sisältää setuid-tiedostoja. Koska "/tmp"-tiedostojärjestelmä on tarkoitettu ainoastaan väliaikaista tiedostojen säilytystä varten, tämä optio tulisi asettaa varmistaakseen, että käyttäjät eivät voi luoda setuid-tiedostoja "/tmp"-hakemistoon.
1.1.3	Konfiguroi /var				
1.1.3.1	Varmista, että /var-hakemistolle on erillinen osio	2	K	A	"/var"-hakemisto on tarkoitettu järjestelmäpalveluiden dynaamiselle datalle. Erillisen osion käyttö "/var"-hakemistolle ehkäisee resurssien liikakäyttöä, tarjoaa tarkemman hallinnan osion asetuksiin ja suojaa potentiaalisilta hyväksikäyttöyrityksiltä. Pilvipohjaisissa ympäristöissä tiedostojärjestelmien koon muuttaminen on yleistä, ja erillisten osioiden käyttö voi vaikuttaa näihin toimintoihin ja tuoda lisätietoturvaan liittyviä näkökohtia.
1.1.3.2	Varmista, että /var-osiossa on asetettu nodev-optio	1	K	A	"Nodev"-kiinnitysoptio estää erityislaitteiden luomisen tiedostojärjestelmässä. Koska "/var"-tiedostojärjestelmä ei ole tarkoitettu tukemaan laitteita, tämän option asettaminen takaa, etteivät käyttäjät voi luoda lohko- tai merkkierityislaitteita "/var"-hakemistoon.
1.1.3.3	Varmista, että /var-osiossa on asetettu nosuid-optio	1	K	A	"Nosuid"-kiinnitysoptio estää setuid-tiedostojen luomisen tiedostojärjestelmässä. Koska "/var"-tiedostojärjestelmä on tarkoitettu pääasiassa muuttuville tiedostoille, kuten lokeille, tämän option asettaminen takaa, etteivät käyttäjät voi luoda setuid-tiedostoja "/var"-hakemistoon.
1.1.4	Konfiguroi /var/tmp				
1.1.4.1	Varmista, että /var/tmp-hakemistolle on erillinen osio	2	E	A	"/var/tmp"-hakemisto on maailmanlaajuisesti kirjoitettavissa oleva hakemisto, jota kaikki käyttäjät ja jotkut sovellukset käyttävät väliaikaiseen tallennukseen, ja sen tulee säilyä käynnistysten välillä. Sen asettaminen erilliselle osiolle suojaa järjestelmää resurssien uupumiselta, koska se voi täyttää koko levyn. Lisäksi erillinen osio mahdollistaa hienosyisen hallinnan kiinnitysoptioille, kuten noexec/nosuid/nodev, rajoittaen hyökkääjän kykyä luoda järjestelmään haavoittuvuuksia. Kuitenkin pilvipalvelimissa tiedostojärjestelmien koon muuttaminen on yleistä, ja erilliset osiot voivat hankaloittaa tätä toimintaa ja tuoda omia turvallisuusharkintoja.
1.1.4.2	Varmista, että /var/tmp-osioon on asetettu noexec-optio	1	E	A	Noexec-kiinnitysoptio määrittelee, että tiedostojärjestelmä ei voi sisältää suoritettavia binäärejä. Koska "/var/tmp"-tiedostojärjestelmä on tarkoitettu vain väliaikaiselle tiedostojen tallennukselle, tämä optio tulisi asettaa varmistaakseen, etteivät käyttäjät voi suorittaa suoritettavia binäärejä "/var/tmp"-hakemistosta.

Nro	Suositus	T	K	S	Kommentti
1.1.4.3	Varmista, että /var/tmp-osioon on asetettu nosuid-optio	1	E	A	Nosuid-kiinnitysoptio määrittelee, että tiedostojärjestelmä ei voi sisältää setuid-tiedostoja. Koska "/var/tmp"-tiedostojärjestelmä on tarkoitettu vain väliaikaiselle tiedostojen tallennukselle, tämä optio tulisi asettaa varmistaakseen, etteivät käyttäjät voi luoda setuid-tiedostoja "/var/tmp"-hakemistossa.
1.1.4.4	Varmista, että /var/tmp-osioon on asetettu nodev-optio	1	E	A	Nodev-kiinnitysoptio määrittelee, että tiedostojärjestelmä ei voi sisältää erityislaitteita. Koska "/var/tmp"-tiedostojärjestelmä ei ole tarkoitettu laitteiden tukemiseen, tämä optio tulisi asettaa varmistaakseen, etteivät käyttäjät voi luoda erityisiä lohko- tai merkkilaitteita "/var/tmp"-hakemistossa.
1.1.5	Konfiguroi /var/log				
1.1.5.1	Varmista, että /var/log-hakemistolle on olemassa erillinen osio	2	E	A	"/var/log"-hakemistoa käytetään järjestelmäpalveluiden lokitietojen tallentamiseen. Sen sijoittaminen omalle osiolleen suojaa järjestelmää resurssien ehtymiseltä, erityisesti kun otetaan huomioon lokitiedostojen mahdollinen nopea kasvu. Oma osio mahdollistaa myös tarkemman hallinnan kiinnitysoptioilla, rajoittaen potentiaalisia hyökkäyksiä. Pilvipohjaisissa palvelimissa osioiden koon muuttaminen on yleistä, ja erilliset osiot saattavat tuoda haasteita tai vaatia erityistyökaluja, jotka voivat tuoda mukanaan omia turvallisuusriskejä.
1.1.5.2	Varmista, että /var/log-osioon on asetettu nodev-optio	1	E	A	Nodev-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää erikoislaitteita. Koska /var/log on tarkoitettu ainoastaan lokitiedostoille, tämän asetuksen käyttöönotto estää käyttäjiä luomasta lohko- tai merkki-erikoislaitteita /var/log-kansiosta.
1.1.5.3	Varmista, että /var/log-osioon on asetettu noexec-optio	1	E	A	Noexec-kiinnitysoptio estää suoritettavien binääritiedostojen käytön tiedostojärjestelmässä. Koska /var/log on tarkoitettu ainoastaan lokitiedostoille, tämän asetuksen käyttöönotto estää käyttäjiä suorittamasta binääritiedostoja /var/log-kansiosta.
1.1.5.4	Varmista, että /var/log-osioon on asetettu nosuid-optio	1	E	A	Nosuid-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää setuid-tiedostoja. Koska /var/log on tarkoitettu ainoastaan lokitiedostoille, tämän asetuksen käyttöönotto estää käyttäjiä luomasta setuid-tiedostoja /var/log-kansiosta.
1.1.6	Konfiguroi /var/log/audit				
1.1.6.1	Varmista, että /var/log/audit-hakemistolle on erillinen osio	2	E	A	/var/log/audit-kansiossa auditointidaemoni, auditd, tallentaa lokitietonsa. On suositeltavaa määrittää /var/log/audit omaksi tiedostojärjestelmäkseen, jotta estetään resurssien uupuminen, kun audit.log-tiedosto kasvaa suureksi. Tämä ehkäisee myös järjestelmän häiriöitä. Lisäksi erillinen osio mahdollistaa tarkemman hallinnan kiinnitysoptioilla, kuten noexec, nosuid ja nodev, parantaen järjestelmän turvallisuutta. Erityistä huomiota on kiinnitettävä auditointilokien turvallisuuden ja eheyden varmistamiseen. Vaikka erillisten osioiden käyttö voi tehdä tiedostojärjestelmän koon muuttamisesta haastavaa pilvipalvelimissa, se on perusteltua tietoturvasyistä.
1.1.6.2	Varmista, että /var/log/audit-osioon on asetettu noexec-optio	1	E	A	/var/log/audit-tiedostojärjestelmän tarkoitus on säilyttää ainoastaan auditointilokeja. noexec-kiinnitysoption käyttö tällä osiolla varmistaa, että käyttäjät eivät voi suorittaa suoritettavia binääritiedostoja /var/log/audit-kansiosta, mikä lisää järjestelmän turvallisuutta.

Nro	Suositus	T	K	S	Kommentti
1.1.6.3	Varmista, että /var/log/audit-osioon on asetettu nodev-optio	1	E	A	/var/log/audit-tiedostojärjestelmä ei ole tarkoitettu erityislaitteiden tukemiseen. nodev-kiinnitysoption käyttö tällä osiolla varmistaa, että käyttäjät eivät voi luoda lohko- tai merkkilaitteita /var/log/audit-kansioon, tehostaen järjestelmän suojausta haitallisilta toiminnoilta.
1.1.6.4	Varmista, että /var/log/audit-osioon on asetettu nosuid-optio	1	E	A	/var/log/audit-tiedostojärjestelmä on tarkoitettu vain muuttuville tiedostoille, kuten lokeille. nosuid-kiinnitysoption käyttö tällä osiolla varmistaa, että käyttäjät eivät voi luoda setuid-tiedostoja /var/log/audit-kansioon, lisäten järjestelmän turvallisuutta ja suojaten sitä mahdollisilta uhilta.
1.1.7	Konfiguroi /home				
1.1.7.1	Varmista, että /home-hakemistolle on erillinen osio	2	K	A	/home-kansio tukee paikallisten käyttäjien levytallennustarpeita. Sen sijoittaminen omaan osioonsa suojaa järjestelmää resurssien loppumiselta ja antaa järjestelmänvalvojille mahdollisuuden säätää kiinnitysoptioita parantaen turvallisuutta. Erillinen osio voi myös helpottaa käyttäjätietojen suojaamista. Kuitenkin pilvipalvelimissa tiedostojärjestelmien muuttaminen voi olla yleistä, ja erilliset osiot voivat tehdä tästä haasteellista tai vaatia lisätyökaluja, jotka tuovat omat turvallisuusnäkökohdat.
1.1.7.2	Varmista, että /home-osioon on asetettu nodev-optio	1	K	A	Nodev-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää erityisiä laitteita. Koska /home-tiedostojärjestelmä ei ole tarkoitettu laitteiden tukemiseen, tämän option tulisi olla asetettuna, jotta käyttäjät eivät voi luoda erityisiä lohko- tai merkkilaitteita /home-kansiossa.
1.1.7.3	Varmista, että /home-osioon on asetettu nosuid-optio	1	K	A	Nosuid-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää setuid-tiedostoja. Koska /home-tiedostojärjestelmä on tarkoitettu ainoastaan käyttäjien tiedostojen säilytykseen, tämän option tulisi olla asetettuna varmistaakseen, että käyttäjät eivät voi luoda setuid-tiedostoja /home-kansiossa.
1.1.8	Konfiguroi /dev/shm				
1.1.8.1	Varmista, että /dev/shm-osioon on asetettu nodev-optio	1	K	A	Nodev-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää erikoislaitteita. Koska /dev/shm-tiedostojärjestelmä ei ole tarkoitettu laitteiden tukemiseen, tämän option tulisi olla asetettuna varmistaakseen, että käyttäjät eivät voi yrittää luoda erikoislaitteita /dev/shm-osioihin.
1.1.8.2	Varmista, että /dev/shm-osioon on asetettu noexec-optio	1	K	A	Noexec-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää suoritettavia binäärejä. Tämän option asettaminen estää käyttäjiä suorittamasta ohjelmia jaettusta muistista. Tämä vähentää riskiä, että käyttäjät toisivat potentiaalisesti haitallista ohjelmistoa järjestelmään.
1.1.8.3	Varmista, että /dev/shm-osioon on asetettu nosuid-optio	1	K	A	Nosuid-kiinnitysoptio määrittää, ettei tiedostojärjestelmä voi sisältää setuid-tiedostoja. Tämän option asettaminen estää käyttäjiä tuomasta järjestelmään etuoikeutettuja ohjelmia ja antamasta ei-root-käyttäjien suorittaa niitä. Tämä lisää järjestelmän turvallisuutta rajoittamalla mahdollisia pääsytapauksia.
1.1.9	Poista automaattinen liittäminen käytöstä	2	K	A	Autofs mahdollistaa laitteiden, kuten CD/DVD-levyjen ja USB-asemien, automaattisen liittämisen. Kun automaattinen liittäminen on käytössä, kenellä tahansa fyysisellä pääsyllä voi liittää USB-aseman tai levyn ja saada sen sisällön käyttöönsä, vaikka heillä ei olisi oikeuksia liittää sitä itse. Kuitenkin kannettavien kovalevyjen käyttö on yleistä työasemien käyttäjille. Jos organisaatio sallii kannettavien tallennusvälineiden käytön ja fyysiset pääsynvalvonnat työasemiin katsotaan riittäviksi, automaattisen liittämisen poistamisesta on vähän lisäarvoa.

Nro	Suositus	T	K	S	Kommentti
1.1.10	Poista USB-tallennus käytöstä	2	E	A	USB-tallennus mahdollistaa tiedostojen siirtämisen ja tallentamisen varmistaen tiedostojen pysyvyyden ja saatavuuden riippumatta verkkoyhteyden tilasta. Sen suosio ja käyttökelpoisuus ovat johtaneet USB-pohjaisen haittaohjelman yleistymiseen, mikä on yksinkertainen ja yleinen tapa soluttautua verkkoon ja ensimmäinen askel pysyvän uhan perustamisessa verkkoympäristöön. USB-pääsyn rajoittaminen järjestelmässä pienentää laitteen fyysistä hyökkäyspintaa ja vähentää mahdollisia vektoreita haittaohjelman tuomiseksi järjestelmään.
1.2	Ohjelmistopäivitysten konfigurointi				
1.2.1	Varmista, että paketinhallintajärjestelmien repositoriot on määritetty	1	K	M	Järjestelmien tulee olla määritettyjä paketinhallintajärjestelmän repositorioiden kanssa varmistaakseen, että ne saavat uusimmat korjaukset ja päivitykset. Jos järjestelmän ohjelmistovarastot ovat väärin määriteltyjä, tärkeitä korjauksia saatetaan jättää huomiotta tai rogue repositorio saattaa tuoda mukanaan kompromisoidun ohjelmiston.
1.2.2	Varmista, että GPG-avaimet on määritetty	1	K	M	Useimmat pakettienhallintaohjelmat toteuttavat GPG-avaimen allekirjoituksen varmistaakseen paketin eheyden asennuksen aikana. On tärkeää varmistaa, että päivitykset saadaan kelvollisesta lähteestä, jotta voidaan suojautua huijaukselta, joka voisi johtaa haittaohjelman tahattomaan asentamiseen järjestelmään.
1.3	Tiedostojärjestelmän eheyden tarkistus				
1.3.1	Varmista, että AIDE on asennettu	1	K	A	AIDE ottaa tiedostojärjestelmän tilasta otoksen, johon sisältyy muokkausaikoja, oikeuksia ja tiedostojen hajautusarvoja. Näitä voidaan sitten verrata tiedostojärjestelmän nykyiseen tilaan havaitakseen muutoksia järjestelmässä. Tiedostojärjestelmän tilaa seuraamalla voidaan havaita kompromisoituneita tiedostoja ja näin estää tai rajoittaa tahattomien tai ilkeämielisten virheellisten määritysten tai muutettujen binääritiedostojen altistumista.
1.3.2	Varmista, että tiedostojärjestelmän eheys tarkistetaan säännöllisesti	1	K	A	Tiedostojärjestelmän eheyden säännöllinen tarkistaminen on tarpeen havaitakseen muutokset tiedostojärjestelmässä. Säännöllinen tiedostojen tarkistus mahdollistaa järjestelmänvalvojan määrittää säännöllisesti, onko kriittisiä tiedostoja muutettu ilman lupaa.
1.4	Turvallisen käynnistyksen asetukset				
1.4.1	Varmista, että käynnistyslataimen salasana on asetettu	1	E	A	Asettamalla käynnistyslataimen salasanan käyttöön varmistetaan, että käyttäjien on syötettävä salasana ennen komentorivin käynnistysparametrien asettamista tai käynnistysosiota muutettaessa. Tämä lisää turvallisuutta estämällä luvattomat käyttäjät heikentämästä järjestelmän turva-asetuksia, kuten AppArmorin pois kytkemistä käynnistyksen yhteydessä. Salasanansuojaus rajoittaa myös GRUB 2 -valikon muokkaamista ja komentorivin käyttöä vain määritetylle superkäyttäjälle. Jos käynnistyslataimeen liittyviä ongelmia ilmenee salasanasuojausasetusten vuoksi, ne voidaan ratkaista muokkaamalla konfiguraatiotiedostoja esimerkiksi LiveCD:n avulla. On myös mahdollista sallia järjestelmän käynnistyminen ilman salasanan syöttämistä tietyissä tapauksissa lisäämällä "--unrestricted" -asetus valikkokohtiin.

Nro	Suositus	T	K	S	Kommentti
1.4.2	Varmista, että käynnistyslataimen konfiguraatiotiedoston oikeudet on määritetty	1	E	A	GRUB-konfiguraatiotiedosto sisältää tietoa käynnistyksen asetuksista sekä salasanoista, joilla voidaan avata käynnistysasetuksia. On tärkeää rajoittaa tämän tiedoston oikeudet vain juurikäyttäjälle. Asettamalla oikeudet vain juurikäyttäjän luku- ja kirjoituskäyttöön estetään muiden kuin juurikäyttäjien pääsy näkemään tai muuttamaan käynnistysparametreja. Käyttäjät, jotka eivät ole juurikäyttäjiä ja jotka voivat lukea käynnistysparametreja, saattavat tunnistaa turvallisuusheikkouksia käynnistyksessä ja mahdollisesti hyödyntää niitä.
1.4.3	Varmista, että single user mode -tilassa vaaditaan tunnistautuminen	1	K	A	Single user mode -tilaa käytetään järjestelmän palautukseen, kun järjestelmä havaitsee ongelman käynnistyksen aikana tai kun käyttäjä manuaalisesti valitsee sen käynnistyslataimesta. Tunnistautumisen vaatiminen yhden käyttäjän tilassa estää luvattoman käyttäjän uudelleenkäynnistämästä järjestelmää tähän tilaan ja saamasta juurikäyttöoikeuksia ilman asianmukaisia tunnistetietoja.
1.5	Lisätoimenpiteet				
1.5.1	Varmista, että osoiteavaruuden asettelun satunnaistaminen (ASLR) on käytössä	1	K	A	Osoiteavaruuden asettelun satunnaistaminen (ASLR) on hyväksikäytön estämistekniikka, joka järjestää satunnaisesti prosessin keskeisten datavyöhykkeiden osoiteavaruuden. Osoiteavaruuden satunnaistaminen tekee virtuaalimuistivyöhykkeiden paikkojen ennustamisesta vaikeaa, mikä puolestaan tekee muistisivujen hyväksikäyttöyritykset hankaliksi, koska muistin sijoittelu muuttuu jatkuvasti.
1.5.2	Varmista, että prelink ei ole asennettuna	1	K	A	prelink on ohjelma, joka muokkaa ELF-yhteiskirjastoja ja ELF dynaamisesti linkitettyjä binäärejä siten, että dynaamisen linkittimen suorittamien uudelleensijoitusten aika käynnistyksen yhteydessä lyhenee merkittävästi. Prelink-toiminto voi häiritä AIDE:n toimintaa, koska se muuttaa binääritiedostoja. Lisäksi, jos haitallinen käyttäjä pystyy kompromisoimaan yleisen kirjaston kuten libc:n, prelinking voi lisätä järjestelmän haavoittuvuutta.
1.5.3	Varmista, että automaattinen virheraportointi ei ole käytössä	1	K	A	Apport-virheraportointipalvelu luo automaattisesti kaatumisraportteja virheiden jäljittämiseksi. Tämä palvelu voi kerätä potentiaalisesti arkaluontoisia tietoja, kuten ydinten varmuuskopiot, pinokutsut ja lokitiedostot. Nämä tiedot saattavat sisältää salasanoja, luottokorttinumeroita, sarjanumeroita ja muita yksityisiä tietoja.
1.5.4	Varmista, että ydindumppien käyttö on rajoitettu	1	K	A	Ydindumppi (Core dump) on suoritettavan ohjelman muisti. Sitä käytetään yleensä määrittämään, miksi ohjelma keskeytettiin. Sitä voidaan myös käyttää keräämään luottamuksellista tietoa ydintiedostosta. Järjestelmä tarjoaa mahdollisuuden asettaa pehmeän rajan ydindumpeille, mutta käyttäjä voi ohittaa tämän. Asettamalla kovan rajan ydindumpeille estetään käyttäjiä ohittamasta pehmeää muuttujaa. Jos ydindumppien käyttö on tarpeen, harkitse rajojen asettamista käyttäjäryhmille (katso limits.conf(5)). Lisäksi fs.suid_dumpable-muuttujan asettaminen arvoon 0 estää setuid-ohjelmat tekemästä ydindumppia.
1.6	Pakollinen pääsynvalvonta				
1.6.1	Konfiguroi AppArmor				
1.6.1.1	Varmista, että AppArmor on asennettu	1	E	A	AppArmor tarjoaa pakolliset käyttöoikeudet (Mandatory Access Controls) järjestelmissä. Jos AppArmoria tai vastaavaa järjestelmää ei ole asennettu, vain oletuksena oleva harkinnanvarainen käyttöoikeusjärjestelmä (Discretionary Access Control) on käytettävissä.

