Mika Taavitsainen

Ratkaisumalli OSINT-työasemalle

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

28.4.2024

Tiivistelmä

Tekijä:	Mika Taavitsainen
Otsikko:	Ratkaisumalli OSINT-työasemalle
Sivumäärä:	31 sivua
Aika:	28.4.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Tietojenkäsittely ja tietoliikenne
Ohjaajat:	Osaamisaluejohtaja Janne Salonen

OSINT-työkaluille sekä -käyttötarkoituksille löytyy useita käytännön ohjeita helposti. OSINT-työskentelyyn tarvittavasta työaseman ratkaisusta puolestaan on huomattavasti hankalammin löydettävissä tietoa. Tämän perusteella lähdin selvittämään, miten saadaan selvitettyä OSINT-työasemalle käytännön ratkaisumalli.

Tämän opinnäytetyön alussa esittelin OSINT-perusteita sekä yleisiä työkaluja. OSINT-työaseman selvitystyön pohjaksi annettiin tiettyjä määritteitä kuten se, että OSINT-tiedustelu tehdään verkkoselameilla. Näiden pohjalta selvitettiin eri osat, joita vaaditaan työaseman turvalliseen ja käytännön toteutukseen.

Selvitystyön perusteella rakensin omasta kannettavasta tietokoneestani OSINT-työaseman käyttäen selvitystyön tuloksia. Työaseman rakentaminen onnistui selvitystyön mukaisesti, yksityiskohtien tarkentuessa sen aikana. Työaseman näkyvyyttä verkkosivuilla päästiin tutkimaan opinnäytetyön lopussa. Tässä nähtiin, että verkkoselaimet pystytään yksilöimään, vaikka niissä käytettiin VPN-sovellusta ja vaikka tietokoneet olivat kovennuttuja.

Opinnäytetyön selvityksen tuloksia voidaan hyödyntää organisaatioiden tai yksityishenkilöiden miettiessä OSINT-työasemalle ratkaisuja. Selvitystyöstä voidaan ottaa osia tai muokata kokonaisuutta paremmin sopimaan tiettyyn käyttötarkoitukseen. Opinnäytetyössä käytiin myös muutamia vaihtoehtoisia ratkaisumalleja läpi.

Avainsanat: OSINT, avoimen lähteen tiedustelu, työasema, tietoturva

Abstract

Author:	Mika Taavitsainen
Title:	Solution model for OSINT workstation
Number of Pages:	31 pages
Date:	28 April 2024
Degree:	Bachelor of Engineering
Degree Programme:	Degree Programme in Information and Communication Technology
Professional Major:	Information and Communication Technologies (ICTs)
Supervisors:	Janne Salonen, Director of school

You can easily find several practical instructions for OSINT tools and purposes. On the other hand, it is significantly more difficult to find information about the workstation solution needed for OSINT work. Based on this, I set out to find out how to find out a practical solution model for the OSINT workstation.

At the beginning of this thesis, I presented OSINT basics and general tools. Certain attributes were given as the basis for the investigation work of the OSINT workstation, such as the fact that OSINT intelligence is carried out using web browsers. Based on these, the various parts that are required for the safe and practical implementation of the workstation were clarified.

Based on the research, I built an OSINT workstation from my own laptop using the results of the research. The building of the workstation was successful in accordance with the research work, the details being refined during it. The digital fingerprint of the workstation on the internet was examined at the end of the thesis. Web browsers can be identified, even if they used a VPN application and even if the computers were hardened.

The results of the thesis report can be used when organizations or individuals are thinking about solutions for an OSINT workstation. Parts of the survey can be taken or the whole can be modified to better suit a specific purpose. A few alternative solution models were also reviewed in the thesis.

Keywords: OSINT, Open source intelligence, workstation, information security

Sisällys

Lyhenteet

OSINT:	Open source intelligent. Avoimista lähteistä olevien tietojen keräämistä ja analyysia, jota käytetään tiedusteluun.
TOR	The Onion Router. Mahdollistaa anonyymin kommunikoinnin verkossa .
VPN	Virtual Private Network. Virtuaalinen erillisverkko, joka yhdistää eri verkot julkisen verkon yli.
VM	Virtual Machine. Ohjelma, jolla pystyy ajamaan ohjelmia ja käyttöjärjestelmiä, kuten oikeassa koneessa.
BIOS	Basic Input Output System. Tietokoneen esikäynnistysohjelma, jolla saadaan ladattua käyttöjärjestelmä käynnistyksessä.
DISA-STIG	Defense Information Systems Agency - Security Technical Implementation Guide. Turvallisuussuositukset Yhdysvaltain Puolustusministeriön virastoille sekä heidän yhteistyökumppaneille.
CIS	Center of Interner Security. Voittoa tavoittelematon organisaatio, jonka tehtävä on auttaa ihmisiä ja yrityksiä suojaamaan itseään leviäviltä kyberuhkilta.
LTS	Long Term Support. Pidempi aikainen tuki ohjelmistoille kuin yleensä.
FDE	Full Disk Encryption. Suojausmenetelmä, jolla salataan tiedot laitteistotasolla.
LVM	Logical Volume Management. Tietojärjestelmien hallintajärjestelmä.
TPM	Trusted Platform Module. Käytetään tietokoneen suojauksen parantamiseen.