Nro	Suositus	T	K	S	Kommentti
1.6.1.2	Varmista, että AppArmor on käytössä käynnistyslataajan asetuksissa	1	E	A	AppArmor tulee olla konfiguroitu siten, että se on käytössä järjestelmän käynnistyessä, ja varmistettu, ettei sitä ole ohitettu käynnistyslataajan käynnistysparametreissä. Huomio: Tämä suositus on suunniteltu grub-käynnistyslataajan näkökulmasta. Jos käytössä on LILO tai jokin muu käynnistyslataaja, toteutetaan vastaavat asetukset. AppArmorin on oltava käynnistettynä käynnistyslataajan asetuksissa, jotta varmistetaan sen tarjoamien kontrollien olevan voimassa eikä niitä ohiteta.
1.6.1.3	Varmista, että kaikki AppArmor-profiilit ovat joko "enforce" tai "complain" -tilassa	1	E	A	AppArmor-profiilit määrittävät, mihin resursseihin sovelluksilla on pääsy. Turvallisuusasetusvaatimukset vaihtelevat sivustojen välillä. Jotkin sivustot saattavat vaatia oletusasetuksia tiukempaa käytäntöä, mikä on täysin hyväksyttävää. Tämän kohdan tarkoituksena on varmistaa, että järjestelmässä olemassa olevat käytännöt ovat aktivoituna ja niitä noudatetaan tiukasti.
1.6.1.4	Varmista, että kaikki AppArmor-profiilit ovat "enforcing"-tilassa	2	E	A	AppArmor-profiilit määrittävät, mihin resursseihin sovelluksilla on pääsy. Turvallisuusasetusvaatimukset vaihtelevat sivustojen välillä. Jotkin sivustot saattavat vaatia oletusasetuksia tiukempaa käytäntöä, mikä on täysin hyväksyttävää. Tämän kohdan tarkoituksena on varmistaa, että järjestelmässä olemassa olevat käytännöt ovat aktivoituna ja niitä noudatetaan tiukasti.
1.7	Komentorivin varoitusviestit				
1.7.1	Varmista, että päivän viesti on asianmukaisesti määritetty	1	K	A	Päivän viesti, joka näkyy tiedostossa /etc/motd, näytetään käyttäjille kirjautumisen jälkeen. Unix-pohjaisissa järjestelmissä on tyypillisesti näytetty tietoa käyttöjärjestelmän versiosta ja päivitystasosta kirjautuessa. Tämä tieto voi olla hyödyllistä kehittäjille, jotka kehittävät ohjelmistoja tietylle alustalle. Varoitusviestit kertovat kirjautumista yrittäville käyttäjille heidän laillisesta asemastaan järjestelmään nähden ja niiden tulee sisältää järjestelmän omistavan organisaation nimi sekä voimassa olevat valvontapolitiikat. Käyttöjärjestelmän ja päivitystason tiedon näyttäminen kirjautumistiedoissa voi kuitenkin tarjota hyökkääjille yksityiskohtaista tietoa järjestelmästä. Valtuutetut käyttäjät voivat saada tämän tiedon helposti komennolla "uname -a" kirjautumisen jälkeen.
1.7.2	Varmista, että paikallisen kirjautumisen varoitusviesti on asianmukaisesti määritetty	1	K	A	Tiedoston /etc/issue sisältö näytetään käyttäjille ennen kirjautumista paikallisissa terminaaleissa. Unix-pohjaisissa järjestelmissä on tyypillisesti näytetty tietoa käyttöjärjestelmän versiosta ja päivitystasosta kirjautuessa. Tämä tieto voi olla hyödyllistä kehittäjille, jotka kehittävät ohjelmistoja tietylle alustalle. Varoitusviestit kertovat kirjautumista yrittäville käyttäjille heidän laillisesta asemastaan järjestelmään nähden ja niiden tulee sisältää järjestelmän omistavan organisaation nimi sekä voimassa olevat valvontapolitiikat. Käyttöjärjestelmän ja päivitystason tiedon näyttäminen kirjautumistiedoissa voi kuitenkin tarjota hyökkääjille yksityiskohtaista tietoa järjestelmästä. Valtuutetut käyttäjät voivat saada tämän tiedon helposti komennolla "uname -a" kirjautumisen jälkeen.

Nro	Suositus	T	K	S	Kommentti
1.7.3	Varmista, että etäkirjautumisen varoitusviesti on asianmukaisesti määritetty	1	K	A	Tiedoston /etc/issue.net sisältö näytetään käyttäjille ennen kirjautumista etäyhteyksissä määritetyistä palveluista. Unix-pohjaisissa järjestelmissä on tyypillisesti näytetty tietoa käyttöjärjestelmän versiosta ja päivitystasosta kirjautuessa. Tämä tieto voi olla hyödyllistä kehittäjille, jotka kehittävät ohjelmistoja tietylle alustalle. Varoitusviestit kertovat kirjautumista yrittäville käyttäjille heidän laillisesta asemastaan järjestelmään nähden ja niiden tulee sisältää järjestelmän omistavan organisaation nimi sekä voimassa olevat valvontapolitiikat. Käyttöjärjestelmän ja päivitystason tiedon näyttäminen kirjautumistiedoissa voi kuitenkin tarjota hyökkääjille yksityiskohtaista tietoa järjestelmästä. Valtuutetut käyttäjät voivat saada tämän tiedon helposti komennolla "uname -a" kirjautumisen jälkeen.
1.7.4	Varmista, että /etc/motd -tiedoston käyttöoikeudet on määritetty oikein	1	K	A	Tiedoston /etc/motd sisältö näytetään käyttäjille kirjautumisen jälkeen ja toimii päivän viestinä autentikoiduille käyttäjille. Jos /etc/motd-tiedostolla ei ole oikeaa omistajuutta, luvattomat käyttäjät saattavat muokata sitä sisältämään virheellistä tai harhaanjohtavaa tietoa.
1.7.5	Varmista, että /etc/issue -tiedoston käyttöoikeudet on määritetty oikein	1	K	A	Tiedoston /etc/issue sisältö näytetään käyttäjille ennen kirjautumista paikallisissa terminaaleissa. Jos /etc/issue-tiedostolla ei ole oikeaa omistajuutta, luvattomat käyttäjät saattavat muokata sitä sisältämään virheellistä tai harhaanjohtavaa tietoa.
1.7.6	Varmista, että /etc/issue.net -tiedoston käyttöoikeudet on määritetty oikein	1	K	A	Tiedoston /etc/issue.net sisältö näytetään käyttäjille ennen kirjautumista etäyhteyksissä määritellyistä palveluista. Jos /etc/issue.net-tiedostolla ei ole oikeaa omistajuutta, luvattomat käyttäjät saattavat muokata sitä sisältämään virheellistä tai harhaanjohtavaa tietoa.
1.8	GNOME-näyttöhallinta				
1.8.1	Varmista, että GNOME-näyttöhallintaohjelma on poistettu	1	K	A	GNOME-näyttöhallintaohjelma (GDM) on ohjelma, joka hallinnoi graafisia näyttöpalvelimia ja käsittelee graafisten käyttäjien kirjautumiset. Jos graafista käyttöliittymää (GUI) ei tarvita, se tulisi poistaa järjestelmän mahdollisten hyökkäyspintojen vähentämiseksi. **GNOME-näyttöhallintaohjelman poistaminen poistaa graafisen käyttöliittymän (GUI) järjestelmästä.**
1.8.2	Varmista, että GDM-kirjautumisbanneri on määritetty	1	E	A	GDM on GNOME-näyttöhallintaohjelma, joka käsittelee graafisia kirjautumisia GNOME-pohjaisissa järjestelmissä. Varoitusviestit tiedottavat käyttäjille, jotka yrittävät kirjautua järjestelmään, heidän laillisesta asemastaan järjestelmää kohtaan. **Viestien tulee sisältää järjestelmän omistavan organisaation nimi sekä mahdolliset käytössä olevat seurantakäytännöt.**
1.8.3	Varmista, että GDM:n disable-user-list -vaihtoehto on käytössä	1	E	A	GDM on GNOME-näyttöhallintaohjelma, joka käsittelee graafisia kirjautumisia GNOME-pohjaisissa järjestelmissä. Disable-user-list -vaihtoehto määrittää, näytetäänkö käyttäjälista kirjautumisruudulla. Käyttäjälistan näyttäminen voi paljastaa puolet käyttäjätunnus/salasana-yhdistelmästä, jonka luvaton henkilö tarvitsisi kirjautuakseen järjestelmään.

Nro	Suositus	T	K	S	Kommentti
1.8.4	Varmista, että GDM lukitsee näytön, kun käyttäjä on epäaktiivinen	1	E	A	GNOME Desktop Managerin avulla voidaan lukita näytön automaattisesti aina, kun käyttäjä on epäaktiivinen tietyn ajanjakson. Tämä voidaan määrittää "idle-delay" ja "lock-delay" -asetuksilla. Esimerkiksi idle-delay=uint32 900 määrittää, että näyttö menee pimenee 900 sekunnin epäaktiivisen olon jälkeen, ja lock-delay=uint32 5 määrittää, että näyttö lukitaan 5 sekuntia sen jälkeen, kun näyttö on mennyt pimeäksi. Näytön lukitsemisen määrittäminen vähentää mahdollisuutta, että luvaton käyttäjä pääsisi käsiksi toisen käyttäjän käynnissä olevaan istuntoon.
1.8.5	Varmista, että GDM-näytön lukituksia ei voi ohittaa	1	E	A	GNOME Desktop Managerin avulla voidaan lukita näytön automaattisesti aina, kun käyttäjä on epäaktiivinen tietyn ajanjakson. dconfin avulla voidaan estää käyttäjiä muuttamasta tiettyjä asetuksia käyttämällä "lockdown" -tilaa. Tämä tehdään luomalla "locks"-alihakemisto avaintiedostohakemistoon, ja nämä tiedostot sisältävät luettelon lukittavista avaimista tai alipoluista. Esimerkiksi voidaan lukita näytön säästäjän asetukset määrittämällä /org/gnome/desktop/session/idle-delay ja /org/gnome/desktop/screensaver/lock-delay tiedostossa. Tämän toiminnon määrittäminen vähentää mahdollisuutta, että luvaton käyttäjä pääsisi käsiksi toisen käyttäjän käynnissä olevaan istuntoon. Lisäksi, ellei järjestelmäasetuksia lukita, käyttäjän asetukset ovat ensisijaisia verrattuna järjestelmäasetuksiin.
1.8.6	Varmista, että GDM:n irrotettavien medioiden automaattinen liittäminen on poistettu käytöstä	2	E	A	Oletuksena GNOME liittää automaattisesti irrotettavat mediat, kun ne asetetaan paikalleen käyttäjän mukavuuden vuoksi. Tämä toiminto voi kuitenkin olla turvallisuusriski. Kun automaattinen liittäminen on käytössä, kuka tahansa, jolla on fyysinen pääsy laitteeseen, voi liittää USB-aseman tai levyn ja saada sen sisällön käytettäväksi järjestelmässä, vaikka hänellä ei olisi oikeuksia liittää sitä itse. **On kuitenkin huomioitava, että kannettavien kovalevyjen käyttö on työasemakäyttäjille erittäin yleistä. Jos organisaatiosi sallii kannettavien tallennuslaitteiden tai -välineiden käytön työasemissa ja työasemien fyysinen pääsy on riittävä, automaattisen liittämisen poistamisesta on vain vähän hyötyä.**
1.8.7	Varmista, että GDM:n automaattisen irrotettavien medioiden liittämisen estämistä ei voida ohittaa	2	E	A	GNOME liittää oletuksena automaattisesti irrotettavat mediat, kun ne asetetaan paikalleen käyttäjän mukavuuden vuoksi. Vaikka tämä toiminto on käyttäjälle mukava, se voi aiheuttaa turvallisuusriskin. Automaattisen liittämisen ollessa käytössä, jokainen, jolla on fyysinen pääsy laitteeseen, voi liittää USB-aseman tai levyn ja saada sen sisällön käytettäväksi järjestelmässä, vaikka hänellä ei olisi oikeuksia tehdä niin. Dconfin lukitustilassa voidaan estää käyttäjiä muuttamasta tiettyjä asetuksia. Tätä varten on luotava "locks"-alihakemisto avaintiedostohakemistoon. Tämä alihakemisto sisältää avaimia tai alipolkuja, jotka halutaan lukita. Tähän hakemistoon voidaan niin monta tiedostoa kuin halutaan. Esimerkiksi, voidaan lukita asetukset estämään irrotettavien medioiden automaattisen liittämisen. **Vaikka kannettavien kovalevyjen käyttö on työasemakäyttäjille yleistä, on tärkeää varmistaa, että näitä turvallisuusasetuksia ei voida ohittaa, jotta laitteen turvallisuus voidaan taata kaikissa tilanteissa.**

Nro	Suositus	T	K	S	Kommentti
1.8.8	Varmista, että GDM:n auto-run-never on käytössä	1	E	A	GNOME Desktop Display Managerissa on asetus nimeltään "autorun-never", joka mahdollistaa autorun-toiminnon poistamisen käytöstä GDM:n kautta. Tämä toiminto on erityisen tärkeä, koska **haittaohjelmat irrotettavilla medioilla voivat hyödyntää Autorun-ominaisuuksia, kun media asetetaan laitteeseen, ja suorittaa niitä automaattisesti**. Siksi on suositeltavaa poistaa autorun-toiminto käytöstä järjestelmän turvallisuuden parantamiseksi ja haittaohjelmien leviämisen estämiseksi.
1.8.9	Varmista, että GDM:n auto-run-never -asetusta ei ohiteta	1	E	A	GNOME Desktop Display Managerissa on asetus nimeltään "autorun-never", joka mahdollistaa autorun-toiminnon poistamisen käytöstä GDM:n kautta. Järjestelmänvalvojien tulisi käyttää dconf:n lukitustilaa estääkseen käyttäjiä muuttamasta tätä ja muita erityisiä asetuksia. Tätä varten voidaan luoda locks-alihakemisto avainkansioon, joka sisältää tiedostoja, jotka määrittelevät, mitkä avaimet tai alipolut lukitaan. Tämän toimenpiteen tarkoituksena on estää haittaohjelmia hyödyntämästä Autorun-ominaisuuksia, kun irrotettava media asetetaan järjestelmään ja niitä suoritetaan automaattisesti. **Lukitsemalla tämä asetus estetään käyttäjiä muuttamasta sitä, mikä vahvistaa järjestelmän turvallisuutta.**
1.8.10	Varmista, että XDMCP ei ole käytössä	1	K	A	X Display Manager Control Protocol (XDMCP) on suunniteltu tarjoamaan autentikoitu pääsy näytönhallintapalveluihin etänäytöille. Vaikka se voi olla hyödyllinen joissakin tapauksissa, se sisältää useita turvallisuushaavoittuvuuksia. XDMCP ei ole salattu protokolla, mikä tarkoittaa, että hyökkääjä voisi potentiaalisesti siepata käyttäjän näppäinpainallukset. Lisäksi se on haavoittuva man-in-the-middle -hyökkäyksille. Tällaisessa hyökkäyksessä hyökkääjä voi esittää olevansa XDMCP-palvelin ja varastaa laillisten käyttäjien tunnistetiedot. Näistä syistä on suositeltavaa, että XDMCP ei ole käytössä järjestelmissä, jotta näitä mahdollisia turvallisuusriskejä voidaan välttää.
1.9	Varmista, että päivitykset, korjaukset ja lisäsuojausohjelmat on asennettu	1	K	M	Ohjelmistolle julkaistaan ajoittain päivityksiä joko turvallisuuspuutteiden korjaamiseksi tai lisätoiminnallisuuksien sisällyttämiseksi. On välttämätöntä pitää järjestelmät ajan tasalla näillä päivityksillä, koska ne saattavat sisältää turvallisuusparannuksia, jotka eivät olisi saatavilla pelkästään viimeisimmän täydellisen päivityksen kautta. Käyttämällä uusimpia ohjelmistokorjauksia voidaan hyödyntää uusinta toiminnallisuutta. Organisaatioiden on kuitenkin harkittava, täyttääkö tietty päivitys heidän vaatimuksensa ja varmistettava minkä tahansa lisäohjelmiston yhteensopivuus ja tuki valittua päivitysversiota vasten.
2	**Palvelut**				
2.1	Ajan synkronoinnin konfigurointi				
2.1.1	Varmista, että ajan synkronointi on käytössä				

Nro	Suositus	T	K	S	Kommentti
2.1.1.1	Varmista, että vain yksi ajan synkronointipalvelu on käytössä	1	K	A	Järjestelmän ajan tulisi olla synkronoitu määritellyn aikapalvelimen kanssa. Virtuaalijärjestelmissä, joissa on isäntäpohjainen synkronointi, tulee noudattaa virtualisointiohjelmiston suosituksia. Vain yksi synkronointimenetelmä tulisi olla käytössä kerrallaan. Tämä takaa johdonmukaiset aikamerkinnät lokitiedostoissa ja tukee turvallisuusmekanismeja.
2.1.2	Konfiguroi chrony				
2.1.2.1	Varmista, että chrony on konfiguroitu käyttämään valtuutettua aikapalvelinta	1	E	M	Chrony voi määrittää NTP-palvelimia server direktiivillä ja NTP-palvelinaltaita pool direktiivillä. Server direktiivi määrittää yksittäisen NTP-palvelimen, kun taas pool direktiivi määrittää useita NTP-palvelimia. Aikasynkronointi on tärkeää johdonmukaisten aikamerkintöjen ja turvallisuusmekanismien tukemiseksi.
2.1.2.2	Varmista, että chrony toimii _chrony-käyttäjänä	1	E	A	Chrony-paketti on asennettu omistetulla käyttäjätilillä _chrony. Tälle tilille on myönnetty oikeudet, joita chronyd-palvelu tarvitsee. On suositeltavaa, että chronyd-palvelu toimii vain tarvittavilla oikeuksilla.
2.1.2.3	Varmista, että chrony on aktivoitu ja käynnissä	1	E	A	Chrony on daemon, joka synkronoi järjestelmän kellon verkon yli. Sen tulee olla käytössä ja käynnissä, jotta järjestelmä voidaan synkronoida aikapalvelimen kanssa. Ajan synkronointi on tärkeää, jotta tuetaan aikaan sidottuja turvamekanismeja ja varmistetaan, että lokitiedostot ovat yhdenmukaisia koko yrityksen laajuudessa, mikä auttaa rikostutkinnassa.
2.1.3	Konfiguroi systemd-timesyncd				
2.1.3.1	Varmista, että systemd-timesyncd on konfiguroitu käyttämään valtuutettua aikapalvelinta	1	E	M	Systemd-timesyncd mahdollistaa ajan synkronoinnin käyttämällä NTP- ja FallbackNTP-asetuksia määritelläkseen aikapalvelimet. NTP-asetus sisältää listan aikapalvelimista, joihin daemon yrittää ottaa yhteyttä, kunnes saa vastauksen, kun taas FallbackNTP on varalistana, jos muita aikapalvelimia ei ole saatavilla. Ajan synkronointi on tärkeää, jotta tuetaan aikaan sidottuja turvamekanismeja ja varmistetaan, että lokitiedostot ovat yhdenmukaisia koko yrityksen laajuudessa, mikä auttaa rikostutkinnassa.
2.1.3.2	Varmista, että systemd-timesyncd on aktivoitu ja käynnissä	1	E	A	Systemd-timesyncd on daemon, joka on lisätty järjestelmän kellon synkronoimiseksi verkon yli. Jotta järjestelmä voidaan synkronoida aikapalvelimeen, systemd-timesyncd tulee olla käytössä ja käynnissä. Ajan synkronointi on tärkeää, jotta tuetaan aikaan sidottuja turvamekanismeja ja varmistetaan, että lokitiedostot ovat yhdenmukaisia koko yrityksen laajuudessa, mikä auttaa rikosteknisissä tutkimuksissa.
2.1.4	Konfiguroi ntp				
2.1.4.1	Varmista, että ntp-pääsynhallinta on konfiguroitu	1	K	A	NTP-palvelimella on erilaisia pääsynhallintakomentoja, jotka määrittävät, miten ulkopuoliset laitteet voivat kommunikoida palvelimen kanssa. Pääsynhallintasäännöissä määritellään osoitteet, maskit ja erilaiset liput, jotka määräävät tietoliikenteen rajoitukset. Esimerkiksi 'kod'-lippu lähettää "kiss-o'-death" (KoD) -paketin pääsynrikkomuksen sattuessa, kun taas 'noquery'-lippu estää ntpq ja ntpdc -kyselyt. Jos järjestelmässä käytetään NTP:tä, on välttämätöntä, että sen määritykset ovat oikein, jotta ajan synkronointi on tarkkaa.

Nro	Suositus	T	K	S	Kommentti
2.1.4.2	Varmista, että ntp on konfiguroitu käyttämään valtuutettua aikapalvelinta	1	K	M	NTP määrittää erilaisia tiloja komennon avainsanojen ja vaaditun IP-osoitteen tyypin perusteella. Osoitteet jaetaan tyyppeihin: (s) etäpalvelin tai vertainen, (b) paikallisen rajapinnan lähetysosoite, (m) monilähetysosoite tai (r) referenssikellon osoite. Jos IPv6:n perusliittymän laajennukset on havaittu, tuotetaan tuki IPv6-osoiteperheelle lisäksi oletustukeen IPv4-osoiteperheelle. IPv6-osoitteita voidaan käyttää lähes kaikkialla, missä IPv4-osoitteita voidaan käyttää, paitsi referenssikellojen osoitteissa. 'pool'- ja 'server'-komennolla voidaan määrittää, miten paikallinen kello synkronoidaan etäpalvelimeen. Ajan synkronointi on tärkeää tukemaan aikaan sidottuja turvamekanismeja ja varmistamaan, että lokitiedostoilla on yhdenmukaiset aikamerkinnät koko yrityksessä, mikä auttaa rikosteknisissä tutkimuksissa.
2.1.4.3	Varmista, että ntp toimii ntp-käyttäjänä	1	K	A	Ntp-paketti käyttää omistettua käyttäjätiliä nimeltä ntp. Jos järjestelmässä käytetään chronyta tai systemd-timesyncd:ä, ntp pitäisi poistaa. Ainoastaan yksi ajan synkronointimenetelmä tulisi olla käytössä järjestelmässä. Tämän toimenpiteen tarkoitus on varmistaa, että ntpd-daemoni toimii vain tarvittavilla oikeuksilla.
2.1.4.4	Varmista, että ntp on aktivoitu ja käynnissä	1	K	A	Ntp on daemon, joka synkronoi järjestelmän kellon verkon yli. Ntp:n on oltava käynnissä ja käytössä, jotta järjestelmä voidaan synkronoida aikapalvelimeen. Ajan synkronointi on tärkeää tukemaan aikaan sidottuja turvamekanismeja ja varmistamaan, että lokitiedostoilla on johdonmukaiset aikamerkinnät koko yrityksessä, mikä auttaa rikostutkimuksissa.
2.2	Järjestelmäpalvelut				
2.2.1	Varmista, että X Window System ei ole asennettu	1	K	A	X Window System tarjoaa graafisen käyttöliittymän (GUI), jossa käyttäjät voivat käyttää useita ikkunoita suorittaakseen ohjelmia ja erilaisia lisäosia. X Window Systemiä käytetään tyypillisesti työasemilla, joissa käyttäjät kirjautuvat sisään, mutta ei palvelimilla, joissa käyttäjät eivät tyypillisesti kirjaudu sisään. Ellei organisaatiosi erityisesti vaadi graafista kirjautumista X Windowsin kautta, poista se vähentääksesi mahdollista hyökkäyspintaa. Monet Linux-järjestelmät ajavat sovelluksia, jotka vaativat Java-ympäristön. Joissakin Linuxin Java-paketeissa on riippuvuus erityisistä X Windowsin xorg-x11-fonteista. Yksi keino välttää tämä riippuvuus on käyttää "headless" Java-paketteja tiettyyn Java-ympäristöön, jos jakelu tarjoaa ne.
2.2.2	Varmista, että Avahi Server ei ole asennettu	1	K	A	Avahi on ilmainen zeroconf-toteutus, joka sisältää järjestelmän multicast DNS/DNS-SD palvelun löytämiseen. Avahi mahdollistaa ohjelmien julkaisun ja palveluiden ja isäntien löytämisen paikallisessa verkossa ilman erityistä konfiguraatiota. Esimerkiksi käyttäjä voi liittää tietokoneen verkkoon ja Avahi löytää automaattisesti tulostimet tulostusta varten, tiedostot, joihin katsotaan, ja ihmiset, joiden kanssa keskustellaan, sekä verkkopalvelut, jotka toimivat koneella. **Verkkopalvelujen automaattista löytämistä ei yleensä vaadita järjestelmän toiminnallisuudelle**. On suositeltavaa poistaa tämä paketti vähentääksesi mahdollista hyökkäyspintaa.

Nro	Suositus	T	K	S	Kommentti
2.2.3	Varmista, että CUPS ei ole asennettu	2	K	A	Common Unix Print System (CUPS) tarjoaa mahdollisuuden tulostaa sekä paikallisiin että verkon tulostimiin. Järjestelmä, jossa CUPS on käytössä, voi myös vastaanottaa tulostustehtäviä etäjärjestelmistä ja tulostaa ne paikallisille tulostimille. Se tarjoaa myös verkkopohjaisen etähallintamahdollisuuden. Jos järjestelmän ei tarvitse tulostaa tehtäviä tai vastaanottaa tulostustehtäviä muista järjestelmistä, suositellaan CUPS:n poistamista vähentääksesi mahdollista hyökkäyspintaa. **CUPS:n poistaminen estää tulostuksen järjestelmästä, mikä on yleinen tehtävä työasemajärjestelmissä.**
2.2.4	Varmista, että DHCP Server ei ole asennettu	1	K	A	Dynamic Host Configuration Protocol (DHCP) on palvelu, joka mahdollistaa koneiden dynaamisen IP-osoitteen määrittämisen. **Ellei järjestelmää ole nimenomaisesti määritetty toimimaan DHCP-palvelimena, on suositeltavaa poistaa tämä paketti vähentääksesi mahdollista hyökkäyspintaa.**
2.2.5	Varmista, että LDAP-palvelin ei ole asennettu	1	K	A	Lightweight Directory Access Protocol (LDAP) esiteltiin korvaamaan NIS/YP. Se on palvelu, joka tarjoaa tavan hakea tietoa keskitetystä tietokannasta. **Jos järjestelmän ei tarvitse toimia LDAP-palvelimena, on suositeltavaa poistaa ohjelmisto vähentääksesi mahdollista hyökkäyspintaa.**
2.2.6	Varmista, että NFS ei ole asennettu	1	K	A	Network File System (NFS) on yksi ensimmäisistä ja laajimmin jaetuista tiedostojärjestelmistä UNIX-ympäristössä. Se tarjoaa mahdollisuuden järjestelmille liittää muiden palvelimien tiedostojärjestelmiä verkon kautta. **Jos järjestelmä ei jaa NFS-osakkeita, on suositeltavaa poistaa nfs-kernel-server -paketti vähentääksesi etähyökkäyspintaa.**
2.2.7	Varmista, että DNS-palvelin ei ole asennettu	1	K	A	Domain Name System (DNS) on hierarkkinen nimeämissysteemi, joka määrittää nimet IP-osoitteiksi tietokoneille, palveluille ja muille verkkoon liitetyille resursseille. **Ellei järjestelmää ole nimenomaisesti määritetty toimimaan DNS-palvelimena, on suositeltavaa poistaa kyseinen paketti vähentääksesi potentiaalista hyökkäyspintaa.**
2.2.8	Varmista, että FTP-palvelin ei ole asennettu	1	E	A	File Transfer Protocol (FTP) mahdollistaa tiedostojen siirron verkkoon liitettyjen tietokoneiden välillä. FTP ei suojaa tiedon luottamuksellisuutta eikä autentikointitietoja. Jos tiedostojen siirtoa tarvitaan, on suositeltavaa käyttää SFTP:tä. Ellei järjestelmän tarvitse toimia FTP-palvelimena (esimerkiksi sallimaan anonyymit lataukset), on suositeltavaa poistaa paketti vähentääksesi potentiaalista hyökkäyspintaa.
2.2.9	Varmista, että HTTP-palvelin ei ole asennettu	1	E	A	HTTP- eli verkkopalvelimet tarjoavat mahdollisuuden isännöidä verkkosivuston sisältöä. Ellei järjestelmän tarvitse toimia verkkopalvelimena, on suositeltavaa poistaa paketti vähentääksesi potentiaalista hyökkäyspintaa.
2.2.10	Varmista, että IMAP- ja POP3-palvelimet eivät ole asennettuna	1	K	A	dovecot-imapd ja dovecot-pop3d ovat avoimen lähdekoodin IMAP- ja POP3-palvelimia Linux-pohjaisille järjestelmille. Ellei järjestelmän ole tarkoitus tarjota POP3- ja/tai IMAP-palvelimia, on suositeltavaa poistaa paketti vähentääksesi potentiaalista hyökkäyspintaa.
2.2.11	Varmista, että Samba ei ole asennettu	1	E	A	Samba-daemoni mahdollistaa järjestelmänvalvojille Linux-järjestelmiensä konfiguroinnin tiedostojärjestelmien ja hakemistojen jakamiseen Windows-työpöydille. Samba mainostaa tiedostojärjestelmiä ja hakemistoja Server Message Block (SMB) -protokollan kautta. Windows-työpöytäkäyttäjät voivat liittää nämä hakemistot ja tiedostojärjestelmät kirjainasemiksi järjestelmissään. Jos ei ole tarvetta liittää hakemistoja ja tiedostojärjestelmiä Windows-järjestelmiin, tämä palvelu tulisi poistaa vähentääksesi potentiaalista hyökkäyspintaa.

Nro	Suositus	T	K	S	Kommentti
2.2.12	Varmista, että HTTP Proxy -palvelin ei ole asennettu	1	K	A	Squid on standardi välityspalvelin, jota käytetään monissa jakeluissa ja ympäristöissä. Jos välityspalvelimelle ei ole tarvetta, suositellaan, että squid-välityspalvelin poistetaan vähentämään potentiaalista hyökkäyspintaa.
2.2.13	Varmista, että SNMP-palvelin ei ole asennettu	1	E	A	Simple Network Management Protocol (SNMP) on laajasti käytetty protokolla verkkolaitteiden, tietokonelaitteiden ja laitteiden, kuten UPS-laitteiden, terveyden ja hyvinvoinnin seuraamiseen. SNMP-palvelin voi kommunikoida käyttäen SNMPv1:stä, joka lähettää tietoja salaamattomasti eikä vaadi autentikointia komentojen suorittamiseen. Jos SNMP-palvelua ei tarvita, net-snmp-paketti tulisi poistaa järjestelmästä vähentämään sen hyökkäyspintaa. Jos SNMP on välttämätöntä, palvelin tulisi konfiguroida käyttämään vain SNMPv3:sta ja käyttäjän autentikointi sekä viestien salaaminen tulisi ottaa käyttöön.
2.2.14	Varmista, että NIS-palvelin ei ole asennettu	1	K	A	Network Information Service (NIS), joka tunnetaan aiemmin nimellä Yellow Pages, on asiakas-palvelin hakemistopalveluprotokolla järjestelmän konfiguraatiotiedostojen jakamiseen. NIS-palvelu on luonteeltaan turvaton järjestelmä, joka on ollut haavoittuvainen DOS-hyökkäyksille, puskuriylivuodoille ja sillä on heikko autentikointi NIS-karttojen kyselyssä. Yleensä NIS on korvattu sellaisilla protokollilla kuin Lightweight Directory Access Protocol (LDAP). Suositus on, että palvelu poistetaan ja muita, turvallisempia palveluita käytetään sen sijaan.
2.2.15	Varmista, että sähköpostin-siirtopalvelin on konfiguroitu vain paikalliseen tilaan	1	K	A	Sähköpostin siirtoagentit (MTA), kuten sendmail ja Postfix, kuuntelevat saapuvia viestejä ja siirtävät ne asianmukaiselle käyttäjälle tai sähköpostipalvelimelle. Jos järjestelmää ei ole tarkoitettu sähköpostipalvelimeksi, on suositeltavaa, että MTA on konfiguroitu käsittelemään vain paikallista postia. MTA-ohjelmistot ovat monimutkaisia ja useimmilla niistä on pitkä historia turvallisuusongelmista. Vaikka on tärkeää varmistaa, että järjestelmä voi käsitellä paikallisia sähköpostiviestejä, MTA-daemonin ei tarvitse kuunnella porttia, ellei palvelimen ole tarkoitus vastaanottaa ja käsitellä postia muista järjestelmistä.
2.2.16	Varmista, että rsync-palvelu ei ole asennettu tai se on estetty	1	E	A	rsync-palvelua voidaan käyttää tiedostojen synkronointiin järjestelmien välillä verkkoyhteyksien yli. rsync-palvelu muodostaa turvallisuusriskin, koska se käyttää salaamattomia protokollia viestintään. rsync-paketti tulisi poistaa järjestelmän hyökkäyspinta-alan vähentämiseksi.
2.3	Asiakasohjelmistot				
2.3.1	Varmista, että NIS-asiakasohjelma ei ole asennettu	1	K	A	NIS, aiemmin Yellow Pages, on vanhentunut hakemistopalveluprotokolla, joka on haavoittuvainen useille hyökkäyksille ja siinä on heikko autentikointi. Vaikka se on suunniteltu jakamaan konfigurointitiedostoja, sen turvattomuus tekee siitä riskin. Modernimmat ja turvallisemmat protokollat, kuten LDAP, ovat yleensä korvanneet NIS:n. Vaikka turvattomia asiakasohjelmistoja käytetään usein testauksessa ja vianmäärityksessä, on tärkeää poistaa ne käytön jälkeen välttääkseen väärinkäytökset.
2.3.2	Varmista, että rsh-asiakasohjelma ei ole asennettu	1	K	A	rsh-client -paketti sisältää vanhoja asiakasohjelmia, joissa on turvallisuusaukkoja ja jotka on korvattu SSH-paketilla. Vaikka rsh-palvelin poistetaan, on suositeltavaa poistaa myös rsh:n, rcp:n ja rloginin asiakasohjelmat estääkseen vahingossa tapahtuvan tunnistetietojen paljastumisen. Vaikka monet käyt-

Nro	Suositus	T	K	S	Kommentti
					tävät turvattomia asiakasohjelmistoja testauksessa ja vianmäärityksessä, on tärkeää poistaa ne käytön jälkeen välttääkseen väärinkäytökset.
2.3.3	Varmista, että talk-asiakasohjelma ei ole asennettu	1	K	A	Talk-ohjelmisto mahdollistaa viestien lähettämisen ja vastaanottamisen terminaali-istunnossa, mutta se aiheuttaa turvallisuusriskin käyttämällä salaamattomia protokollia. Vaikka monet käyttävät turvattomia asiakasohjelmistoja testauksessa ja vianmäärityksessä, on tärkeää poistaa ne käytön jälkeen välttääkseen väärinkäytökset.
2.3.4	Varmista, että telnet-asiakasohjelma ei ole asennettu	1	E	A	Telnet-paketti mahdollistaa yhteyksien aloittamisen telnet-protokollan kautta, mutta se on turvaton ja salaamaton, mikä voi johtaa tunnistetietojen varastamiseen. Vaikka ssh-paketti tarjoaa parempaa turvallisuutta ja on mukana useimmissa Linux-jakeluissa, monet käyttävät turvattomia palveluasiakkaita testaustarkoituksiin. On suositeltavaa poistaa turvattomat asiakasohjelmat käytön jälkeen välttääkseen väärinkäytökset.
2.3.5	Varmista, että LDAP-asiakasohjelma ei ole asennettu	1	K	A	LDAP tarjoaa keskitetystä tietokannasta tiedon hakumenetelmän ja se esiteltiin korvaamaan NIS/YP. Jos järjestelmä ei tarvitse LDAP-asiakasominaisuuksia, sen poistaminen on suositeltavaa pienentämään hyökkäyspintaa. Tämän toimenpiteen seurauksena LDAP:n käyttö tunnistautumisessa saattaa estyä tai vaikeutua.
2.3.6	Varmista, että RPC ei ole asennettu	1	K	A	RPC on matalan tason asiakas-palvelinsovellusten luontimenetelmä, jota tukee rpcbind-paketti. Jos järjestelmä ei tarvitse RPC:ää, palveluiden poistaminen on suositeltavaa hyökkäyspinnan vähentämiseksi.
2.4	Varmista, että tarpeettomat palvelut on poistettu tai estetty	1	K	M	Verkkoliitäntä määrittyy numeronsa, IP-osoitteensa ja protokollatyyppinsä (esim. TCP tai UDP) perusteella. Kuunteleva portti toimii kommunikaatiopisteenä sovellukselle tai prosessille. Avoin portti hyväksyy saapuvia paketteja. Kuuntelevat palvelut ovat potentiaalisia hyökkäysvektoreita. Jos niitä ei tarvita, ne tulisi pysäyttää ja niihin liittyvät paketit poistaa. Välttämättömien palveluiden riippuvuuksien kohdalla palvelu tulisi pysäyttää ja maskata hyökkäyspinnan pienentämiseksi.
3	**Verkon konfigurointi**				
3.1	Poista käyttämättömät verkkoprotokollat ja -laitteet				
3.1.1	Varmista, että järjestelmästä tarkastetaan, onko IPv6 käytössä	1	K	M	IPv6 on IP:n uusin versio, suunniteltu tukemaan suurempaa määrää IP-osoitteita ja parantamaan turvallisuutta. Se perustuu 128-bittiseen osoitteistoon, mahdollistaen valtavan määrän osoitteita. IETF RFC 4038 suosittelee sovellusten rakentamista kahden pinon oletuksella. Vaikka IPv6:n käyttöönottoa ja konfigurointia suositellaan, jos järjestelmässä ei käytetä sitä, se voidaan poistaa käytöstä pienentämään hyökkäyspintaa. Tämä voi kuitenkin aiheuttaa ongelmia joissain sovelluksissa.
3.1.2	Varmista, että langattomat verkkoliitännät ovat poistettu käytöstä	2	E	A	Langaton verkko mahdollistaa yhteyden, kun langallista verkkoa ei ole saatavilla. Debian tarjoaa työkalupaketin langattoman verkon määrittämiseen ja käyttöön. Jos langatonta verkkoa ei tarvita, laitteet kannattaa poistaa käytöstä pienentämään hyökkäyspintaa. Monissa kannettavissa ja joissakin pöytäkoneissa langaton yhteys on kuitenkin välttämätön.