1 Johdanto

OSINT-työkaluille sekä -käyttötarkoituksille löytyy helposti hakukoneella useita hakutuloksia ja käytännön ohjeita. OSINT-työasemalle löytyy vastaavasti huomattavasti vähemmän ja käytännön ratkaisuja ei juurikaan. Googlen hakukoneella löytyy ”osint tools” -haulla 4 920 000 tulosta ja ”osint workstation” -haulla noin 47 900 tulosta tilanne (27.3.2024).

Tämän opinnäytetyön tarkoituksena on tehdä ratkaisumalli OSINT-työaseman käytännön toteutukseen. Työasemalle annetaan myöhemmin opinnäytetyössä tietyt määrittelyt, jonka pohjalta työasemamallia aletaan selvittämään. Selvitystyön jälkeen tehdään selvitystyön mukainen työasema ja verrataan tämän digitaalista jalanjälkeä ja toimintaa muihin tietokoneisiin. Työasemallin pääasiallisena työvälineenä tullaan käyttämään verkkoselainta ja muita määrittelyitä, jonka pohjalta työasemamallia lähdetään rakentamaan. Opinnäytetyön työasemamallissa ei lähdetä selvittämään kehittyneempiä OSINT-työkalujen käyttöä.

Opinnäytetyön toisessa luvussa avataan tarkemmin, mitä OSINT tarkoittaa. Tämän jälkeen avaan OSINT-käytössä olevia ohjelmistoja ja käyttöjärjestelmiä. Kolmannessa luvussa selvitän, mitä työaseman tekemiseen tarvitaan, ja asiat, jotka tulee ottaa huomioon. Neljännessä luvussa teen tämän selvitystyön perusteella käytännön toteutuksen työasemalle. Viidennessä luvussa tutkitaan työaseman käyttöä OSINT-tiedusteluun ja verrataan työasemaa muihin tietokoneisiin. Tämän ja aikaisempien lukujen pohjalta tehdään loppukäyttäjälle käytännön ohjeita OSINT-työaseman käyttöön ja katsotaan sen digitaalista jalanjälkeä. Viimeisessä luvussa pohditaan opinnäytetyön tuloksena tehtyä työasemallia ja sen onnistumista.

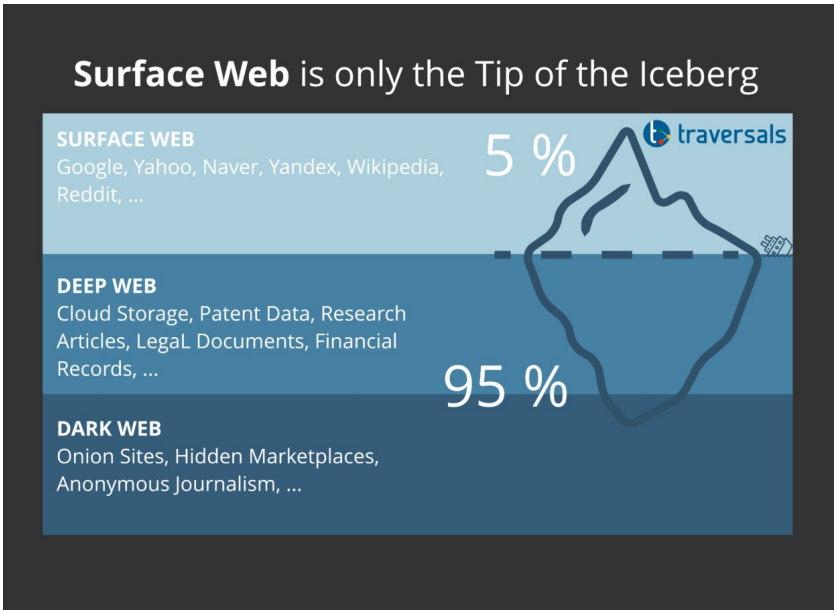
2 Mikä on OSINT?

OSINT (open source intelligence) tarkoittaa suomeksi avoimien lähteiden tiedustelua. Avoimien lähteiden tiedustelulla pyritään vastaamaan johonkin tiettyyn tiedustelukysymykseen. OSINT tapahtuu kaikkien vapaasti saatavilla tiedon käyttämistä tiedustelukysymykseen vastaamiseen. Yksinkertaisimmillaan OSINT tapahtuu hakemalla internetin eri hakukoneilla asiaan liittyvillä hakusanoilla tietoa tiedustelun kohteesta olevasta asiasta/henkilöstä.