Nro	Suositus	T	K	S	Kommentti
3.1.3	Varmista, että DCCP on poistettu käytöstä	2	K	A	DCCP on siirtokerroksen protokolla, joka tukee suoratoistomediaa ja puheluita. Se mahdollistaa ruuhkansäätelyn sovelluskerroksessa, mutta ei takaa tiedon toimittamista oikeassa järjestyksessä. Jos DCCP:tä ei käytetä, sen ajureiden asentamista tulisi välttää hyökkäyspinnan pienentämiseksi.
3.1.4	Varmista, että SCTP on poistettu käytöstä	2	K	A	SCTP on siirtokerroksen protokolla, joka yhdistää TCP:n ja UDP:n ominaisuudet tukien viestipohjaista viestintää. Jos SCTP:tä ei käytetä, ydinmoduulia ei tulisi ladata hyökkäyspinnan vähentämiseksi.
3.1.5	Varmista, että RDS on poistettu käytöstä	2	K	A	RDS on siirtokerroksen protokolla, joka on suunniteltu klusterin solmujen väliseen nopeaan viestintään. Jos RDS:tä ei käytetä, ydinmoduulia ei tulisi ladata hyökkäyspinnan vähentämiseksi.
3.1.6	Varmista, että TIPC on poistettu käytöstä	2	K	A	TIPC on protokolla, joka on suunniteltu mahdollistamaan viestintä klusterin solmujen välillä. Jos TIPC:tä ei käytetä, ydinmoduulia ei tulisi ladata hyökkäyspinnan vähentämiseksi.
3.2	Verkon parametrit (Vain isäntä)				
3.2.1	Varmista, että pakettien uudelleenlähetys on poistettu käytöstä	1	K	A	Isännät eivät toimi reitittiminä ja eivät tarvitse ICMP-uudelleenohjauksia. Hyökkääjä voisi käyttää heikkoa isäntää ohjaamaan liikennettä haitallisiin kohteisiin.
3.2.2	Varmista, että IP-reititys on poistettu käytöstä	1	K	A	Järjestelmän net.ipv4.ip_forward- ja net.ipv6.conf.all.forwarding -liput määrittävät, voiko järjestelmä välittää paketteja vai ei. Asetuksen ollessa 0 järjestelmä ei välitä paketteja, eikä toimi reitittimenä, vaikka siinä olisi useita verkkoliitäntöjä.
3.3	Verkon parametrit (Isäntä ja reititin)				
3.3.1	Varmista, ettei lähteestä reititetyt paketit ole hyväksyttyjä	1	K	A	Lähdeohjaus mahdollistaa lähettäjän määrittelemään osittain tai kokonaan pakettien kulkeman reitin. Asettamalla järjestelmä niin, ettei se hyväksy lähdeohjattuja paketteja, estetään mahdollisia hyökkäyksiä, joissa hyökkääjä voisi käyttää järjestelmää tavoittaakseen yksityiset osoitteet, jotka normaalisti eivät olisi saavutettavissa.
3.3.2	Varmista, ettei ICMP-uudelleenohjauksia hyväksytä	1	K	A	ICMP-uudelleenohjausviestit ovat paketteja, jotka välittävät reititystietoa ja voivat muuttaa järjestelmän reititystauluja. Hyökkääjät voivat käyttää väärennettyjä ICMP-uudelleenohjausviestejä muuttaakseen haitallisesti järjestelmän reititystauluja. Asettamalla järjestelmä niin, ettei se hyväksy ICMP-uudelleenohjausviestejä, estetään ulkopuolisia päivittämästä järjestelmän reititystauluja.
3.3.3	Varmista, ettei turvallisia ICMP-uudelleenohjauksia hyväksytä	1	K	A	Turvalliset ICMP-uudelleenohjausviestit ovat samankaltaisia kuin tavalliset ICMP-uudelleenohjausviestit, mutta ne tulevat järjestelmän tuntemilta yhdyskäytäviltä. Vaikka näiden yhdyskäytävien oletetaan olevan luotettavia, ne voivat silti olla vaarantuneita. Asetus estää mahdollisesti vaarantuneiden tunnettujen yhdyskäytävien tekemät reititystaulun päivitykset.
3.3.4	Varmista, että epäilyttävät paketit kirjataan lokiin	1	K	A	Kun tämä ominaisuus on käytössä, se kirjaa paketit, joilla on reitittämättömiä lähdeosoitteita, ytimen lokiin. Kirjaamalla nämä paketit järjestelmänvalvoja voi tutkia mahdollisuutta, että hyökkääjä lähettää väärennettyjä paketteja järjestelmään.
3.3.5	Varmista, että lähetys-ICMP-pyynnöt jätetään huomiotta	1	K	A	Järjestelmän asettaminen niin, että se jättää huomiotta kaikki lähetys- ja monilähetysosoitteille lähetetyt ICMP echo ja timestamp -pyynnöt, suojaa järjestelmää osallistumasta Smurf-hyökkäyksiin. Smurf-hyökkäyksessä hyökkääjä käyttää ICMP:n

Nro	Suositus	T	K	S	Kommentti
					lähetysviestejä väärennetyllä lähdeosoitteella, mikä voi moninkertaistaa verkon liikenteen, kun useat isännät vastaavat näihin viesteihin.
3.3.6	Varmista, että virheelliset ICMP-vastaukset jätetään huomiotta	1	K	A	Järjestelmän asettaminen niin, että se jättää huomiotta RFC-1122:n vastaiset virheelliset ICMP-vastaukset estää järjestelmää kirjaamasta näitä virheellisiä viestejä. Tämä suojaa järjestelmää tietyiltä reitittimiltä ja hyökkääjiltä, jotka saattavat yrittää täyttää lokitiedostojärjestelmän merkityksettömillä virheviesteillä.
3.3.7	Varmista, että reverse path suodatus on käytössä	1	K	A	Reverse path suodatuksen avulla Linux-ydin tarkistaa vastaanotetun paketin validiteetin varmistaen, että paluupaketti käyttää samaa liitäntää kuin alkuperäinen lähdepaketti. Tämä estää hyökkääjiä lähettämästä järjestelmälle epäkelpoja paketteja. Kuitenkin jos järjestelmässä käytetään epäsymmetristä reititystä, tämä ominaisuus voi aiheuttaa ongelmia reitityksessä.
3.3.8	Varmista, että TCP SYN -evästeet ovat käytössä	1	K	A	TCP SYN-evästeiden avulla ydin käsittelee TCP SYN -paketteja normaalisti, kunnes puoliavoin yhteysjono on täynnä. Tällöin SYN-evästetoiminto aktivoituu. Jos järjestelmää vastaan tehdään SYN-tulva hyökkäys, joka pyrkii estämään palvelun yrittämällä kuluttaa kaikki puoliavoin yhteysjonojen paikat, SYN-evästeiden käyttö mahdollistaa silti legitiimien yhteyksien muodostamisen. Tämä suojaa järjestelmää palvelunestohyökkäyksiltä.
3.3.9	Varmista, ettei järjestelmä hyväksy IPv6-reitittimen ilmoituksia	1	K	A	Tämä asetus estää järjestelmän kyvyn hyväksyä IPv6-reitittimen ilmoituksia. Järjestelmiä suositellaan estämään reitittimen ilmoitukset, jotta niitä ei huijattaisi ohjaamaan liikennettä vaarantuneisiin koneisiin. Määrittämällä kovat reitit järjestelmään suojataan sitä epäluotettavilta reiteiltä.
3.5	Palomuurin konfiguraatio				
3.5.1	Konfiguroi UncomplicatedFirewall				
3.5.1.1	Varmista, että ufw on asennettu	1	K	A	Ufw on yksinkertainen palomuurin hallintatyökalu, joka toimii iptablesin kanssa. Se on suunniteltu erityisesti isäntäpohjaisille palomuureille. Palomuurin työkalu on välttämätön Linuxin netfilter-rakenteen määrittämiseksi. On tärkeää suojata järjestelmää sisäverkon uhilta, kuten haitalliselta koodilta ja virheellisesti määritetyltä ohjelmistolta. Vain yksi palomuurityökalu tulisi asentaa ja konfiguroida.
3.5.1.2	Varmista, että iptables-persistent ei ole asennettu ufw:n kanssa	1	K	A	Iptables-persistent on käynnistysaikainen lataaja netfilter-säännöille. Samanaikaisten ufw- ja iptables-persistent-palveluiden käyttö voi johtaa ristiriitoihin.
3.5.1.3	Varmista, että ufw-palvelu on käytössä	1	K	A	UncomplicatedFirewall (ufw) on iptablesin käyttöliittymä, joka tarjoaa kehyksen netfilterin hallintaan. Kun ufw otetaan käyttöön, se voi katkaista olemassa olevia yhteyksiä, mutta sääntöjä voidaan lisätä ennen palomuurin käyttöönottoa. On tärkeää varmistaa, että ufw on käytössä järjestelmän suojauksen takaamiseksi. Palomuuriasetusten muuttaminen verkkoyhteyden yli voi johtaa yhteyden menetykseen järjestelmään.
3.5.1.4	Varmista, että ufw:n silmukkaliikenne on konfiguroitu	1	K	A	Määritä silmukkaliitäntä hyväksymään liikenne ja muiden liitäntöjen torjumaan silmukkaverkon liikenne. Silmukkaliikenne on välttämätöntä järjestelmän toiminnalle ja muiden liitäntöjen tulisi sivuuttaa tämä liikenne väärinkäytön estämiseksi.

Nro	Suositus	T	K	S	Kommentti
3.5.1.5	Varmista, että ufw:n lähtevät yhteydet ovat konfiguroitu	1	K	M	Määritä palomuurisäännöt uusille lähteville yhteyksille. Muutettaessa palomuuriasetuksia verkossa on riski lukita itsensä ulos järjestelmästä. Ufw hoitaa automaattisesti liittyvät vakiintuneet yhteydet, kun uusi lähtevä sääntö lisätään. Ilman sääntöjä kaikki paketit hylätään oletussäännöstön mukaan estäen verkon käytön.
3.5.1.6	Varmista, että ufw-palomuurisäännöt ovat olemassa kaikille avoimille porteille	1	K	A	Kaikki avoimet portit, jotka eivät ole loopback-osoitteissa, tarvitsevat palomuuri-säännöt liikenteen hallintaan. Muuttamalla palomuurin asetuksia verkon yli voi estää pääsyn järjestelmään. Ilman palomuurisääntöjä avoimille porteille oletuspalomuurikäytäntö estää kaiken liikenteen näihin portteihin.
3.5.1.7	Varmista, että ufw käyttää "kiellä oletusarvoisesti" -palomuurikäytäntöä	1	K	A	Oletuspolitiikan hylkääminen varmistaa, että kaikki määrittämätön verkkoaktiviteetti torjutaan. On helpompaa luoda sallittujen käyttöjen luettelo kuin määritellä kielletyt käytöt. Jos tätä sääntöä sovelletaan, kaikki portit ja protokollat, joita ei ole nimenomaisesti sallittu, estetään.
3.5.2	Konfiguroi nftables				
3.5.2.1	Varmista, että nftables on asennettu	1	E	A	Nftables on uusi sisäisen ytimen pakettien luokittelujärjestelmä, joka perustuu verkkoerityiseen virtuaalikoneeseen ja uuteen nft-käyttäjätilan komentorivityökaluun. Se suojaa sisäisistä uhista, kuten haitallisesta mobiilikoodista ja huonosti määritellystä ohjelmistosta isännällä. Muista, että vain yksi palomuurisovellus tulisi asentaa ja muokata, ja palomuuriasetusten muuttaminen verkon yli voi johtaa järjestelmään pääsyn estämiseen.
3.5.2.2	Varmista, että ufw on poistettu asennuksesta tai poistettu käytöstä nftables:n kanssa	1	E	A	UFW on yksinkertainen palomuurihallintatyökalu. Nftables-palvelun ja ufw:n samanaikainen käyttö voi johtaa ristiriitoihin ja odottamattomiin tuloksiin.
3.5.2.3	Varmista, että iptables on tyhjennetty nftables:n kanssa	1	E	M	Nftables on korvaaja iptablesille, ip6tablesille, ebtablesille ja arptablesille. Vaikka iptablesin ja nftablesin yhdistäminen on mahdollista, se lisää monimutkaisuutta ja virheiden riskiä. Tyhjennä kaikki iptables-säännöt ja varmista, ettei sitä ole ladattu.
3.5.2.4	Varmista, että nftables-taulukko on olemassa	1	E	A	Taulukot sisältävät ketjuja ja liittyvät aina yhteen osoiteperheeseen. Ilman rakennettua taulukkoa nftables ei suodata verkkoliikennettä. Sääntöjen lisääminen käynnissä olevaan nftablesiin voi katkaista yhteyden järjestelmään.
3.5.2.5	Varmista, että nftables-perusketjut ovat olemassa	1	E	A	Ketjut ovat sääntöjen säiliöitä, ja ne voidaan jakaa perusketjuihin ja tavallisiin ketjuihin. Ilman perusketjuja tiettyjen pakettien käsittely nftables-sääntöjen avulla ei onnistu. Jos konfiguroit nftablesia SSH:n yli ja asetat perusketjun pudottamaan paketit, yhteys katkeaa. Varmista, että SSH:lle on sääntö ennen kuin asetat perusketjun pudottamaan paketit.
3.5.2.6	Varmista, että nftables-silmukkaliikenne on konfiguroitu	1	E	A	Loopback-liikenne on tärkeää järjestelmän toiminnalle ja sitä tulisi sallia vain loopback-rajapinnassa. Kaikki muut rajapinnat tulisi määrittää hylkäämään loopback-verkon liikenne väärennösten estämiseksi.
3.5.2.7	Varmista, että nftables-lähtevät ja vakiintuneet yhteydet ovat konfiguroitu	1	E	M	Palomuurisäännöt tulisi määrittää uusille lähteville ja jo vakiintuneille yhteyksille. Ilman näitä sääntöjä kaikki paketit hylätään oletussäännöllä, estäen verkon käytön.

Nro	Suositus	T	K	S	Kommentti
3.5.2.8	Varmista, että nftables:n oletuskieltosääntö on käytössä	1	E	A	Perusketjun politiikka on oletustuomio paketeille, jotka saavuttavat ketjun lopun. On helpompaa sallia haluttu liikenne kuin estää ei-haluttu liikenne. Virheelliset palomuuriasetukset voivat katkaista yhteyden, erityisesti SSH-yhteyksissä. Asettaessasi politiikaksi "drop", varmista, että SSH on sallittu ennen muutoksia.
3.5.2.9	Varmista, että nftables-palvelu on käytössä	1	E	A	Nftables-palvelu mahdollistaa nftables-sääntöjen lataamisen käynnistyksen aikana tai palvelun käynnistämisen yhteydessä. Palvelu palauttaa nftables-säännöt /etc/nftables.conf-tiedostossa olevista sääntötiedostoista.
3.5.2.10	Varmista, että nftables-säännöt ovat pysyviä	1	E	A	Nftables on Linux-ytimen alijärjestelmä, joka tarjoaa verkkopakettien suodattamisen ja luokittelun. Säännöstössä määritetään, kuinka verkkoliikenne suodatetaan. Muutokset nftables-säännöstöön vaikuttavat vain käynnissä olevaan järjestelmään, joten säännöt on myös määritettävä käynnistettäessä.
3.5.3	Konfiguroi iptables				
3.5.3.1	Konfiguroi iptables-ohjelmisto				
3.5.3.1.1	Varmista, että iptables-paketit ovat asennettu	1	E	A	Iptables mahdollistaa järjestelmänvalvojalle Linux-ytimen palomuuritaulukoiden konfiguroinnin. Se soveltuu IPv4:lle, kun taas muut työkalut soveltuvat muihin protokolliin. Palomuurisääntöjen määrittämiseen ja ylläpitämiseen tarvitaan konfigurointimenetelmä.
3.5.3.1.2	Varmista, että nftables ei ole asennettu iptables:n kanssa	1	E	A	nftables on Linux-ytimen alijärjestelmä, joka korvaa iptablesin ja suodattaa verkkojen paketteja. Iptablesin ja nftablesin samanaikainen käyttö voi aiheuttaa ristiriitoja.
3.5.3.1.3	Varmista, että ufw on poistettu asennuksesta tai poistettu käytöstä iptables:n kanssa	1	E	A	UFW on helppokäyttöinen palomuuriohjelma, joka käyttää iptablesia konfigurointiin. UFW:n ja iptables.persistentin samanaikainen käyttö voi aiheuttaa ristiriitoja ja odottamattomia tuloksia.
3.5.3.2	Konfiguroi IPv4 iptables				
3.5.3.2.1	Varmista, että iptables:n oletuskieltosääntö on käytössä	1	E	A	Oletuksena kaikki kieltävä politiikka varmistaa, että kaikki määrittämätön verkkokäyttö hylätään. Oletuksena hyväksyvällä politiikalla palomuuri hyväksyy kaikki määrittämättömät paketit. On helpompaa sallia vain hyväksytty käyttö kuin estää ei-toivottu käyttö. Muista olla varovainen muuttaessasi palomuurin asetuksia verkossa, jotta et jää ulos järjestelmästä.
3.5.3.2.2	Varmista, että iptables-silmukkaliikenne on konfiguroitu	1	E	A	Silmukkaliikenne on välttämätöntä koneen prosessien välillä ja on yleensä kriittistä järjestelmän toiminnalle. Silmukkaliittymän pitäisi olla ainoa paikka, josta silmukkaverkon (127.0.0.0/8) liikenne näkyy, kun taas kaikkien muiden liittymien tulisi hylätä tämä liikenne väärennösten estämiseksi. Muista, että palomuurin muuttaminen verkkoyhteyden yli voi johtaa järjestelmästä lukkiutumiseen.
3.5.3.2.3	Varmista, että iptables-lähtevät ja vakiintuneet yhteydet ovat konfiguroitu	1	E	M	Määritä palomuurisäännöt uusille lähteville ja vahvistetuille yhteyksille. Palomuuriasetusten muuttaminen verkon yli voi johtaa järjestelmän lukitsemiseen. Ilman näitä sääntöjä kaikki paketit hylätään oletuspolitiikan mukaisesti, estäen verkon käytön.
3.5.3.2.4	Varmista, että iptables-palomuurisäännöt ovat olemassa kaikille avoimille porteille	1	E	A	Kaikki avoimet portit ei-loopback-osoitteissa tarvitsevat palomuurisääntöjä liikenteen hallitsemiseksi. Muuttamalla palomuurin asetuksia verkkoyhteyden yli voi menettää yhteyden järjestelmään. On tärkeää varmistaa, että oletuksena oleva palomuuripolitiikka on asetettu myös käynnistyksen yhteydessä. Ilman määriteltyä palomuurisääntöä, oletuspalomuuripolitiikka hylkää kaikki paketit näihin porteihin.

Nro	Suositus	T	K	S	Kommentti
3.5.3.3	Konfiguroi IPv6 ip6tables				
3.5.3.3.1	Varmista, että ip6tables:n oletuskieltosääntö on käytössä	1	E	A	Oletuskieltosäännöllä varmistetaan, että kaikki määrittämätön verkkoliikenne hylätään. Oletuksena hyväksyvällä säännöllä palomuuri hyväksyy kaikki paketit, joita ei ole erikseen kielletty. On helpompi sallia hyväksytty liikenne kuin kieltää ei-toivottu liikenne. Muuta palomuuriasetuksia varoen, jotta et joudu lukitsemaan itsesi ulos järjestelmästä.
3.5.3.3.2	Varmista, että ip6tables-silmukkaliikenne on konfiguroitu	1	E	A	Loopback-liikenne on tärkeää järjestelmän toiminnalle ja sitä tulisi sallia vain loopback-rajapinnan kautta. Kaikkien muiden rajapintojen tulisi hylätä loopback-verkon (::1) liikenne. Tämä on välttämätöntä turvallisuustoimenpiteenä. Huomioi, että palomuuriasetusten muuttaminen verkon yli voi johtaa yhteyden menettämiseen järjestelmään.
3.5.3.3.3	Varmista, että ip6tables-lähtevät ja vakiintuneet yhteydet ovat konfiguroitu	1	E	M	Määritä palomuurisäännöt uusille lähteville ja vakiintuneille IPv6-yhteyksille. Muutos palomuuriasetuksiin verkkoyhteyden aikana voi johtaa järjestelmästä lukkiutumiseen. Varmista myös, että oletuspolitiikka on määritetty käynnistettäessä. Ilman näitä sääntöjä oletuspolitiikka hylkää kaikki paketit, mikä estää verkon käytön.
3.5.3.3.4	Varmista, että ip6tables-palomuurisäännöt ovat olemassa kaikille avoimille porteille	1	E	A	Kaikki avoimet portit ei-loopback-osoitteissa tarvitsevat palomuurisäännöt. Muuttamalla palomuuriasetuksia verkkoyhteyden yli voi johtaa järjestelmän uloskirjautumiseen. Palomuuri avaa portin kaikelle liikenteelle. Ilman palomuurisääntöjä oletuspolitiikka hylkää kaikki näihin portteihin tulevat paketit.
4	**Lokitus ja auditointi**				
4.1	Konfiguroi järjestelmän auditointi (auditd)				
4.1.1	Varmista, että auditointi on käytössä				
4.1.1.1	Varmista, että auditd on asennettu	2	K	A	Auditd on Linuxin valvontajärjestelmän käyttäjätilan komponentti, joka kirjoittaa valvontatietueet levylle. Tämä auttaa järjestelmänvalvojia tunnistamaan mahdolliset luvattomat käyttöyritykset.
4.1.1.2	Varmista, että auditd-palvelu on käytössä ja aktiivinen	2	K	A	Ota käyttöön auditd-daemoni järjestelmätapahtumien tallentamiseksi. Tämä antaa järjestelmänvalvojille mahdollisuuden tunnistaa mahdolliset luvattomat käyttöyritykset.
4.1.1.3	Varmista, että auditointi on käytössä prosesseille, jotka käynnistyvät ennen auditd:tä	2	K	A	Määritä grub2 niin, että prosessit, jotka voivat olla auditoitavissa, voidaan auditoida jopa ennen auditd:n käynnistymistä. Tämä on välttämätöntä, jotta mahdollista haitallista toimintaa ei jää huomaamatta.
4.1.1.4	Varmista, että audit_backlog_limit on riittävä	2	K	A	Järjestelmässä audit-tapahtumat tallennetaan puskurijonoon. Parametri "audit_backlog_limit" määrittää tämän jonon maksimikoon. Jos jono ylittää tämän rajan, audit-tapahtumat menetetään, mikä voi johtaa mahdollisen haitallisen toiminnan jäämiseen huomaamatta.
4.1.2	Konfiguroi tietojen säilytys				
4.1.2.1	Varmista, että auditointilokin tallennustila on konfiguroitu	2	K	A	Määritä audit-lokin maksimikoko. Kun loki saavuttaa maksimikoon, se siirretään ja aloitetaan uusi lokitiedosto. On tärkeää määrittää lokitiedostoille sopiva koko, jotta ne eivät vaikuta järjestelmään ja jotta audit-tietoja ei menetetä.
4.1.2.2	Varmista, että auditointilokeja ei poisteta automaattisesti	2	K	A	max_log_file_action -asetus määrittää, miten toimia, kun audit-lokitiedosto saavuttaa maksimikokonsa. Arvolla keep_logs lokitiedostot pyörivät, mutta vanhoja ei koskaan poisteta. Erityisen turvallisissa ympäristöissä pitkän audit-historian säilyttämisen hyödyt ovat suuremmat kuin sen tallennuskustannukset.