Kaikki tieto ei kuitenkaan ole tiedustelutietoa. Kerätyllä tiedolla ei ole väliä, mikäli sille ei ole merkitystä vastaamaan tiedustelukysymykseen. Vasta kun tietoa tarkastellaan kriittisesti ja analysoidaan, siitä tulee tiedustelutietoa. Esimerkiksi Facebookin kaverilistan tallentaminen ei ole tiedustelutietoa, ennen kuin pystytään näyttämään, että tämä tieto on oleellista tiedustelukysymyksen kannalta. Vasta tämän jälkeen tätä voidaan käyttää tiedustelutietona. [Gill 2023.]

2.1 OSINT-tietolähteet

Tiedonlähteitä avoimien lähteiden tiedustelulle on runsaasti. Lohsen ym. [2019: 88] mainitsee tyypillisiksi avoimiksi tietolähteiksi muun muassa kirjallisuuden, tilastot, kartat, lehdet, yksityisten sekä viranomaisten julkaisut, viranomaisten julkiset rekisterit sekä tietokannat, yleisölle suunnatut televisio- ja radiolähetykset sekä tietoverkon ja sosiaalisen median sisällöt. Internetissä on paljon tietolähteitä, joihin ei ole mahdollista löytää hakukoneiden kautta tai edes päästä perusselaimella. Kolbin [2020] mukaan tämä kaikille avoin pintaverkko (surface web) on 5 % maailmanlaajuisesta tietoverkoista. Loput tietoverkosta ovat syväverkkoja (deep web) tai pimeitä verkkoja (dark web). Syväverkot ovat yleisesti suljettuja verkkoja salasanojen takana. Pimeät verkot vaativat erityisohjelmistoja päästääkseen verkon tietoihin käsiksi (esimerkiksi TOR).



Kuva 1: Avoin verkko on vain jäävuoren huippu ja käsittääkin vain 5 % kaikista tietoverkoista. [Kolb. 2020. Surface Web]

Yritykset käyttävät paljon OSINT:a tutkiessaan esimerkiksi kilpailevaa yritystä. Yksityishenkilöiden Facebook- tai X-palvelun selailu myös voidaan laskea OSINT:n alle. Hiter [2023] mainitsee yleisinä OSINT-käyttökohteina seuraavat kohteet:

- haavoittuvuuksien tiedustelu ja hallinta, sekä penetraatiotestaus
- markkinatutkimus ja brändi seuranta
- paikkatietojen hankinta ja analyysi
- kilpailuedun hakeminen
- reaaliaikainen analyysi suurista väestöryhmistä
- taustojen ja laillisuuden tarkastus
- faktojen tarkastus.

2.2 OSINT-työkalut

OSINT-työkaluja on hyvin erilaisia, ja yleensä ne on räätälöity tiettyyn tarkoitukseen. Perusselaimella päästään jo hyvin pitkälle avoimen lähteen tiedustelussa. Selaimella ei kuitenkaan pääse kaikkeen saatavilla olevaan tietoon käsiksi, eikä näiden välisiä yhteyksiä pystytä näkemään. Myös tiedon hakeminen esimerkiksi tuhannesta lähteestä samaan aikaan on mahdotonta, mutta erilaisia työkaluja hyödyntäen se on helppoa. Työkaluilla tieto saadaan helpommin muotoon, joka on ihmisen ymmärrettävissä.

Avoimen lähdekoodin työkaluja löytyy paljon OSINT-tarkoitukseen. OSINT Frameworkin sivuilta (https://osintframework.com/) löytää melkeinpä jokaiseen tarkoitukseen työkalun tai resurssin, jota voi käyttää avoimien lähteiden tiedustelun avuksi. Alle olen listannut muutamia yleisesti käytössä olevia työkaluja.

- Google Dorks
    - Tarkoitetaan Googlen haun käyttöä OSINT-työkaluna. Haussa käytetään kehittyneitä hakulauseita tai mukautettuja hakuja, joilla saadaan tarkempaa ja/tai tietoa mikä ei yksinkertaisella haulla onnistuisi. [Awati 2022.]
- Shodan
    - Shodan on hakukone, jota käytetään internettiin kytkettyihin laitteisiin. Hauilla ei etsitä verkkosivuja, vaan laitteita, jotka on kytketty internettiin. Tällä voidaan saada tietoon esimerkiksi tietyn käyttöjärjestelmän suosio tai selvittää, kuinka moneen tietokoneeseen jokin haavoittuvuus vaikuttaa. [What is Shodan?]
- Maltego

- Hakutulosten ja internet-infrastruktuurin välillä on yhteyksiä, joita ei pysty havaitsemaan itse helposti. Maltego auttaa tässä esittämällä ne visuaaliseti. [What can I use Maltego for? 2020.]

- SpiderFoot

  - On tiedustelutyökalu, joka automaattisesti etsii yli sadasta julkisesta tietolähteestä tietoa valitusta kohteesta. Kohteesta etsitään esimerkiksi IP-osoitteita, verkkotunnuksia, sähköpostiosotteita sekä nimiä. Näitä tietoja voidaan käyttää lisätiedon saamiseen tiedustelukohteesta.

3 Työasemamallin selvitys

OSINT-käyttökohteita sekä -tarpeita on hyvin erilaisia ja näihin kaikkiin on mahdotonta vastata yhdellä työasemamallilla. Tämän takia onkin tärkeää tehdä ratkaisumalli, joka on hyvin yleispätevä. Työasemamallia voidaan sitten muokata helposti enemmän vastaamaan tarkoitusta. Selvitystyötä varten työaseman tulevaa käyttöä ja muita ominaisuuksia on kirjattu seuraavaan lukuun. Tämän perusteella selvitystyö voidaan aloittaa.

Työaseman käyttö rajataan selaimella tapahtuvaan avoimien lähteiden tiedusteluun, eikä työasemalle asenneta kehittyneempiä OSINT-työkaluja. Tietokoneen laitteisto ei ole vakioitua, jolloin se saattaa muuttua. Käyttöjärjestelmä ja BIOS ovat kovennettuja, jotta työsema olisi mahdollisimman turvallinen. Työasemasta löytyy VPN-sovellus.

3.1 Laitteisto

Tietokone, jota käytetään OSINT-työasemaan ei tarvitse olla erityisen tehokas. Tietokoneen tehoksi riittää se, että sillä voidaan selata verkkosivuja ja suorittaa tietokoneella olevia ohjelmia. Selvitystyön aikana ohjelmistot ja käyttöjärjestelmät tarkentuvat ja yhteenvedossa voimme tarkistella näiden minimitehovaatimuksia. Tämän perusteella saamme työasemamallille minimivaatimukset.

Tietokone, jota käytetään työasemamallissa olisi syytä olla pelkästään käytössä OSINT-tarkoituksiin. Mikäli kone on ollut tai sitä käytetään muuhun tarkoituksiin, kuten henkilökohtaisiin ostoksiin internetissä saattavat nämä selailut kontaminoida OSINT-tulokset. Tietokone voi olla täysin uusi, jolloin siinä ei ole mitään tietoa käyttäjän aikaisimmista toimista. Vaihtoehtoisesti tietokone voi olla myös käytetty, jolloin tietokoneen kiintolevy täytyy alustaa ja asentaa uusi käyttöjärjestelmä. Näin pystytään varmistumaan siitä, että käyttäjän edelliset tiedot häviävät. [Bazzel 2023: 2.]

3.2 Käyttöjärjestelmä

Määrittelyissä käyttö on rajattu pelkästään selaimella tapahtuvaan OSINT-tiedusteluun. Näin ollen kaikki yleisimmä käytössä olevat käyttöjärjestelmät (Windows, Linux, macOs) kävisivät tämän määrittelyn alle. Bazzel [2023: 14] suosittelee käyttämään Linux-käyttöjärjestelmää OSINT-tarkoituksiin sen helpon ajettavuuden, asennettavuuden, ilmaisuuden sekä turvallisuuden takia.

Linux on suomalaisen Linus Torvaldsin kehittämä käyttöjärjestelmäydin, jonka päälle on rakennettu erilaisia Linux-jakeluita. Linux-jakeluita on yli 600 aktiivista ja 500 kehitysvaiheessa olevaa. [Branka 2024]. Linux-jakeluita on räätälöity eri käyttötarkoituksiin. Linux-jakeluista Bazzel [2023: 16] suosittelee käyttämään Ubuntua lähinnä sen helppokäyttöisyyden takia. Ubuntua voidaan myös automaatti koventaa ja auditoida käyttämällä automaattisia skriptejä Ubuntulle.

Linux-käyttöjärjestelmä kannattaa ajaa virtuaalikoneessa. Tästä saadaan paljon hyötyjä verrattuna suoraan raudalla ajettavaan käyttöjärjestelmästä. Näitä hyötyjä ovat esimerkiksi seuraavat asiat. Virtuaalikoneen helpot alkuasetukset ja helppo nollaaminen, mahdollisuus ottaa Snapshotteja, jolloin koneen tila voidaan palauttaa Snapshotin ottohetken tilanteeseen sekä mahdollisuus kopioida Image-virtuaalikoneesta useampaan eri OSINT-työasemaan.

Virtuaalikone kuitenkin tulee ajaa jossain käyttöjärjestelmässä. Käytettävällä käyttöjärjestelmällä ei ole juurikaan väliä, kun käytännön OSINT tehdään vir-

tuaalikoneessa pyörivällä Ubuntulla. Helpoin ja käytännöllisin tapa on ajaa virtuaalikone koneessa jo olevalla käyttöjärjestelmällä. Pöytäkoneista 72,13 % [Desktop Operating System Market Share Worldwide 2024] käyttää Windows-käyttöjärjestelmää, joten työasemamalli rakennetaan myös Windows-käyttöjärjestelmän ympärille. Suurimmassa osassa tietokoneista Windows tulee myös valmiiksi asennettuna.