Nro	Suositus	T	K	S	Kommentti
4.1.2.3	Varmista, että järjestelmä poistetaan käytöstä, kun auditointilokit ovat täynnä	2	K	A	Auditd-daemoni voidaan konfiguroida sammuttamaan järjestelmän, kun auditoinnin lokit ovat täynnä. On erilaisia toimintoja määrittämään järjestelmän käyttäytyminen, kun levytila vähenee. Korkean turvallisuuden ympäristöissä luvattoman käytön havaitsemisen riski ylittää järjestelmän saatavuuden edun. Mikäli asetus on määritelty sammuttamaan järjestelmä, se tekee niin kun levytila loppuu.
4.1.3	Konfiguroi auditd-säännöt				
4.1.3.1	Varmista, että järjestelmänvalvojan toiminnan laajuuden muutokset (sudoers) kerätään	2	K	A	Tarkkaillaan järjestelmänvalvojien toimintasovelluksen muutoksia. Kun järjestelmä on määritetty siten, että järjestelmänvalvojien on kirjauduttava sisään ensin itsenään ja sitten käytettävä sudo-komentoa, muutosten seuraaminen on mahdollista. Muutokset /etc/sudoers- ja /etc/sudoers.d-tiedostoissa voivat viitata luvattomaan muutokseen järjestelmänvalvojien toimintalaajuudessa.
4.1.3.2	Varmista, että toiminnot toisena käyttäjänä kirjataan aina	2	K	A	Sudo mahdollistaa käyttäjille tilapäiset laajennetut oikeudet suorittaa toimintoja. On tärkeää kirjata nämä toiminnot auditointia varten, jotta voidaan varmistaa, ettei luvattomia komentoja ole suoritettu.
4.1.3.3	Varmista, että sudo-lokitiedostoa muuttavat tapahtumat kerätään	2	K	A	Seuraa sudo-lokitiedostoa. Jos järjestelmä on määritetty estämään "su"-komennon käyttö ja vaatimaan ylläpitäjien käyttöön ottoa ja sudo-komentojen käyttöä, kaikki ylläpitäjän toiminnot kirjataan /var/log/sudo.log-tiedostoon. Muutokset tässä tiedostossa osoittavat, että ylläpitäjä on suorittanut komennon tai että lokitiedostoa on manipuloitu.
4.1.3.4	Varmista, että päivämäärän ja ajan muutoksia koskevat tapahtumat kerätään	2	K	A	Järjestelmässä ajan muutosten seuranta on olennaista turvallisuuden varmistamiseksi. Tapahtumien kerääminen, jotka vaikuttavat järjestelmän päivämäärään tai aikaan, voi paljastaa mahdollisia turvallisuusriskejä. On suositeltavaa merkitä nämä auditointitietueet ainutlaatuisilla tunnisteilla, jotta ne voidaan helposti tunnistaa ja tarkastaa.
4.1.3.5	Varmista, että tapahtumat, jotka muokkaavat järjestelmän verkkoympäristöä, kerätään	2	K	A	Verkkoympäristön muutosten valvonta on keskeinen turvatoimi, jolla havaitaan epäautorisoituja muutoksia, jotka voivat vaikuttaa järjestelmän turvallisuuteen. Seurattavia kohteita ovat järjestelmän isäntänimen ja verkkotunnuksen muutokset sekä kriittiset verkkoasetustiedostot. Tämän seurannan avulla voidaan tunnistaa mahdolliset hyökkäykset ja ehkäistä väärinkäytöksiä, kuten virheellisiin palvelimiin ohjautumista. Auditoinnin tarkoituksenmukainen taggaus on tärkeää, jotta tietoturvatapahtumat voidaan jäljittää ja analysoida tehokkaasti.
4.1.3.6	Varmista, että etuoikeutettujen komentojen käyttö kerätään	2	K	A	Valvonta yksinoikeuksilla varustettujen komentojen käytöstä on tärkeää, sillä se auttaa tunnistamaan tilanteita, joissa tavalliset käyttäjät suorittavat oikeuksia vaativia toimintoja. Tämä voi olla merkki luvattomista yrityksistä päästä käsiksi järjestelmän suojattuihin osiin. Huomionarvoista on, että valvonta- ja korjaustoimet voivat vaikuttaa järjestelmän suorituskykyyn, erityisesti suurilla tiedostojärjestelmillä, ellei niitä ole asennettu noexec- tai nosuid-asennusvaihtoehdoilla. Ennen valvonta- tai korjaustoimien suorittamista on suositeltavaa tarkastaa, mitkä tiedostojärjestelmät tulevat olemaan skannauksen kohteena, ja tarvittaessa rajata suorituskyvyn heikentymisen välttämiseksi tiettyjä tiedostojärjestelmiä pois tarkistuksista.

Nro	Suositus	T	K	S	Kommentti
4.1.3.7	Varmista, että epäonnistuneet tiedostopääsy-yritykset kerätään	2	K	A	Valvonta epäonnistuneista yrityksistä päästä käsiksi tiedostoihin on tärkeää, koska se voi osoittaa, että joku yrittää luvattomasti päästä järjestelmään. Seuranta kohdistuu tiedostonkäsittelyyn liittyviin järjestelmäkutsuihin, kuten tiedostojen luomiseen, avaamiseen ja katkaisemiseen. Lokitietue kirjoitetaan vain, jos kaikki seuraavat ehdot täyttyvät: käyttäjä ei ole yksinoikeuksilla varustettu, kyseessä ei ole palveluprosessin tapahtuma, ja järjestelmäkutsu palauttaa joko EACCES (pääsy estetty) tai EPERM (muu pysyvä virhe). Tällainen toiminta voi viitata luvattomaan pääsyyn tai muihin turvallisuusongelmiin.
4.1.3.8	Varmista, että tapahtumat, jotka muokkaavat käyttäjä-/ryhmätietoja, kerätään	2	K	A	On tärkeää seurata käyttäjien ja ryhmien tietojen, kuten salasanojen ja vanhojen salasanojen, muokkaustapahtumia. Järjestelmässä valvottavia tiedostoja ovat /etc/group, /etc/passwd, /etc/gshadow, /etc/shadow ja /etc/security/opasswd. Seuranta kohdistuu näiden tiedostojen kirjoitusyrityksiin ja attribuuttimuutoksiin, kuten käyttöoikeuksiin, ja nämä tapahtumat merkitään lokitiedostoon tunnisteella "identity". Odottamattomat muutokset näissä tiedostoissa voivat viitata järjestelmän mahdolliseen kompromettoitumiseen ja luvattoman käyttäjän yritykseen peitellä toimintaansa tai vaarantaa lisää tilejä.
4.1.3.9	Varmista, että harkinnanvaraiset käyttöoikeuksien muutosilmoitukset kerätään	2	K	A	Valvonta tiedostojen käyttöoikeuksien, attribuuttien, omistajuuden ja ryhmän muutoksille on olennainen turvatoimi. Tämä osio sisältää parametreja, jotka seuraavat järjestelmäkutsuja liittyen tiedostojen käyttöoikeuksien ja attribuuttien muutoksiin. Seurantaan kuuluvat sellaiset komennot ja järjestelmäkutsut kuten chmod, chown, setxattr ja niiden eri muunnelmat, jotka vaikuttavat tiedostojen oikeuksiin, omistajuuteen ja attribuutteihin. Lokitietue kirjoitetaan vain ei-järjestelmäkäyttäjien toimesta ja daemon-prosesseja ei oteta huomioon. Kaikki lokitapahtumat merkitään tunnisteella "perm_mod". Muutokset tiedostojen attribuutteihin voivat varoittaa järjestelmänvalvojaa mahdollisista tunkeutumisyrityksistä tai käytäntörikkomuksista.
4.1.3.10	Varmista, että onnistuneet tiedostojärjestelmän liittämiset kerätään	2	K	A	Järjestelmänvalvontaa on tärkeä tehostaa seuraamalla ei-privilegioitujen käyttäjien harvinaisia mount-järjestelmäkutsuja, jotka viittaavat tiedostojärjestelmien kiinnittämiseen. Vaikka tämä voi ilmoittaa ulkoisen aseman käytöstä, se ei yksinään osoita datan siirtoa. Todisteet tiedonsiirrosta vaativat myös muiden tiedostonkirjoitusoperaatioiden seurantaa, mutta liiallinen seuranta voi ylittää lokitilan ja on suositeltavaa rajoittaa tarkkailu vain olennaisiin tapahtumiin.
4.1.3.11	Varmista, että istunnon aloitustiedot kerätään	2	K	A	On tärkeää valvoa käyttäjien istuntojen aloitus- ja lopetustapahtumia. Järjestelmät pitävät kirjaa aktiivisista käyttäjäistunnoista, sisään- ja uloskirjautumisista sekä järjestelmän käynnistys- ja sammutustapahtumista erityisissä lokitiedostoissa. Näitä lokitiedostoja tarkkailemalla järjestelmänvalvoja voi havaita poikkeavia kirjautumisia, jotka saattavat viitata luvattomiin tunkeutumisyrityksiin tai muihin epätavallisiin aktiviteetteihin. Kaikki tähän liittyvät tapahtumat merkitään tunnisteella "session" lokitiedostoihin.
4.1.3.12	Varmista, että kirjautumis- ja uloskirjautumistapahtumat kerätään	2	K	A	On olennaista seurata kirjautumis- ja kirjautumispoistumistapahtumia. Järjestelmänvalvojat voivat tunnistaa tietoturvauhkia, kuten brute force -hyökkäykset, tarkastelemalla lokitiedostoja, jotka pitävät kirjaa käyttäjien viimeisistä onnistuneista kirjautumisista sekä kirjautumisyritysten epäon-

Nro	Suositus	T	K	S	Kommentti
					nistumisista. Tämä valvonta auttaa järjestelmänvalvojaa havaitsemaan mahdolliset väärinkäytökset ja tietoturvarikkomukset.
4.1.3.13	Varmista, että käyttäjien tiedostojen poistotapahtumat kerätään	2	K	A	On tärkeää valvoa tiedostojen poisto- ja uudelleennimentapahtumia, joita ei-privilegoidut käyttäjät suorittavat. Järjestelmäkutsujen, kuten unlink ja rename, käyttö voi olla merkki siitä, että suojattuja tiedostoja poistetaan tai niiden attribuutteja muutetaan luvattomasti. Tällaisen toiminnan valvonta auttaa järjestelmänvalvojia tunnistamaan epäilyttävät toimet ja ryhtymään tarvittaviin toimenpiteisiin.
4.1.3.14	Varmista, että tapahtumat, jotka muokkaavat järjestelmän pakollisia pääsyoikeuksia, kerätään	2	E	A	Valvonta on tärkeää järjestelmän pakollisten pääsykontrollien (Mandatory Access Controls, MAC) muutosten osalta, erityisesti järjestelmissä, jotka käyttävät AppArmor-ohjelmistoa. Seuraamalla kirjoituspääsyä tai attribuuttien muutoksia /etc/apparmor/ ja /etc/apparmor.d/ hakemistoissa, järjestelmänvalvojat voivat havaita luvattomia yrityksiä muuttaa turvallisuuskonteksteja tai pääsykontrolleja. Tällaiset muutokset voivat vaarantaa järjestelmän eheyden, joten näiden tapahtumien valvonta on olennaista vahvan turvallisuuden ylläpitämiseksi. Jos käytössä on toinen MAC-järjestelmä, vastaavien hakemistojen muutoksia on valvottava samankaltaisesti.
4.1.3.15	Varmista, että onnistuneet ja epäonnistuneet chcon-komennon yritykset kirjataan	2	K	A	Valvontatietueiden luominen chcon-komennon onnistuneista ja epäonnistuneista käyttökerroista on olennainen osa käyttöjärjestelmän turvallisuutta. Chcon-komento on tarkoitettu tiedoston turvallisuuskontekstin muuttamiseen. Ilman näitä turvallisuus- ja tehtäväsidoskohtaisia auditointitietueita olisi vaikeaa perustaa, korreloida ja tutkia turvallisuuspoikkeamia tai tunnistaa vastuulliset henkilöt. Auditointitietueita voidaan tuottaa järjestelmän eri komponenteista, kuten moduuleista tai käytäntösuodattimista.
4.1.3.16	Varmista, että onnistuneet ja epäonnistuneet setfacl-komennon yritykset kirjataan	2	K	A	Järjestelmän tulee luoda valvontatietueita setfacl-komennon onnistuneista ja epäonnistuneista käyttökerroista. Setfacl on työkalu tiedostojen ja hakemistojen pääsynvalvontalistojen (Access Control Lists, ACLs) asettamiseen. Valvontatietueiden luominen mahdollistaa turvallisuuspoikkeamien perustamisen, korreloinnin ja tutkinnan, mikä on olennaista tapahtumiin liittyvien seikkojen selvittämisessä ja niistä vastuussa olevien henkilöiden tunnistamisessa. Valvontatietueita voidaan tuottaa järjestelmän eri komponenteista, kuten moduuleista tai käytäntösuodattimista.
4.1.3.17	Varmista, että onnistuneet ja epäonnistuneet chacl-komennon yritykset kirjataan	2	K	A	Valvontalokeihin tulee kirjata sekä onnistuneet että epäonnistuneet yritykset käyttää chacl-komentoa, joka muokkaa tiedostojen ja hakemistojen pääsyvalvontalistoja. Tämä komento on erityisesti tärkeä IRIX-yhteensopivuuden kannalta. Auditoinnin avulla voidaan tunnistaa mahdolliset tietoturvatapahtumat ja vastuussa olevat tahot. Valvontatietueet ovat osa tietojärjestelmän tietoturvakäytäntöjä ja niitä generoidaan järjestelmän eri osista.

Nro	Suositus	T	K	S	Kommentti
4.1.3.18	Varmista, että onnistuneet ja epäonnistuneet usermod-komennon yritykset kirjataan	2	K	A	On tärkeää, että järjestelmä tuottaa valvontalokitiedot käyttäjien onnistuneista ja epäonnistuneista yrityksistä käyttää usermod-komentoa. Tämä komento muuttaa käyttäjätilien tietoja järjestelmässä. Valvontalokien avulla voi olla mahdollista tunnistaa ja selvittää tietoturvaloukkauksiin liittyviä tapahtumia sekä määrittää vastuulliset tahot. Valvontalokit tuotetaan eri järjestelmän osista tietoturvapolitiikan ja organisatoristen tarpeiden mukaisesti.
4.1.3.19	Varmista, että ytimen moduulien lataaminen, purkaminen ja muokkaaminen kerätään	2	K	A	Järjestelmänvalvojien on tärkeää valvoa ytimen moduulien lataamista ja purkamista. Kaikki moduulien lataaminen, listaus ja riippuvuuksien tarkistaminen tapahtuu kmod:n kautta symbolisten linkkien avulla. Valvontaa varten järjestelmäkutsut kuten init_module, finit_module, delete_module, create_module ja query_module tulisi seurata. Mikä tahansa näiden toimintojen suoritus kirjataan valvontalokiin tunnisteella "modules". Valvonta on perusteltua, koska ilman seurantaa, mahdolliset luvattomat muutokset ytimen moduuleissa voisivat jäädä huomaamatta ja vaarantaa järjestelmän tietoturvan.
4.1.3.20	Varmista, että auditoinnin konfiguraatio on muuttumaton	2	K	A	Järjestelmän auditointi tulee asettaa muuttumattomaksi, jolloin auditointisääntöjä ei voi muokata auditctl-komennolla. Asetus "-e 2" lukitsee auditointijärjestelmän muuttumattomaan tilaan, ja muutoksia voi tehdä vain järjestelmän uudelleenkäynnistyksen yhteydessä. Tämän toiminnon perustelu on, että muuttumattomassa tilassa luvattomat käyttäjät eivät voi tehdä muutoksia auditointijärjestelmään, mikä voisi mahdollistaa haitallisen toiminnan peittämisen. Käyttäjät todennäköisesti huomaisivat järjestelmän uudelleenkäynnistyksen, mikä voisi hälyttää ylläpitäjiä mahdollisista luvattomista muutoksista auditointiin.
4.1.3.21	Varmista, että käynnissä oleva ja levylle tallennettu konfiguraatio on sama	2	K	M	Tarkista ja varmista, että järjestelmän auditointikonfiguraatio levyllä ja käynnissä oleva konfiguraatio ovat yhteneväiset. On mahdollista, että nämä asetukset eroavat toisistaan. Huomioi, että augenrules- ja auditctl-työkalujen rajoitusten vuoksi ei voida täysin taata, että sääntöjen lataaminen augenrules --load -komennolla lataa kaikki säännöt tai että käyttäjää informoidaan, mikäli sääntöjen lataamisessa ilmenee ongelmia. Konfiguraation eriävyydet käynnissä olevan ja levylle tallennetun asetuksen välillä voivat aiheuttaa odottamattomia ongelmia tai antaa väärän kuvan noudatettavista vaatimuksista. Siksi on tärkeää varmistaa, että konfiguraatiot ovat synkronissa ja vastaavat toisiaan.
4.1.4	Konfiguroi auditd-tiedostojen pääsy				
4.1.4.1	Varmista, että auditoinnin lokitiedostot ovat tilassa 0640 tai vähemmän sallivassa tilassa	2	K	A	Auditointilokit sisältävät tärkeitä tietoja järjestelmästä ja sen toiminnasta. Auditointitietojen lukuoikeuksien rajoittaminen on tärkeää, sillä niiden sisältämä tieto voi paljastaa järjestelmän konfiguraatiotietoja ja muita arkaluonteisia tietoja, mikä voisi vaarantaa järjestelmän luottamuksellisuuden.
4.1.4.2	Varmista, että vain valtuutetut käyttäjät omistavat auditointilokitiedostot	2	K	A	Auditointilokit sisältävät tärkeitä tietoja järjestelmästä ja sen toiminnasta. Vain valtuutettujen käyttäjien omistusoikeus varmistaa, ettei luvaton pääsy paljasta järjestelmän konfiguraatioita tai muita tietoja, jotka voisivat vaarantaa järjestelmän luottamuksellisuuden.