3.3 Ohjelmistot

OSINT-työasemamaallissa Ubuntu ajetaan virtuaalikoneessa. Virtuaalikonetta varten Bazzel [Bazzel 2023: 16] ehdottaa omiin kokemuksiinsa perustuen VirtualBoxia. Myös Das [2024] on sijoittanut VirtuaBoxin parhaaksi virtuaalikoneeksi sen hyvien ominaisuuksien takia. Näitä ominaisuuksia ovat hyvä tuki usealle eri käyttöjärjestelmälle, helppokäyttöinen käyttöliittymä, nopea suorituskyky, säännölliset päivitykset sekä sen useat ominaisuudet. Tämän perusteella VirtualBox valitaan työasemamamallin virtuaalikoneen ohjelmaksi.

Käytännön OSINT-tiedustelun tekemiseen tarvitaan verkkoselainta. Verkkoselaimet ovat hyvin samankaltaisia keskenään ja jokaisella niistä voidaan tehdä OSINT-tiedustelua. Ubuntussa tulee automaattisesti Firefox-verkkoselain, joten sitä käytetään työasemamallin ratkaisussa. Firefox on hyvin tuettu ja päivitetään usein ja siihen löytyy runsaasti lisäosia, joilla pystytään räätälöimään ja tuomaan uusia ominaisuuksia verkkoselaimeen.

VPN:llä eli virtuaalisilla erillisverkoilla voidaan suojata ja piilottaa tietokoneen IP-osoite. Käyttäjän tietoliikenne ohjataan normaalisti suoraan kohdepalvelimelle mutta VPN-yhteydellä se reititetään salattuna VPN-palvelimen kautta kohdepalvelimelle. Näin kohdepalvelin ei pysty havaitsemaan, mistä käyttäjän tietoliikenne tulee. VPN-yhteyttä voidaan myös käyttää antamaan vaikutelma, että tietoliikenne tulee eri maasta tai kohteesta kuin mistä se todellisuudessa tuleekaan. Tämän ominaisuuden avulla pystytään kiertämään maantieteellisiä aluerajauksia. Useilla uutissivuistoilla saattaa olla osa materiaalista vain kotimaisille käyttäjille lukittuna. Esimerkiksi osa Yle Areenan materiaalista on rajattu ainoastaan

näkymään ja kuulumaan Suomessa [Areenan käyttö ulkomailla]. VPN-palveluntarjoajien tulisi tallentaa mahdollisimman vähän lokeja VPN:n käytöstä, jotta tietoliikennettä ei voida jälkikäteen tutkia.

Kun kaikki tietoliikenne reititetään VPN-palvelimien kautta on tärkeää, että VPN-palveluntarjoajaan voi luottaa. Uutisissa on ollut useampia tapauksia, joissa VPN-palveluntarjoajat eivät ole toimineet kuten ovat mainostaneet. Vuonna 2020 uutisoitiin, että seitsemän VPN-palveluntarjoajaa olivat tallentaneet nimiä, salasanoja, sähköpostiosoitteita sekä kotiosotteita, vaikka palveluntarjoajat olivat erikseen mainostaneet, etteivät tallenna lokeja. Tämä vaikutti yli 20 miljoonaan käyttäjään [Kan: 2020]. Myös vuonna 2017 uutisoitiin, että Androidilla olevista VPN-sovelluksista 38% sisältäisi haittaohjelmia [Heathman: 2017].

VPN-palveluntarjoaja löytyy paljon. Yksi suosituista on Proton VPN. Proton VPN on avoimeen lähdekoodiin perustuva VPN-sovellus. Avoimen lähdekoodin takia jokainen voi vapaasti käydä katsomassa, miten Proton VPN on ohjelmoitu. Tämän takia Proton VPN on hyvin läpinäkyvä ja vastuullinen palveluntarjoaja [Yen: 2020]. Proton VPN ei myöskään tallenna lokeja. Lokien tallentamatta jättäminen on myös auditoitu kolmannen osapuolen toimesta [Yen: 2022]. VPN-sovellukseksi valitaan näistä syistä Proton VPN.

Virus- ja haittaohjelmatorjuntaan tarvitaan myös omat sovellukset Windows- ja Ubuntu-käyttöjärjestelmiin. Windows-käyttöjärjestelmästä löytyy suoraan asennettuna Microsoft Defender. Defender on saanut vuonna 2023 AV-testin arvostelussa 6/6 pisteet kaikissa kategorioissa. [AV-TEST Product Review and Certification Report: 2023]. Ilmaisuuden ja valmiiksi asennuksen takia Windows-käyttöjärjestelmässä käytetään Microsoft Defenderiä. Linux-käyttöjärjestelmän virustorjuntaohjelmaksi Bazzel [Bazzel: 2023: 12] suosittelee käyttämään ClamAV-sovellusta. Clamav on avoimeen lähdekoodiin perustuva ilmainen virustorjuntaohjelma.

3.4 Kovennus

Kovennuksella (eng. hardening) tarkoitetaan järjestelmän turvaamista vähentämällä haavoittuvuuksien pinta-alaa. Käytännössä tämä voi näkyä poistamalla turhia käyttäjiä tai sovelluksia, oletussalasanojen vaihtamisella ja sulkemalla käyttämättömiä protokollia. On tärkeä myös muistaa päivittää käyttöjärjestelmä ja sovellukset aina, kun niistä tulee uusi versio. Uusissa versioissa on yleensä tietoturvapäivityksiä, joiden kautta tiedettyjä haavoittuvuuksia on voitu korjata.

Kovennus aloitetaan tietokoneen koventamisesta. Tietokoneita ja niiden BiOS-ohjelmia on useita ja niissä on eri asetuksia riippuen tietokoneesta ja valmistajasta. Tämän takia kovennusohjeita ei pysty antamaan yksityiskohtaisesti, vaan käydään yleisiä periaatteita koventamiseen.

Kovennuksessa on otettava huomioon seuraavat asiat. BIOS-koventaminen aloitetaan suojaamalla se salasanalla, Secure Boot -valinta tulee laittaa päälle, jotta vain allekirjoitetut alkulatausohjelmat käynnistetään. BIOS tulee myös päivittää säännöllisesti, jotta uudet haavoittuvuudet saadaan korjattua. Turhat oheislaiteportit tulee sulkea, jotta niitä ei voida käyttää hyökkäykseen. Kovalevy pitää salata, jotta kovalevystä ei voida lukea tietoja, vaikka se saataisiinkin irrotettua tietokoneesta [Meier: 2023].

Windowsia käytetään pelkästään virtuaalikoneen ajamiseen. Käytännön OSINT-tiedustelu tehdään Ubuntulla, joten keskitymme sen koventamiseen. Ubuntuun onneksi löytyy 2 automaattiskriptiä koventamiseen. Nämä ovat DISA-STIG (Defense Information Systems Agency-Security Technical Implementation Guides) ja CIS (Center for Internet Security). DISA-STIG on suunniteltu Yhdysvaltain Puolustusministeriön virastojen sekä heidän yhteistyökumppaneidensa käytettäväksi. CIS puolestaan on tehty Center for Internet Securityn yleiseen käyttöön eri toimialoille. [Book 2023.]

Työasemamallia ei ole suunniteltu osaksi Yhdysvaltain Puolustusministeriön järjestelmiä. DISA-STIG on myös ainoastaan tuettuna kirjoitushetkellä (31.3.2024)

Ubuntu 20.04 -versiolle ja sitä vasta sertifioidaan 22.04 -versiolle. [Security Compliance & Certifications for 22.04]. Uusin LTS (Long term support) on 22.04-versio, jota tuetaan 2027 asti ja Ubuntu Pro tilaajille tuetaan 2032 asti. 20.04-versiota tuki loppuu kaksi vuotta aikaisemmin kuin 22.04. CIS-kovennuksen saa tehtyä uusimpaan 22.04-versioon ja se on yleisesti enemmän käytössä oleva. Pidemmän tuen ja yleisemmän käytön takia OSINT -työasemamalliin valitaan CIS-kovennukset. CIS-kovennuksia on level 1 ja level 2 tason kovennuksia. Level 1 on suunniteltu niin, että se ei vaikuta tietokoneen tehokkuuteen tai sen käytettävyyteen juurikaan. Level 2 on suunniteltu taas ympäristöihin, joissa turvallisuus on tärkeää ja se saattaa vaikuttaa tietokoneen toimintaan, mikäli sitä ei ole toteutettu kunnolla. Työasemamallissa riittää level 1 tason kovennus. [CIS Benchmarks™ FAQ.]

Kovalevyt tulee myös salata. Mikäli kovalevyä ei ole salattu, voidaan se kopioida tai irrottaa ja siirtää toiseen tietokoneeseen, jossa kovalevyn tiedostot pystytään lukemaan selkokielisinä. Kovalevyn salauksella estetään kovalevystä tietojen lukeminen ilman salasanaa tai avainta. Windows-käyttöjärjestelmälle löytyy suoraan Bitlocker-niminen salausohjelma. Ubuntulle löytyy oma FDE (full disk encryption) -salausohjelma. Työasemamalli tulee käyttämään näitä salauksessa. Kummatkin ohjelmat tarvitsevat TPM-turvapiirin ollakseen mahdollisimman turvallisia. Ilman TPM-turvapiiriä salausta voi käyttää, mutta se antaa mahdollisuuden esimerkiksi käyttää brute force -hyökkäystä salasanan murtamiseen [BitLocker and TPM: 2023]. TPM-moduuli pitää myös ottaa huomioon työasemallin tietokonetta valittaessa.