Nro	Suositus	T	K	S	Kommentti
4.1.4.3	Varmista, että vain valtuutetut ryhmät omistavat auditointilokitiedostot	2	K	A	Auditointilokit sisältävät tietoa järjestelmän toiminnoista ja aktiviteeteista. Valtuutettujen ryhmien rajoitettu omistusoikeus auttaa estämään tietoturvauhkia, sillä luvattomilla ei ole pääsyä tietoihin, jotka voisivat paljastaa järjestelmän konfiguraatioita tai muita arkaluonteisia tietoja.
4.1.4.4	Varmista, että auditoinnin lokitiedoston hakemisto on 0750 tai tiukempi	2	K	A	Auditointilokien hakemisto sisältää järjestelmän auditointiin liittyvät lokitiedostot. Auditointitieto koostuu kaikista tapahtumien kirjauksista, auditoinnin asetuksista ja raporteista, jotka ovat välttämättömiä järjestelmän toiminnan valvonnassa. Nämä tiedot on suojattava luvattomalta muokkaukselta tai poistolta, sillä komprometoituneet auditointitiedot tekevät järjestelmän toiminnan laillisen tarkastelun ja mahdollisesti haitallisen toiminnan todellisen alkuperän selvittämisen mahdottomaksi.
4.1.4.5	Varmista, että auditoinnin konfiguraatiotiedostot ovat 640 tai tiukemmassa tilassa	2	K	A	Auditoinnin konfiguraatiotiedostot määrittävät auditd:n toimintaa ja mitkä tapahtumat kirjataan. Luvaton pääsy näihin konfiguraatiotiedostoihin voi mahdollistaa valtuuttamattoman henkilöstön estää kriittisten tapahtumien auditoinnin. Virheelliset konfiguraatiot voivat johtaa kriittisten tapahtumien auditoinnin estymiseen tai järjestelmän suorituskyvyn heikkenemiseen ylikuormittamalla auditointilokit. Lisäksi auditointikonfiguraation virheellinen asetus voi vaikeuttaa tapahtumiin liittyvien tapausten tutkimista ja selvittämistä.
4.1.4.6	Varmista, että auditoinnin konfiguraatiotiedostot omistaa root	2	K	A	Nämä tiedostot määrittelevät auditd:n toimintaa ja sen, mitä tapahtumia auditoidaan. Mikäli valtuuttamattomilla on pääsy näihin tiedostoihin, he voivat estää kriittisten tapahtumien auditoinnin. Väärin konfiguroidut auditointitiedostot voivat estää kriittisten tapahtumien auditoinnin tai vaikuttaa järjestelmän suorituskykyyn kuormittamalla auditointilokia liikaa. Lisäksi konfiguraatiotiedostojen virheellinen asetus voi vaikeuttaa tapahtumiin liittyvien tapausten tutkimista ja selvittämistä.
4.1.4.7	Varmista, että auditoinnin konfiguraatiotiedostot kuuluvat ryhmälle root	2	K	A	Nämä tiedostot ohjaavat auditd-palvelun toimintaa ja määrittävät, mitä tapahtumia seurataan. Jos näihin tiedostoihin pääsevät käsiksi valtuuttamattomat henkilöt, he saattavat estää tärkeiden tapahtumien valvonnan. Väärin määritellyt auditointiasetustiedostot voivat estää kriittisten tapahtumien seurannan tai kuormittaa järjestelmän toimintaa ylikuormittamalla auditointilokia. Auditoinnin konfiguraatiotiedostojen väärä konfigurointi voi myös vaikeuttaa tapauksiin liittyvien tapahtumien tutkimista ja selvittämistä.
4.1.4.8	Varmista, että audit-työkalujen oikeudet ovat 755 tai tiukemmat	2	K	A	Auditointityökaluja ovat esimerkiksi valmistajien tarjoamat ja avoimen lähdekoodin auditointityökalut, joita tarvitaan järjestelmän toiminnan ja tapahtumalokien katsomiseen ja käsittelyyn. Tällaisia työkaluja voivat olla myös räätälöidyt kyselyt ja raporttien luontiohjelmat. Auditointitietojen suojaaminen sisältää käytössä olevien tarkastelu- ja käsittelytyökalujen tunnistamisen ja suojaamisen. Auditointityökalujen suojaaminen on tarpeen, jotta estetään luvattomat toimenpiteet auditointitiedoissa.

Nro	Suositus	T	K	S	Kommentti
4.1.4.9	Varmista, että audit-työkalut ovat rootin omistamia	2	K	A	Auditointityökaluja ovat muun muassa valmistajien tarjoamat ja avoimen lähdekoodin työkalut, joita tarvitaan järjestelmän toiminnan ja kirjattujen tapahtumien tarkastelemiseen ja käsittelyyn. Näihin työkaluihin kuuluvat myös mukautetut kyselyt ja raporttien generointityökalut. Auditointitietojen suojeluun kuuluu käytössä olevien tarkastelu- ja käsittelytyökalujen tunnistaminen ja suojaaminen. Auditointityökalujen suojelu on tarpeen luvattoman pääsyn ja toiminnan estämiseksi auditointitiedoissa.
4.1.4.10	Varmista, että audit-työkalut kuuluvat root-ryhmälle	2	K	A	Näitä työkaluja käytetään järjestelmän toiminnan ja kirjattujen tapahtumien tarkasteluun ja käsittelyyn, ja ne voivat olla sekä valmistajien tarjoamia että avoimen lähdekoodin työkaluja. Työkaluihin voivat kuulua myös räätälöidyt kyselyt ja raporttien luontityökalut. Auditointitietojen suojelu edellyttää niiden työkalujen tunnistamista ja suojelua, joita käytetään lokitietojen katseluun ja käsittelyyn. On tärkeää suojata auditointityökalut luvattomilta toimenpiteiltä, jotka kohdistuvat auditointitietoihin.
4.1.4.11	Varmista, että audit-työkalujen eheys suojataan kryptografisilla mekanismeilla	1	K	A	Varmista, että auditointityökalujen eheys suojataan käyttämällä kryptografisia mekanismeja. Auditointityökalut käsittävät muun muassa valmistajien tarjoamat ja avoimen lähdekoodin työkalut, jotka ovat tarpeen järjestelmän toiminnan ja tapahtumien tarkasteluun ja käsittelyyn sekä räätälöidyt kyselyt ja raporttien luontivälineet. Auditointityökalujen eheyden suojeleminen on kriittinen askel auditointitietojen eheyden varmistamiseksi. Hyökkääjät voivat vaihtaa auditointityökalut tai lisätä koodia olemassa oleviin työkaluihin piilottaakseen tai poistaakseen järjestelmän toimintaa lokitiedoista. Auditointityökalut tulisi varmentaa kryptografisesti, mikä mahdollistaa havaita, jos työkaluja on muutettu, manipuloitu tai vaihdettu. Esimerkkinä voidaan käyttää tiedostojen tiivistelaskentaa eli checksum-hahmoa.
4.2	Konfiguroi lokitus				
4.2.1	Konfiguroi journald				
4.2.1.1	Varmista, että journald on konfiguroitu lähettämään lokit etälokituskoneelle				
4.2.1.1.1	Varmista, että systemd-journal-remote on asennettu	1	E	A	Tämä ohjelmisto mahdollistaa lokitietojen lähettämisen etälokipalvelimelle tai niiden vastaanottamisen etäjärjestelmistä, mikä mahdollistaa lokitietojen keskitetyn hallinnan. Lokitietojen tallentaminen etäpalvelimelle suojaa niiden eheyttä paikallisilta hyökkäyksiltä. Jos hyökkääjä saavuttaa pääkäyttäjän oikeudet paikallisessa järjestelmässä, he voisivat muokata tai poistaa paikallisesti tallennettuja lokitietoja.

Nro	Suositus	T	K	S	Kommentti
4.2.1.1.2	Varmista, että systemd-journal-remote on konfiguroitu	1	E	M	Varmista, että systemd-journal-remote on määritetty. Tämä järjestelmä osana systemd-journaldia mahdollistaa lokitapahtumien lähettämisen kaukaiselle lokipalvelimelle tai viestien vastaanottamisen kaukaisista isäntäkoneista, mikä mahdollistaa keskitetyn lokinhallinnan. Lokitietojen tallentaminen kaukaiselle palvelimelle suojaa niitä paikallisilta hyökkäyksiltä. Jos hyökkääjä saa juuripääsyn paikallisjärjestelmään, he voisivat muokata tai poistaa paikallisesti tallennettuja lokitietoja.
4.2.1.1.3	Varmista, että systemd-journal-remote on käytössä	1	E	M	Varmista, että systemd-journal-remote on käytössä. Tämä komponentti mahdollistaa lokitietojen lähettämisen etäisäntäkoneelle ja vastaanottamisen sieltä systemd-journaldin kautta, mikä mahdollistaa keskitetyn lokinhallinnan. Lokitietojen etävarastointi suojaa niiden eheyttä paikallisilta hyökkäyksiltä. Jos hyökkääjä saa juurioikeudet paikalliseen järjestelmään, he voivat väärentää tai poistaa paikallisesti tallennettuja lokitietoja.
4.2.1.1.4	Varmista, että journald ei ole konfiguroitu vastaanottamaan lokeja etäasiakkaalta	1	E	A	Järjestelmän journald-komponentin ei tule olla määritetty vastaanottamaan lokitietoja muilta verkon laitteilta. On tärkeää varmistaa, että systemd-journal-remote-pakettia käytetään ainoastaan lokitietojen lähettämiseen eikä asiakasjärjestelmät toimi lokipalvelimina. Tämä saavutetaan poistamalla systemd-journal-remote.socket ja systemd-journal-remote.service -palvelut käytöstä, sillä asiakasjärjestelmän ei pidä toimia toiminnallisten rajojensa ulkopuolella palvelimen roolissa.
4.2.1.2	Varmista, että journald-palvelu on käytössä	1	E	A	Järjestelmäpalvelun systemd-journaldin tulee olla aktivoituna, jotta lokitapahtumien tallennus on mahdollista. Mikäli tämä palvelu ei ole määritetty käynnistymään järjestelmän käynnistyksen yhteydessä, järjestelmä ei tallenna lokitapahtumia, mikä voi johtaa tärkeiden tietojen menetykseen ja heikentää järjestelmän tarkastuskykyä.
4.2.1.3	Varmista, että journald on konfiguroitu puristamaan suuret lokitiedostot	1	E	A	Järjestelmälokitiedostojen journald-palvelun tulisi käyttää tiedostojen pakkaustoimintoa suurten lokitiedostojen hallitsemiseksi. Tämä estää liian suurten lokitiedostojen aiheuttaman levytilan loppumisen tai lokien muodostumisen hallitsemattoman suuriksi. Pakkaamattomat suuret lokitiedostot saattavat täyttää tiedostojärjestelmän odottamattomasti, mikä voi johtaa resurssien saatavuusongelmiin. Tiedostojen pakkaaminen ennen kirjoittamista auttaa ehkäisemään äkillisiä ja odottamattomia vaikutuksia tiedostojärjestelmään.
4.2.1.4	Varmista, että journald on konfiguroitu kirjoittamaan lokitiedostot pysyvälle levylle	1	E	A	Journald-palvelun tulee olla konfiguroitu tallentamaan lokitiedostot pysyvästi palvelimen levytilaan. Kun lokitiedot tallennetaan vain väliaikaiseen muistiin, ne katoavat järjestelmän uudelleenkäynnistyksen yhteydessä. Lokitietojen tallentaminen pysyvästi levylle varmistaa, että tiedot eivät katoa uudelleenkäynnistyksen yhteydessä, mahdollistaen tapahtumien jälkikäteisen rekonstruoinnin jopa järjestelmäkaatumisen tai uudelleenkäynnistyksen jälkeen. Tämä on tärkeää, koska se mahdollistaa järjestelmän toiminnan tai turvallisuuden kannalta merkittävien tapahtumien tutkimisen ja analysoinnin.

Nro	Suositus	T	K	S	Kommentti
4.2.1.5	Varmista, että journald ei ole konfiguroitu lähettämään lokeja rsyslogille	1	E	M	On suositeltavaa, että journald-palvelu säilyttää lokitiedot oman palvelunsa rajoissa eikä välitä niitä eteenpäin muille palveluille. Mikäli järjestelmän lokitietojen keruu on keskitetty journald-palvelulle, kaikkien lokitietojen tulisi pysyä tämän palvelun käsittelyssä. Tämä estää lokitietojen jakautumisen useiden eri lokitusmekanismien kesken, mikä voisi johtaa lokitietojen hallinnan hankaloitumiseen ja tietoturvariskien lisääntymiseen.
4.2.1.6	Varmista, että journaldin lokien rotaatio on konfiguroitu sivuston käytännön mukaisesti	1	E	M	Journaldin lokitiedostojen kiertämisen konfiguroinnin tulisi noudattaa organisaation käytäntöjä. Säännöllisen lokitiedostojen kierrätyksen avulla voidaan estää järjestelmän täyttyminen lokitiedoista tai lokitiedostojen kasvaminen liian suuriksi. Järjestelmän tiedostossa /etc/systemd/journald.conf määritellään, miten Journaldin tuottamat lokitiedostot tulisi kierrättää. Pienempien ja hallittavampien lokitiedostojen ylläpito helpottaa järjestelmänvalvojaa arkistoimaan nämä tiedostot toiseen järjestelmään ja vähentää aikaa, joka kuluu poikkeuksellisen suurten lokitiedostojen läpikäyntiin.
4.2.1.7	Varmista, että journaldin oletustiedostojen oikeudet on konfiguroitu	1	E	M	Journald-lokitiedostojen oletusoikeudet tulee konfiguroida huolella. Kun Journald luo järjestelmässä aiemmin olemattomia lokitiedostoja, tämä asetus määrittelee uusille tiedostoille asetettavat oikeudet. Asianmukaiset tiedosto-oikeudet ovat keskeisiä, sillä ne varmistavat, että arkaluonteiset tiedot arkistoidaan ja suojataan asianmukaisesti. Näiden oikeuksien asianmukainen määrittely on olennainen osa tietoturvan ylläpitoa, jotta voidaan varmistaa, että vain valtuutetut käyttäjät pääsevät käsiksi lokitietoihin.
4.2.2	Konfiguroi rsyslog				
4.2.2.1	Varmista, että rsyslog on asennettu	1	K	A	On suositeltavaa asentaa rsyslog-ohjelmisto sellaisiin ympäristöihin, joissa journald ei täytä operatiivisia vaatimuksia. Rsyslogin turvallisuutta parantavat ominaisuudet, kuten lokeja siirtävät yhteyspohjaiset (esim. TCP) protokollat, mahdollisuus tallentaa lokitietoja tietokantaformaatteihin ja lokitietojen salaus siirron aikana keskitetylle lokipalvelimelle, oikeuttavat tämän paketin asentamisen ja konfiguroinnin. Näin varmistetaan, että lokiaineisto siirtyy turvallisesti ja vaatimukset täyttäen, myös kun tarvitaan lisäominaisuuksia, joita journald ei tarjoa.
4.2.2.2	Varmista, että rsyslog-palvelu on käytössä	1	K	A	Kun rsyslog-paketti on asennettu, on tärkeää varmistaa, että palvelu on asetettu käynnistymään järjestelmän käynnistyessä. Mikäli rsyslog-palvelu ei ole otettu käyttöön käynnistettäessä, järjestelmä ei tallenna lokitapahtumia, mikä voi jättää kriittiset järjestelmätapahtumat dokumentoimatta ja vaikeuttaa järjestelmän valvontaa ja ongelmien jäljittämistä.
4.2.2.3	Varmista, että journald on konfiguroitu lähettämään lokit rsyslogille	1	E	M	Journaldin tallentamia lokitietoja voidaan säilyttää sekä väliaikaisesti että pysyvästi palvelimen paikallisessa tallennustilassa. Vaikka journald-lokit voidaan siirtää etäyhteyden kautta, rsyslogin käyttö tarjoaa yhdenmukaisen ja johdonmukaisen tavan kerätä ja siirtää lokitietoja. Jos rsyslog on valittu suosituksi tavaksi lokien kokoamiseen, kaikki järjestelmän lokitiedot tulisi toimittaa rsyslogille edelleen käsiteltäväksi.

Nro	Suositus	T	K	S	Kommentti
4.2.2.4	Varmista, että rsyslogin oletustiedostojen oikeudet on konfiguroitu	1	K	A	RSyslog luo uusia lokitiedostoja, joita ei vielä ole järjestelmässä, ja näille tiedostoille määriteltävät oikeudet on konfiguroitava huolellisesti. On tärkeää varmistaa, että lokitiedostojen käyttöoikeudet ovat oikein asetettuja herkän datan suojaamiseksi ja arkistoimiseksi. Järjestelmän laajuiset umask-asetukset voivat tiukentaa RSyslogin asetuksia vain, parantaen tiedostojen turvallisuutta. RSyslogin oma $umask-direktiivi voi myös muokata tiedostojen luontitilaa. Siksi on kriittistä varmistaa, että /etc/rsyslog.conf- ja /etc/rsyslog.d/*conf-tiedostoissa asetetut luontimoodit eivät heikennä turvallisuusasetuksia ja että FileCreateMode-direktiivi on määritetty ennen kuin yhtään tiedostoa luodaan.
4.2.2.5	Varmista, että lokitus on konfiguroitu	1	K	M	Lokitiedostojen konfigurointi on oleellinen toimi, johon kuuluu /etc/rsyslog.conf- ja /etc/rsyslog.d/*.conf-tiedostojen sääntöjen määrittäminen. Nämä säännöt ohjaavat, mihin tiedostoihin tietyn tyyppiset viestit tallennetaan. Lokitustiedot ovat merkittävä osa tietoturvatiedon keräämistä, sillä ne sisältävät tärkeitä tietoja kuten onnistuneet ja epäonnistuneet sukomentoyritykset, kirjautumisyritykset ja rootin kirjautumisyritykset.
4.2.2.6	Varmista, että rsyslog on konfiguroitu lähettämään lokit etälokituskoneelle	1	E	M	RSyslog tukee lokitapahtumien lähettämistä etäloki-isäntään, mahdollistaen keskitetyn lokien hallinnan. Lokitietojen tallentaminen etäisäntään suojaa lokien eheyttä paikallisilta hyökkäyksiltä. Mikäli hyökkääjä pääsee käsiksi juurikäyttäjän oikeuksiin paikallisesti, hän voisi vääristellä tai tuhota paikallisesti tallennetut lokitiedot.
4.2.2.7	Varmista, että rsyslog ei ole konfiguroitu vastaanottamaan lokeja etäasiakkaalta	1	K	A	RSyslog mahdollistaa viestien vastaanottamisen etäisänniltä, toimien näin lokipalvelimena. Asiakasjärjestelmien ei pitäisi kuitenkaan vastaanottaa tietoja muilta isänniltä. Jos asiakasjärjestelmä on konfiguroitu vastaanottamaan tietoja, muuttuu se palvelimeksi, toimien siten toiminnallisesti sille asetettujen rajojen ulkopuolella.
4.2.3	Varmista, että kaikilla lokitiedostoilla on asianmukaiset oikeudet ja omistajuus	1	K	A	Lokitiedostojen on oltava asianmukaisesti suojattuja oikeilla käyttöoikeuksilla ja omistajuudella, jotta arkaluontoiset tiedot ovat turvassa ja vain valtuutetuilla käyttäjillä tai ryhmillä on niihin pääsy. Tiedot monista palveluista kerääntyvät näihin tiedostoihin paikallisella tasolla, tai keskitetyn lokipalvelimen tapauksessa, myös muiden järjestelmien lokit. Lokitiedostot löytyvät yleensä hakemistosta /var/log/, mutta joskus sovellukset voidaan määrittää tallentamaan lokit muualle. Jos sovelluksesi tallentaa lokit muualle, varmista, että suoritat samat turvallisuustarkastukset myös siellä.
5	**Pääsy, tunnistus ja valtuutus**				
5.1	Aikaan perustuvien tehtäväajoittimien konfigurointi				
5.1.1	Varmista, että cron-daemon on käytössä ja käynnissä	1	K	A	Järjestelmässä on tarve suorittaa erilaisia ylläpitotehtäviä, mukaan lukien turvallisuuden valvontaan liittyviä toimintoja, ja näiden tehtävien ajastamiseen käytetään cron-palvelua. Vaikka käyttäjäkohtaisia ajastettuja tehtäviä ei olisikaan, järjestelmän omat huoltotehtävät tulee suorittaa, ja cron mahdollistaa näiden tehtävien ajastetun suorittamisen. On syytä huomioida, että jos ajastustehtäviin käytetään muita järjestelmiä, kuten systemd-ajastimia, tulee cron poistaa käytöstä ja korvaava ratkaisu varmistaa paikallisen turvallisuuskäytännön mukaisesti turvatuksi.