3.5 Yhteenveto

Selvityksen perusteella tiedämme nyt, mitä ohjelmia ja käyttöjärjestelmiä tarvitsemme OSINT-työasemamallin rakentamiseen. Sovellusten ja käyttöjärjestelmien laitteistovaatimuksista voimme katsoa, minkälaiset vaatimukset työasemallin tietokone pitää täyttää. Suurimmat suositellut tehovaatimukset oli merkitty Ubuntu-käyttöjärjestelmälle [Installation/SystemRequirements: 2022] seuraavilla suositelluilla laitteistovaatimuksilla:

- 2 Ghz tuplaydinprosessori
- 4 GiB RAM-muistia
- 25 GB kovalevytilaa.

Näiden lisäksi täytyy ottaa huomioon muut sovellukset ja Windows-käyttöjärjestelmä. 64-bittinen Windows 10 tarvitsee 20 GB tilaa kovalevyltä [Windows 10 system requirements]. Muut sovellukset eivät vie kokonaisuudessaan edes yhtä gigatavua muistia. Yhteensä voidaan katsoa, että kaikki pakollinen vie yhteensä 46 GB tilaa kovalevyltä. Työasemalla tullaan säilyttämään varmasti jonkin verran tiedostoja ja sovelluksiin ja käyttöjärjestelmiin tulee päivityksiä, jotka vievät tilaa. Miniminä voidaan näin ollen pitää 128 GB kovalevyä. Myös tietokoneessa tulee olla TPM-turvapiiri käyttöjärjestelmän salausta varten.

Tietokoneen valinnan jälkeen kovennetaan BIOS, joka suojataan salasanalla. Secure boot tulee laittaa päälle ja BIOS päivittää uusimpaan versioon, jonka jälkeen suljetaan ylimääräisest laiteportit.

Käyttöjärjestelmänä käytetään Windowsia. Antivirusohjelmana käytetään Microsoftin Defender -ohjelmaa. Windowsin kautta kovalevy salataan Bitlockerilla. Windowsiin asennetaan VirtualBox, johon asennetaan Ubuntu pyörimään virtuaalisesti. Ubuntu kovennetaan CIS-skriptillä. Ubuntun kautta kovalevy sala-

taan FDE:llä. Ubuntussa asennetaan antivirusohjelmaksi ClamAV. VPN-sovelluksena käytetään Proton VPN -ohjelmaa.

Näiden toimien jälkeen OSINT-työasemamallin tietokone olisi valmis tekemään OSINT-tiedustelua käyttäen verkkoselainta.

3.6 Vaihtoehdot työasemamalliin

Käytännönratkaisu OSINT-työasemamalliin on lähtenyt tietyistä alkuolettamista, jotka ovat muokanneet ratkaisua tiettyyn suuntaan. Erilaisia ratkaisumalleja on myös, ja ne riippuvat paljon käyttökohteista ja määrittelyistä järjestelmälle. Seuraavaksi käydään läpi, miten työasemamallia voidaan muokata paremmin sopimaan eri käyttötarkoituksiin ja ratkaisumalleihin.

Työasemamalli on lähtenyt ajatuksesta Windowsin päällä pyörivällä virtuaalikoneella. Työasemamallin voisi myös rakentaa suoraan raudan päällä pyörivälle käyttöjärjestelmälle. Tästä on tiettyjä haittoja ja hyötyjä. Hyötyihin kuuluu muun muassa tietokoneen resurssien tehokkaampi käyttö, kun on vain yksi käyttöjärjestelmä, johon resursseja käytetään. Hyötyihin voidaan lukea myös helpompi peruskäyttö käyttäjälle, kun virtuaalikonetta ei tarvitse käyttää. Haitoiksi voidaan katsoa esimerkiksi se, ettei käyttöjärjestelmää voida palauttaa aikaisempaan tilaan helposti ja vapaasti (Snapshot). Tietoturva on myös huonompi kuin virtuaalikoneen kanssa, koska käyttöjärjestelmä ei ole omassa ympäristössään. Tietokoneen laitteisto saattaa vaikuttaa ohjelmistojen tai kovennusten toimintaan. Käyttöjärjestelmän ja kaikkien ohjelmien kopiointi uusille tietokoneille on hitaampaa kuin virtuaalikoneen kanssa.