Nro	Suositus	T	K	S	Kommentti
5.1.2	Varmista, että /etc/crontab-tiedoston oikeudet on määritetty	1	K	A	Cronin omat tehtävät määritellään /etc/crontab-tiedostossa, ja on kriittistä, että vain järjestelmänvalvojalla (root-käyttäjällä) on omistajuus ja pääsy tähän tiedostoon. Tämä estää muiden käyttäjien kirjoitusoikeuden, joka mahdollistaisi heidän käyttöoikeuksiensa kohottamisen, ja lukuoikeuden, joka antaisi heille mahdollisuuden saada tietoa järjestelmän tehtävistä ja sitä kautta pääsyn laittomasti laajennettuihin käyttöoikeuksiin. Jos käytössä on jokin muu menetelmä tehtävien aikatauluttamiseen, kuten systemd-ajastimet, on suositeltavaa poistaa cron käytöstä ja turvata vaihtoehtoinen menetelmä paikallisen turvallisuuspolitiikan mukaisesti.
5.1.3	Varmista, että /etc/cron.hourly-tiedoston oikeudet on määritetty	1	K	A	On tärkeää, että /etc/crontab-tiedosto, joka vastaa tehtävien aikatauluttamisesta, suojataan asettamalla root omistajaksi ja rajoittamalla tiedoston käyttöoikeus ainoastaan omistajalle. Tämä varotoimi estää oikeudettomat käyttäjät muokkaamasta aikataulutettuja tehtäviä lisätäkseen heidän järjestelmäoikeuksiaan tai oppimasta järjestelmätehtävistä, mikä voisi johtaa luvattomaan pääsyyn.
5.1.4	Varmista, että /etc/cron.daily-tiedoston oikeudet on määritetty	1	K	A	On keskeistä, että ainoastaan rootilla on kyky muokata tai päästä käsiksi /etc/cron.daily-hakemistoon, joka on tarkoitettu päivittäisille cron-tehtäville, välttäen näin luvattomat muutokset tai pääsyn, jotka voisivat johtaa tietoturvaloukkauksiin.
5.1.5	Varmista, että /etc/cron.weekly-tiedoston oikeudet on määritetty	1	K	A	Viikoittaisten ajastettujen tehtävien eheyden varmistamiseksi vain juurikäyttäjällä tulee olla muokkaus- ja käyttöoikeus /etc/cron.weekly-hakemistoon, estäen näin oikeudettomat käyttäjät mahdollisesti hyväksikäyttämästä järjestelmää.
5.1.6	Varmista, että /etc/cron.monthly-tiedoston oikeudet on määritetty	1	K	A	Rajoittamalla /etc/cron.monthly -hakemiston muokkaus- ja katseluoikeudet yksinomaan root-käyttäjälle on elintärkeää järjestelmän turvallisuuden ylläpitämiseksi luvattomalta pääsyltä ja mahdolliselta käyttöoikeuksien laajentamiselta tavallisilta käyttäjiltä.
5.1.7	Varmista, että /etc/cron.d-tiedoston oikeudet on määritetty	1	K	A	Tiukka pääsykontrolli on tarpeen /etc/cron.d-hakemistolle, jotta vain root-käyttäjä voi hallita erikoistuneita cron-työkokoonpanoja, näin ollen turvaten järjestelmän luvattomalta käsittelyltä ja mahdollisilta tietoturvariskeiltä.
5.1.8	Varmista, että cron on rajoitettu valtuutetuille käyttäjille	1	K	A	Cron-työjen ajoitusten hallinta tulisi suorittaa käyttäen /etc/cron.allow-tiedostoa paremman turvallisuuden varmistamiseksi, jolloin vain erikseen sallitut käyttäjät pääsevät käsiksi palveluun, toisin kuin vähemmän turvallinen menetelmä käyttäen /etc/cron.deny-tiedostoa, joka voisi tahattomasti myöntää pääsyn.
5.1.9	Varmista, että at on rajoitettu valtuutetuille käyttäjille	1	K	A	Jotta voidaan varmistaa asianmukainen kontrolli siitä, kuka voi ajoittaa 'at'-tehtäviä, tulisi käyttää /etc/at.allow-tiedostoa määrittämään sallitut käyttäjät, tarjoten turvallisemman ja hallittavamman järjestelmän kuin /etc/at.deny:n varassa olo, joka voi olla altis huolimattomuusvirheille ja erehdyksille.
5.2	SSH-palvelimen konfigurointi				
5.2.1	Varmista, että /etc/ssh/sshd_config-tiedoston oikeudet on määritetty	1	E	A	/etc/ssh/sshd_config-tiedoston omistajuuden tulisi kuulua yksinomaan root-käyttäjälle sen suojelemiseksi luvattomilta muutoksilta käyttäjiltä, joilla ei ole asianmukaisia oikeuksia.
5.2.2	Varmista, että SSH:n yksityisen isäntäavaimen tiedostojen oikeudet on määritetty	1	E	A	On tärkeää ylläpitää SSH:n yksityisiä isäntäavaimia turvallisesti tarkoin oikeusasetuksin, koska luvaton pääsy näihin avaimiin voisi johtaa isännän identiteetin väärinkäyttöön.

Nro	Suositus	T	K	S	Kommentti
5.2.3	Varmista, että SSH:n julkisen isäntäavaimen tiedostojen oikeudet on määritetty	1	E	A	SSH-palveluiden turvallisuus riippuu julkisten isäntäavaintiedostojen asianmukaisesta määrittelystä, suojaten niitä luvattomilta muutoksilta, jotka voisivat häiritä todennusprosesseja.
5.2.4	Varmista, että SSH-pääsy on rajoitettu	1	E	A	Paranna järjestelmän turvallisuutta tarkasti ohjaamalla käyttäjien ja ryhmien oikeuksia SSH-yhteyksille, mukaan lukien isäntäkohtaiset rajoitukset varmistaaksesi, että vain sallitut henkilöt voivat muodostaa yhteyden.
5.2.5	Varmista, että SSH:n lokitustason asetus on sopiva	1	E	A	Säädä SSH LogLevel INFO-tasolle perus kirjautumisen seurantaan tai VERBOSE-tasolle yksityiskohtaiseen valvontaan pääsystä ja avaimen käytöstä, mikä on tärkeää tapahtumien käsittelyssä ja perintäjärjestelmissä, välttäen DEBUG-tasoa sen tuottaman suuren määrän tarpeettoman tiedon vuoksi.
5.2.6	Varmista, että SSH PAM on käytössä	1	E	A	Aktivoimalla UsePAM SSH-asetuksissa käynnistetään PAM-pohjainen todennus, tarjoten laajennettuja tarkistuksia istuntojen ja käyttäjätilien aikana ja mahdollistaen ehdolliset käyttöoikeusparametrit, varmistaen hallitut ympäristöasetukset käyttäjän kirjautuessa sisään.
5.2.7	Varmista, että SSH:n root-kirjautuminen on poistettu käytöstä	1	E	A	Säätämällä PermitRootLogin asetuksen estämään root-käyttöoikeuden, se edellyttää, että ylläpitäjät todentavat henkilökohtaisilla tileillään ennen root-oikeuksien saamista, mikä vahvistaa jäljitettävyyttä ja vastuullisuutta turvallisuusprotokollissa.
5.2.8	Varmista, että SSH HostbasedAuthentication on poistettu käytöstä	1	E	A	Kytkeessä pois HostbasedAuthentication SSH:ssä poistetaan mahdollisuus todentamiseen vanhojen luotettujen isäntätiedostojen kautta, tarjoten ylimääräisen turvatoimenpiteen olemassa olevien .rhosts-rajoitusten lisäksi /etc/pam.conf-tiedostossa.
5.2.9	Varmista, että SSH PermitEmptyPasswords on poistettu käytöstä	1	E	A	Poistamalla käytöstä PermitEmptyPasswords-asetuksen varmistetaan, ettei SSH hyväksy kirjautumisia salasanattomilta tileiltä, mikä parantaa turvallisuutta luvattomilta pääsyltä.
5.2.10	Varmista, että SSH PermitUserEnvironment on poistettu käytöstä	1	E	A	Ottamalla pois käytöstä SSH:n PermitUserEnvironment-ominaisuuden, se estää käyttäjiä muokkaamasta ympäristön asetuksia, jotka voisivat vaarantaa turvallisuustoimet.
5.2.11	Varmista, että SSH IgnoreRhosts on käytössä	1	E	A	SSH:n IgnoreRhosts-asetuksen käyttöönotto varmistaa, että .rhosts ja .shosts tiedostoja ei käytetä, vaatien käyttäjiä todentamaan salasanalla.
5.2.12	Varmista, että SSH X11-tunnelointi on poistettu käytöstä	1	E	A	SSH:n X11-välityksen poistaminen käytöstä pienentää etä-X11-palvelimien tietoturvariskiä estämällä X11-liikenteen tunneloinnin, vaikka käyttäjät voivatkin asettaa omat välityspalvelimensa.
5.2.13	Varmista, että käytössä on vain vahvat salausalgoritmit	1	E	A	Rajoita SSH-viestintä vahvoihin, hyväksyttyihin salauksiin, jotka täyttävät FIPS 140-2 standardit, kuten aes256-ctr, taatakseen tietojen eheyden ja luottamuksellisuuden kryptografisten haavoittuvuuksien varalta.
5.2.14	Varmista, että käytössä on vain vahvat MAC-algoritmit	1	E	A	On tärkeää vaatia vahvojen MAC-algoritmien, kuten hmac-sha2-256 ja hmac-sha2-512, käyttöä SSH-yhteyksissä suojatakseen haavoittuvuuksilta ja ylläpitääkseen tietojen eheyttä.
5.2.15	Varmista, että käytössä on vain vahvat avaimenvaihtoalgoritmit	1	E	A	Kryptografisissa avainvaihdoissa on olennaista etusijalle asettaa vahvat algoritmit, jotta yhteydet pysyvät turvattuina ja välittömien hyökkäysten riski pienenee. Suosituimpia protokollia ovat ecdh-sha2-muunnelmat ja turvallista SHA-hashausta käyttävät diffie-hellman-ryhmät, jotka ovat linjassa organisaation käytäntöjen ja FIPS-ohjeiden kanssa.

Nro	Suositus	T	K	S	Kommentti
5.2.16	Varmista, että SSH AllowTcpForwarding on poistettu käytöstä	2	E	A	SSH:n käyttö porttiohjaukseen tarjoaa salausetuja, mutta luo myös merkittäviä turvallisuusuhkia mahdollistamalla luvattomia pääsykohtia. On suositeltavaa poistaa tämä ominaisuus käytöstä, jotta estetään hyväksikäyttö laittomiin tarkoituksiin, kuten tietojen luvattomaan siirtoon, vaikka tietyissä liiketoimintaympäristöissä nämä tunnelit ovatkin olennaisia sääntelyn mukaisuuden varmistamiseksi ilman tarvetta muuttaa sovellusinfrastruktuuria.
5.2.17	Varmista, että SSH:n varoitusbanneri on konfiguroitu	1	E	A	SSH-varoituskyltin asettaminen toimii ilmoituksena etäkäyttäjille politiikasta ja mahdollisista laittoman pääsyn oikeudellisista seuraamuksista, mikä voi tukea oikeustoimia luvattomia käyttäjiä vastaan.
5.2.18	Varmista, että SSH MaxAuthTries on asetettu 4:ään tai vähemmän	1	E	A	SSH:ssä MaxAuthTries-vaihtoehto rajoittaa sisäänkirjautumisyritysten määrää kullakin yhteydellä, toimien suojana brute force -hyökkäyksiä vastaan. Suositus on asettaa tämä kynnys arvoon 4 tai alle, organisaation määritelmiä noudattaen.
5.2.19	Varmista, että SSH MaxStartups on konfiguroitu	1	E	A	SSH:n MaxStartups-direktiivin konfigurointi rajoittaa yhtäaikaisten, tunnistautumattomien yhteyksien määrää, lieventäen palvelunestoriskejä hallitsemalla sisäänkirjautumisyritysten virtaa ja varmistaen SSH-daemonin saatavuuden.
5.2.20	Varmista, että SSH MaxSessions on asetettu 10:een tai vähemmän	1	E	A	MaxSessions-asetus määrittelee rajoituksen samanaikaisten SSH-istuntojen määrälle kullakin yhteydellä, mikä on tärkeää palvelukatkosten torjumiseksi ja sshd-kirjautumisten toiminnallisen eheyden säilyttämiseksi.
5.2.21	Varmista, että SSH LoginGraceTime on asetettu yhteen minuuttiin tai vähemmän	1	E	A	LoginGraceTime-asetus määrittää sallitun aikavälin SSH-palvelimen todennukselle, mikä vähentää onnistuneiden voimaperäisten hyökkäysten riskiä rajoittamalla käytettävissä olevaa aikaa ja samanaikaisten todentamattomien yhteysyritysten määrää.
5.2.22	Varmista, että SSH:n joutenoloaikaintervalli on konfiguroitu	1	E	A	SSH:n joutoajan aikakatkaisuasetusten, ClientAliveInterval ja ClientAliveCountMax, avulla voidaan katkaista toimettomat yhteydet resurssien liikakäytön ehkäisemiseksi ja potentiaalisten DDoS-hyökkäysten riskin minimoimiseksi asettamalla aikakatkaisuja vastaamattomille SSH-istunnoille.
5.3	Käyttöoikeuksien kohottamisen konfigurointi				
5.3.1	Varmista, että sudo on asennettu	1	K	A	sudo on välttämätön komentojen suorittamiseen ylivaltaisena tai muiden käyttäjien oikeuksin, turvallisuuskäytäntöjen mukaisesti. Se tarjoaa laajennettavan arkkitehtuurin mukauttamiseen ja tukee kolmannen osapuolen käytäntöjä ja lokitusta, autentikointivaatimuksilla ja aikarajoilla, jotka on määritelty käytännössä.
5.3.2	Varmista, että sudo-komennot käyttävät pty:tä	1	K	A	On suositeltavaa määrittää sudo toimimaan ainoastaan pseudo-terminaalin kautta, jotta voidaan estää hyökkääjien kyky ajaa taustaprosesseja, jotka säilyvät alkuperäisen ohjelman suorituksen jälkeen. Sudo-asetusten muokkaamisessa on noudatettava varovaisuutta, sillä virheelliset muutokset voivat poistaa sudon toiminnasta.
5.3.3	Varmista, että sudo-lokitiedosto on olemassa	1	K	A	Sudon määrittäminen käyttämään mukautettua lokitiedostoa tehostaa sudo-oikeuksilla suoritettujen komentojen valvontaa. Sudon asetusten muokkauksessa on olennaista käyttää visudoa, jotta sudon toiminta ei keskeydy.
5.3.4	Varmista, että käyttäjien on annettava salasana valtuutuksen korottamiseksi	2	K	A	On välttämätöntä määrittää käyttöjärjestelmä niin, että käyttäjien on syötettävä salasanansa käyttöoikeuksien korottamiseen, varmistaen toimivallan pysyminen käyttöoikeuksien rajoissa ja turvallisuuden ylläpitäminen. Tämä saattaa vaikuttaa

Nro	Suositus	T	K	S	Kommentti
					automatisoituihin toimenpiteisiin, jotka tarvitsevat laajennettuja oikeuksia.
5.3.5	Varmista, että valtuutuksen korottamisen uudelleenautentikointi ei ole globaalisti poistettu käytöstä	1	K	A	Järjestelmän on vaadittava, että käyttäjä vahvistaa henkilöllisyytensä uudelleen pyrkiessään kasvattamaan pääsyn tasoaan, mikä auttaa estämään luvattoman resurssien käytön tai toimien suorittamisen ylittäen heidän käyttöoikeutensa.
5.3.6	Varmista, että sudon autentikointiaika on oikein konfiguroitu	1	K	A	Sudon todennustietojen välimuistiominaisuus, joka oletusarvoisesti säilyttää tunnistetiedot lyhyen ajan, on sovitettava yhteen organisaation turvallisuuskäytäntöjen kanssa, jotta voidaan pienentää luvattoman korotetun käyttöoikeuden riskiä.
5.3.7	Varmista, että pääsy su-komentoon on rajoitettu	1	K	A	Rajoittamalla 'su'-komennon pääsyä vain valituille käyttäjäryhmille ja kannustamalla 'sudo':n käyttöön, ylläpitäjät voivat parantaa käyttöoikeuksien laajennuksen valvontaa ja saada yksityiskohtaisen lokitustiedon. Tämä lähestymistapa on turvallisempi verrattuna 'su':hun, joka kirjaa vain ohjelman käytön, ei erillisiä komentoja, vahvistaen näin turvallisuuskäytäntöjä.
5.4	Autentikointimoduulien (PAM) konfigurointi				
5.4.1	Varmista, että salasanan luontivaatimukset on määritetty	1	K	A	Tiukkojen salasanakäytäntöjen toteuttaminen pam_pwquality.so:n kautta varmistaa vahvojen salasanojen luomisen, yhdistäen pituus- ja merkkityyppivaatimukset. Tämä lähestymistapa parantaa merkittävästi järjestelmän turvallisuutta brute force -yrityksiä vastaan.
5.4.2	Varmista, että lukitus epäonnistuneiden salasanojen yritysten jälkeen on määritetty	1	K	A	Järjestelmän lukitseminen määritetyn määrän epäonnistuneiden kirjautumisyritysten jälkeen, kuten määritelty /etc/security/faillock.conf-tiedostossa, on avainasemassa suojautumisessa murtautumisyrityksiä vastaan. Näiden parametrien huolellinen säätäminen ja testaaminen ovat välttämättömiä varmistamaan, että ne noudattavat organisaation käytäntöjä ja välttääkseen tahattoman pääsyn estämisen.
5.4.3	Varmista, että salasanan uudelleenkäyttö on rajoitettu	1	K	A	Järjestelmän konfigurointi rajoittamaan salasanan uudelleenkäyttöä, seuraamalla viittä viimeistä salasanaa /etc/security/opasswd-tiedostossa, auttaa suojaamaan salasana-arvauksilta hyökkääjien toimesta.
5.4.4	Varmista, että salasanan hajautusalgoritmi on ajantasalla nykyisten standardien kanssa	1	K	A	Siirtyminen yescrypt-salasanan hajautusalgoritmiin parantaa turvallisuutta tekemällä hyökkääjien salasanojen murtamisesta vaikeampaa. Olemassa olevien käyttäjätilien on päivitettävä salasanansa hyötyäkseen tästä parannetusta suojauksesta, ja tämä päivitys koskee vain paikallisesti määriteltyjä käyttäjätilejä.
5.4.5	Varmista, että kaikki nykyiset salasanat käyttävät konfiguroitua hajautusalgoritmia	1	K	M	On tärkeää varmistaa, että kaikki käytössä olevat salasanat noudattavat uusinta hajautusalgoritmia turvallisuuden ylläpitämiseksi. Kuitenkin ylläpitäjien tulee olla tietoisia siitä, että laajojen salasanapäivitysten vaatiminen saattaa väliaikaisesti kuormittaa järjestelmän resursseja korkean CPU-kysynnän vuoksi.
5.5	Käyttäjätilit ja Ympäristö				
5.5.1	Aseta Shadow Password Suite -parametrit				

Nro	Suositus	T	K	S	Kommentti
5.5.1.1	Varmista, että salasanan vaihdon minimipäivät on määritetty	1	K	A	Asettamalla PASS_MIN_DAYS vähintään yhdeksi päiväksi /etc/login.defs-tiedostossa varmistetaan, että käyttäjät eivät voi vaihtaa salasanojaan liian usein, mikä on yleinen tapa kiertää salasanan uudelleenkäyttö- ja historiasääntöjä, näin ollen ylläpitäen näiden turvatoimien eheyttä.
5.5.1.2	Varmista, että salasanan vanhentuminen on 365 päivää tai vähemmän	1	K	A	Asettamalla PASS_MAX_DAYS enintään vuoden (365 päivän) ajanjakson mukaiseksi /etc/login.defs-tiedostossa rajoitetaan tunnistetietojen mahdollista väärinkäyttöä lyhentämällä salasanojen käyttöikää. Tämä strategia kaventaa mahdollisten brute force -hyökkäysten ikkunaa, varmistaen paremmat turvallisuuskäytännöt.
5.5.1.3	Varmista, että salasanan vanhentumisvaroituspäivät on 7 tai enemmän	1	K	A	Asettamalla PASS_WARN_AGE varoittamaan käyttäjiä vähintään 7 päivää ennen salasanan vanhenemista kannustetaan vahvempien, turvallisempien salasanojen luomiseen tarjoamalla riittävästi aikaa harkintaan, näin vähentäen kiireisten, vähemmän turvallisten valintojen riskiä.
5.5.1.4	Varmista, että inaktiivinen salasanan lukitus on 30 päivää tai vähemmän	1	E	A	Käyttäjätilien lukitsemisen toteuttaminen enintään 30 päivän toimettomuuden jälkeen salasanan vanhentumisen jälkeen on olennaista turvallisuusriskien lieventämiseksi, jotka liittyvät valvomattomiin tileihin.
5.5.1.5	Varmista, että kaikkien käyttäjien viimeisin salasanan vaihtopäivä on menneisyydessä	1	K	A	On tärkeää varmistaa, että jokaisen käyttäjän viimeisin salasanan muutospäivämäärä on menneisyydessä, jotta voidaan ylläpitää salasanan vanhentumiskäytäntöjen eheyttä ja estää näiden turvatoimien kiertäminen.
5.5.2	Varmista, että järjestelmätilit ovat turvattuja	1	K	A	Järjestelmätilien turvaaminen määrittämällä ne käyttämään 'nologin'-kuorta varmistaa, ettei niitä voida käyttää komentojen suorittamiseen, mikä lisää ylimääräisen turvallisuustason vakiotapaan määrittää epäkelpoja salasanoja.
5.5.3	Varmista, että root-tilin oletusryhmä on GID 0	1	K	A	Asettamalla GID 0 oletusryhmäksi root-käyttäjätilille autetaan estämään rootin luomien tiedostojen tahattoman käytettävyyden ei-valtuutetuille käyttäjille, ylläpitäen korkeampaa järjestelmän turvallisuustasoa.
5.5.4	Varmista, että oletuskäyttäjän umask on 027 tai tiukempi	1	K	A	Tiukan umask-asetuksen varmistaminen (027 tai tiukempi) on tärkeää tiedostojen ja hakemistojen turvallisen luomisen kannalta. Tämä asetus voidaan toteuttaa joko globaalisti tai käyttäjäkohtaisesti, vaikuttaen käyttöoikeuksiin ja parantaen turvallisuutta. On tärkeää tietää, että USERGROUPS_ENAB:n määrittely /etc/login.defs-tiedostossa vaikuttaa useradd- ja userdel-komentojen toimintaan, erityisesti ryhmäoikeuksien ja hallinnan osalta.
5.5.5	Varmista, että oletuskäyttäjän komentotulkin aikakatkaisu on 900 sekuntia tai vähemmän	1	K	A	Komentotulkin aikakatkaisun konfigurointi 900 sekuntiin tai vähemmän koko järjestelmän kattavissa komentotulkin asetuksissa, kuten /etc/profile, /etc/profile.d/*.sh ja /etc/bash.bashrc, on tärkeää turvallisuuden parantamiseksi automaattisesti päättämällä jouten olevat käyttäjäistunnot, mikä vähentää luvattoman pääsyn riskejä ja hallitsee tehokkaasti järjestelmän resursseja. TMOUT:n asettaminen vain luku -muotoon lisää turvallisuutta estämällä ei-toivotut muutokset.
6	**Järjestelmän ylläpito**				
6.1	Järjestelmän Tiedostojen Oikeudet				
6.1.1	Varmista, että /etc/passwd-tiedoston oikeudet on määritetty	1	K	A	On olennaista varmistaa /etc/passwd-tiedoston suojaus luvattomilta muutoksilta, sillä tämä tiedosto sisältää tärkeitä käyttäjätilitietoja, jotka ovat tarpeellisia useiden järjestelmätyökalujen toiminnalle. Oikeanlaisen tiedostojen käyttöoikeuksien

Nro	Suositus	T	K	S	Kommentti
					ylläpitäminen on välttämätöntä järjestelmän eheyden ja toimivuuden kannalta.
6.1.2	Varmista, että /etc/passwd- -tiedoston oikeudet on määritetty	1	K	A	/etc/passwd- -tiedoston turvaaminen on välttämätöntä, sillä se sisältää tärkeitä varmuuskopioituja käyttäjätilitietoja. On keskeistä varmistaa, että tämä tiedosto ei ole luvattomien käyttäjien saavutettavissa, ottaen huomioon, että sen käyttöoikeudet saattavat muuttua joko vahingossa tai tahallisesti.
6.1.3	Varmista, että /etc/group-tiedoston oikeudet on määritetty	1	K	A	/etc/group-tiedoston suojaaminen on tärkeää estääkseen luvattomat muutokset, sallien vain root-käyttäjien muokata sitä samalla varmistaen, että se pysyy luettavana ei-valtuutetuille ohjelmille, ylläpitäen näin sekä järjestelmän turvallisuutta että toiminnallisuutta.
6.1.4	Varmista, että /etc/group- -tiedoston oikeudet on määritetty	1	K	A	/etc/group- -tiedoston turvaaminen on elintärkeää luvattomien muutosten estämiseksi. Tämä tiedosto sisältää tärkeitä varmuuskopioituja tietoja järjestelmän ryhmistä, ja sen suojan varmistaminen on avainasemassa järjestelmän eheyden ja turvallisuuden ylläpitämiseksi.
6.1.5	Varmista, että /etc/shadow-tiedoston oikeudet on määritetty	1	K	A	/etc/shadow-tiedoston tiukkojen käyttöoikeuksien varmistaminen on tärkeää, koska se sisältää arkaluonteista tietoa, kuten salasanojen hajautuksia ja tiliturvallisuuden tietoja. Asianmukaisten turvatoimien toteuttaminen on välttämätöntä luvattoman pääsyn estämiseksi, mikä voisi johtaa salasanojen murtamiseen ja tilien hyväksikäyttöön.
6.1.6	Varmista, että /etc/shadow- -tiedoston oikeudet on määritetty	1	K	A	On välttämätöntä varmistaa tiukat turvatoimet /etc/shadow--tiedostolle sen sisältämien arkaluontoisten tietojen, kuten varmuuskopioitujen salasanojen hajautusten ja tilin turvatietojen, vuoksi. Sen käyttöoikeuksien aktiivinen ylläpito on tarpeen mahdollisten tietoturvaloukkausten estämiseksi luvattoman pääsyn seurauksena.
6.1.7	Varmista, että /etc/gshadow-tiedoston oikeudet on määritetty	1	K	A	/etc/gshadow-tiedoston suojaaminen on olennaisen tärkeää sen sisältämien arkaluontoisten tietojen, kuten ryhmien salasanojen hajautusten ja hallinnollisten yksityiskohtien, vuoksi. Tiukan käyttöoikeuksien hallinnan varmistaminen on välttämätöntä potentiaalisten tietoturvaloukkausten estämiseksi, jotka voisivat johtua luvattomasta pääsystä ja salasanamurtamisyrityksistä.
6.1.8	Varmista, että /etc/gshadow--tiedoston oikeudet on määritetty	1	K	A	On kriittistä varmistaa /etc/gshadow- -tiedoston turvallisuus sen sisältämien arkaluontoisten varmuuskopiotietojen, kuten ryhmien salasanojen hajautusten ja turvatietojen, vuoksi. Tämän tiedoston tiukkaan käyttöoikeuksien hallintaan kiinnittäminen on tarpeen mahdollisten turvallisuusriskien välttämiseksi, jotka voivat johtua luvattomasta pääsystä.
6.1.9	Varmista, ettei kaikkien kirjoitettavissa olevia tiedostoja ole olemassa	1	K	A	Maailmanlaajuisesti kirjoitettavien tiedostojen esiintyminen Unix-pohjaisessa järjestelmässä aiheuttaa suuren turvallisuusriskin niiden avoimen käyttömahdollisuuden vuoksi, joka sallii minkä tahansa käyttäjän muokata näitä tiedostoja. Tällaisten tiedostojen poistaminen on välttämätöntä järjestelmän turvallisuuden suojaamiseksi ja mahdollisten kompromissien tai syvempien järjestelmähaavoittuvuuksien merkkien estämiseksi.

Nro	Suositus	T	K	S	Kommentti
6.1.10	Varmista, ettei omistamattomia tiedostoja tai hakemistoja ole olemassa	1	K	A	On tärkeää varmistaa, että kaikilla tiedostoilla ja hakemistoilla on asianmukainen omistaja järjestelmän turvallisuuden kannalta. Omistamattomat tiedostot, jotka usein jäävät jäljelle käyttäjien poistamisen jälkeen, saattavat vahingossa antaa liiallisia oikeuksia uusille käyttäjille, jotka on määritetty samoille tunnuksille, johtaen tahattomiin tietoturva-aukkoihin.
6.1.11	Varmista, ettei ryhmättömiä tiedostoja tai hakemistoja ole olemassa	1	K	A	Kaikkien tiedostojen ja hakemistojen oikean ryhmittelyn säännöllinen varmistaminen on tärkeää järjestelmän turvallisuuden ylläpitämiseksi. Ryhmittämättömät tiedostot, jotka yleensä jäävät jäljelle käyttäjien tai ryhmien poistamisen jälkeen, voivat vahingossa tarjota liikaa käyttöoikeuksia uusille käyttäjille, jotka on määritetty samoille tunnuksille, ja johtaa potentiaalisiin tietoturva-aukkoihin.
6.1.12	Tarkasta SUID-suoritettavat tiedostot	1	K	M	SUID-suoritettavien tiedostojen perusteellinen tarkastus on tärkeää järjestelmän turvallisuuden kannalta. Nämä tiedostot, jotka mahdollistavat käyttäjien suorittaa toimintoja tiedoston omistajan oikeuksilla, on säännöllisesti tarkistettava varmistaakseen niiden tarpeellisuuden ja laillisuuden, vähentäen mahdollisia turvallisuusriskejä, jotka liittyvät SUID-oikeuksien väärinkäyttöön.
6.1.13	Tarkasta SGID-suoritettavat tiedostot	1	K	M	Säännöllisten SGID-suoritettavien tiedostojen tarkastusten suorittaminen on keskeistä järjestelmän turvallisuuden ylläpitämisessä. Nämä tiedostot, jotka suoritetaan ryhmätason oikeuksilla, on tarkasti tarkistettava varmistaakseen niiden aitouden ja havaitakseen mahdolliset poikkeamat niiden md5-tarkistussummista verrattuna alkuperäisiin paketteihin, mikä voi viitata mahdolliseen manipulointiin.
6.2	Paikallisten Käyttäjien ja Ryhmien Asetukset				
6.2.1	Varmista, että /etc/passwd-tiedostossa olevat tilit käyttävät shadow-salasanoja	1	K	A	On elintärkeää järjestelmän turvallisuuden kannalta, että paikalliset käyttäjät /etc/passwd-tiedostossa käyttävät varjostettuja salasanoja, merkitty 'x':llä niiden salasanakentässä. Tämä menetelmä salaa salasanat turvallisemmassa /etc/shadow-tiedostossa, vähentäen salasanojen murtamisen riskiä /etc/passwd-tiedostosta. Lisäksi käyttäjätileillä tulee olla joko salasanat tai ne tulee lukita estämään luvaton käyttö, erityisesti niillä, joilla on tyhjä salasanakenttä /etc/passwd-tiedostossa, mikä muodostaa turvallisuusriskin.
6.2.2	Varmista, etteivät /etc/shadow salasanakentät ole tyhjiä	1	K	A	On olennaista järjestelmän turvallisuuden kannalta varmistaa, että kaikilla /etc/shadow-tiedoston tileillä on asetetut salasanat tai ne ovat lukittuja estääkseen luvattoman pääsyn. Tyhjät salasanakentät olevat tilit ovat merkittävä turvallisuusriski, sillä ne mahdollistavat pääsyn ilman salasanan todentamista.
6.2.3	Varmista, että kaikki /etc/passwd-tiedostossa olevat ryhmät ovat olemassa /etc/group-tiedostossa	1	K	A	On tärkeää säännöllisesti varmistaa, että kaikilla /etc/passwd-tiedostossa mainituilla ryhmillä on vastaavat määritelmät /etc/group-tiedostossa. Tämä johdonmukaisuus on olennaista ryhmäoikeuksien asianmukaisen hallinnan ja koko järjestelmän turvallisuuden ylläpitämiseksi, estäen mahdollisia riskejä, jotka aiheutuvat hallitsemattomista ryhmäoikeuksista.
6.2.4	Varmista, että shadow-ryhmä on tyhjä	1	K	A	On tärkeää varmistaa, että shadow-ryhmässä ei ole tavallisia käyttäjiä turvallisuuden vuoksi, koska se rajoittaa pääsyä arkaluontoiseen /etc/shadow-tiedostoon. Luvattoman käyttäjän pääsy tähän tiedostoon voi johtaa salasanojen murtamiseen ja muiden tilien turvatietojen vaarantumiseen, mikä lisää järjestelmän haavoittuvuuksien riskiä.

Nro	Suositus	T	K	S	Kommentti
6.2.5	Varmista, ettei päällekkäisiä UID-tunnuksia ole olemassa	1	K	A	Säännöllinen varmistaminen, ettei järjestelmässä esiinny päällekkäisiä UID-tunnuksia, on välttämätöntä. Yksilölliset UID-tunnukset ovat avainasemassa käyttäjien yksilöllisen vastuun ja oikeiden pääsyoikeuksien ylläpitämisessä, erityisesti koska /etc/passwd-tiedostoon tehtävät manuaaliset muutokset voivat johtaa UID-tunnusten päällekkäisyyksiin.
6.2.6	Varmista, ettei päällekkäisiä GID-tunnuksia ole olemassa	1	K	A	Säännöllinen seuranta, jotta järjestelmässä ei esiinny päällekkäisiä GID-tunnuksia, on olennaista. Yksilölliset GID-tunnukset ovat tärkeitä ryhmäkohtaisen vastuun ja asianmukaisten pääsyoikeuksien ylläpitämisessä, ottaen huomioon, että manuaaliset muutokset /etc/group-tiedostoon voivat johtaa GID-tunnusten päällekkäisyyksiin.
6.2.7	Varmista, ettei päällekkäisiä käyttäjänimiä ole olemassa	1	K	A	On tärkeää säännöllisesti varmistaa, ettei /etc/passwd-tiedostossa ole päällekkäisiä käyttäjänimiä. Päällekkäisyydet voivat johtaa jaetun UID:n käyttöön, luoden turvallisuusriskejä mahdollistamalla pääsyn toiselle käyttäjälle tarkoitettuihin tiedostoihin. Tämä tilanne syntyy, kun järjestelmä käyttää käyttäjänimen ensimmäistä löytyvää UID:tä, jättäen huomiotta myöhemmät päällekkäisyydet.
6.2.8	Varmista, ettei päällekkäisiä ryhmänimiä ole olemassa	1	K	A	Säännöllinen tarkistus ja päällekkäisten ryhmänimien estäminen /etc/group-tiedostossa on tärkeää turvallisuuden kannalta. Päällekkäisyydet voivat aiheuttaa tahattoman GID:en jakamisen, johtaen pääsynvalvonnan ongelmiin ja turvallisuusriskiin, koska järjestelmä yhdistää käyttöoikeudet ryhmänimen ensimmäiseen löytyneeseen GID:een.
6.2.9	Varmista root-käyttäjän PATH-integriteetti	1	K	A	Root-käyttäjän PATH:n eheyden varmistaminen on olennaista turvallisuusriskien estämiseksi. Virheelliset PATH-asetukset, jotka saattavat sisältää nykyisen työskentelyhakemiston tai kirjoitettavat hakemistot, voivat altistaa järjestelmän vaarallisille ohjelmille, mahdollisesti antaen hyökkääjille superkäyttäjäoikeudet.
6.2.10	Varmista, että root on ainoa UID 0 -tunnusta käyttävä tili	1	K	A	Varmistaminen, että root-tili on ainoa UID 0:lla varustettu tili, on elintärkeää järjestelmän turvallisuuden ylläpitämiseksi. Tämä rajoitus takaa, että superkäyttäjän oikeudet on varattu yksinomaan root-tilille ja hallinnolliset tehtävät suoritetaan kontrolloiduissa ja turvallisissa olosuhteissa, vähentäen mahdollisia turvallisuusriskejä.
6.2.11	Varmista, että paikallisten interaktiivisten käyttäjien kotihakemistot ovat olemassa	1	K	A	On tärkeää varmistaa, että jokaisella paikallisella vuorovaikutteisella käyttäjällä on voimassa oleva ja olemassa oleva kotihakemisto, kuten /etc/passwd:ssä on listattu. Asianmukaisten kotihakemistojen puuttuessa käyttäjät ohjautuvat juurihakemistoon ("root"), mikä voi johtaa toiminnallisiin rajoituksiin ja turvallisuusongelmiin.
6.2.12	Varmista, että paikalliset interaktiiviset käyttäjät omistavat kotihakemistonsa	1	K	A	On välttämätöntä varmistaa, että jokainen paikallinen vuorovaikutteinen käyttäjä omistaa kotihakemistonsa, jotta voidaan ylläpitää järjestyksellistä tiedostohallintaa ja turvallisuutta. Kotihakemistojen käyttäjäomistajuus korostaa vastuuta näissä henkilökohtaisissa tiloissa tallennetuista sisällöistä ja asetuksista.
6.2.13	Varmista, että paikallisten interaktiivisten käyttäjien kotihakemistojen tila on 750 tai tiukempi	1	K	A	Käyttäjien kotihakemistojen tiukkojen oikeuksien asettaminen (tila 750 tai tiukempi) on välttämätöntä suojaamaan luvattomalta pääsyltä ja mahdollisilta tietoturvaloukkauksilta. Nämä oikeudet auttavat estämään haitallisia toimia, kuten tietojen varastamisen tai käyttöoikeuksien laajentamisen, rajoittamalla pääsyn ainoastaan käyttäjälle ja hänen ryhmälleen.

Nro	Suositus	T	K	S	Kommentti
6.2.14	Varmista, ettei paikallisilla interaktiivisilla käyttäjillä ole .netrc-tiedostoja	1	K	A	On kriittistä varmistaa, että paikallisilla vuorovaikutteisilla käyttäjillä ei ole .netrc-tiedostoja, jotka ovat turvallisuusriski niiden tallentaessa salaamattomia FTP-kirjautumistietoja. Jos tällaiset tiedostot ovat välttämättömiä, niiden on oltava tiukasti hallinnassa ja oikeudet rajoitettuna 600:aan tai tiukempaan, sivuston käytäntöjen mukaisesti, herkkien tietojen suojelemiseksi.
6.2.15	Varmista, ettei paikallisilla interaktiivisilla käyttäjillä ole .forward-tiedostoja	1	K	A	Paikallisten vuorovaikutteisten käyttäjien tileillä olevien .forward-tiedostojen esiintyminen on turvallisuusriski. Nämä tiedostot, jotka ohjaavat sähköposteja uudelleen, voivat tahattomasti lähettää arkaluontoisia tietoja ulkopuolelle ja niitä voidaan käyttää hyväksi komentojen suorittamiseen. On tärkeää varmistaa, ettei näitä tiedostoja ole käyttäjähakemistoissa, jotta voidaan suojautua tahattomilta tietovuodoilta ja turvallisuusriskiltä.
6.2.16	Varmista, ettei paikallisilla interaktiivisilla käyttäjillä ole .rhosts-tiedostoja	1	K	A	On tärkeää varmistaa, että paikallisilla vuorovaikutteisilla käyttäjillä ei ole .rhosts-tiedostoja, sillä ne voivat muodostaa turvallisuusriskin. Näiden tiedostojen merkitys riippuu /etc/pam.conf-tiedoston asetuksista, mutta jopa tehoton ollessaan ne voivat sisältää herkkiä tietoja muista järjestelmistä, jotka voivat auttaa hyökkääjiä. Säännölliset tarkastukset paikallisilla tileillä estävät näiden tiedostojen esiintymisen ja auttavat ylläpitämään järjestelmän ja verkon turvallisuutta.
6.2.17	Varmista, etteivät paikallisten interaktiivisten käyttäjien pistetiedostot ole ryhmän tai kaikkien kirjoitettavissa	1	K	A	On tärkeää varmistaa, että paikallisten vuorovaikutteisten käyttäjien pistetiedostot (käyttäjän asetustiedostot, jotka alkavat pisteellä '.') eivät ole ryhmän tai kaikkien kirjoitettavissa turvallisuuden kannalta. Jos nämä tiedostot ovat väärin käytettävissä, ne voisivat joutua pahantahtoisten tahojen manipuloitaviksi, mikä johtaisi tietojen varkauteen tai luvattomaan oikeuksien laajentamiseen.