Muita käyttöjärjestelmiä voidaan myös käyttää työasemassa. Windowsia voidaan myös käyttää OSINT-tiedusteluun, mutta se nähdään yleisesti heikompana tietoturvan puolesta, koska se ei ole avoimen lähdekoodin käyttöjärjestelmä. Linuxille löytyy useita jakeluita, jotka on suunniteltu avoimen lähdekoodin tiedustelua, kyberturvallisuutta, penetraatiotestausta yms. silmällä pitäen. Usein näihin jakeluihin on sisällytetty valmiiksi tarpeellisia sovelluksia ja kovennuksia,

jotta ne palvelisivat mahdollisimman hyvin tarkoitustaan. Yleisiä ja suosittuja jakeluita tähän tarkoitukseen ovat Kali Linux, Parrot OS, ArchStrike, Black Arch ja Demon Linux. Näiden sovelluksia saa myös asennettua työasemamallin Ubuntu Linuxiin. Näin toiminallisuutta voidaan lisätä myös työasemamalliin ratkaisuun, mikäli siihen koetaan tarvetta.

Käyttöjärjestelmää on myös mahdollista ajaa ilman asennusta tietokoneelle, jolloin käyttöjärjestelmä ladataan tietokoneen RAM-muistiin ja ajetaan kokonaan sieltä. Näin käyttöjärjestelmästä tai sen käytöstä ei jää jälkiä tietokoneelle. Tätä käyttöjärjestelmää voidaan myös ajaa, mikäli tietokoneeseen on asennettu jokin toinen käyttöjärjestelmä kiintolevylle. Haittoina tässä ratkaisussa on, että kaikki tehdyt muutokset häviävät, joten tiedostoja ei voida tallentaa tietokoneelle. Myös sovellukset joutuu aina lataamaan uudestaan käyttöjärjestelmälle, kun se käynnistyy. Työasemamallin Linuxin Ubuntu voidaan käynnistää esimerkiksi näin.

4 Työasemamallin käytännön toteutus

Työasemamallin selvityksen jälkeen tiedämme kaiken oleellisen toteuttaaksemme työasemallin käytännön toteutuksen. Teen omalle kannettavalleni käytännön toteutuksen työasemamallista. Tämän tarkoituksena on selvittää, onko selvitystyön toimenpiteet mahdollisia ja käytännöllisiä. Työasemamallia voidaan myös seuraavassa luvussa käyttää käytännön ohjeiden tekemiseen sen käytöstä sekä verrata sitä perinteiseen tietokoneeseen, johon on Windows asennettuna ja johon ei ole tehty muutoksia. Käytännön toteutuksessa käydään ainoastaan läpi kaikki oleelliset kohdat, mitä tarvitsee ottaa huomioon OSINT-työasemassa.

4.1 Tietokoneen valinta

Tietokoneelta vaadittiin työasemamallia varten seuraavat laitteistovaatimukset:

- 2 Ghz tuplaydinprosessori

- 4 GiB RAM-muisti
- 128 GB kovalevytila
- TPM-moduuli.

Itseltäni löytyy mallikoneeksi Lenovo ThinPad T490s kannettava tietokone. Tietokoneen laitteistosta löytyy seuraavat ominaisuudet:

- Intel Core i5-8265U (1,6 - 3,9 GHz, 4 ydintä)
- 8 GiB RAM-muisti
- 240 GB SSD -kiintolevy
- TPM 2.0 -turvasiru

Lenovo ThinPad T490s kannettava tietokone ylittää kaikki määrittelyissä olevat laitteistovaatimukset OSINT-työasemalle; joten se voidaan ottaa käytännön toteutuksen mallikoneeksi.

4.2 BIOS-kovennus

BIOS:n kovennuksessa käydään katsomassa BIOS:ta, ovatko sen asennukset selvityksen mukaisessa kunnossa ja että BIOS on uusimmassa mahdollisessa versiossa.

Mallikoneen BIOS oli jo päivitetty uusimpaan versioon, jonka julkaisupäivä on ollut 1.12.2023. Secure Boot ei ollut valittuna valmiiksi, joten se piti laittaa päälle. Oheislaiteporteista pitää sulkea käyttämättömät pois. Mallikoneen tapauksessa seuraavat portit otettiin pois käytöstä: bluetooth, memory card slot, smart card slot, integrated camera, microphone, fingerprint reader ja thunderbolt 3. Seuraavat portit jätettiin päälle: ethenert LAN, wireless LAN, USB port ja integ-

rated audio. Verkkoyhteyksiä varten jätettiin LAN-yhteydet päälle, jotta käytännön OSINT-tiedustelua voidaan tehdä. USB-portit ovat auki, koska niiden kautta voidaan siirtää tietoa ulos OSINT-työasemasta ja käyttää oheislaitteita. Integrated audion kanssa työasemalla voidaan kuunnella äänilähteitä. Lopuksi BIOS:lle asetettiin salasana.

4.3 Windowsin asennus

Kuten luvussa 3.1 on jo todettu tärkeää, että käyttöjärjestelmä asennetaan uudestaan, mikäli tietokone on ollut jo käytössä. Näin vanhat käyttäjätiedot eivät kontaminoi OSINT-tuloksia. Kannettavasta tietokoneesta löytyi kovalevyltä suoraan palautusimage, josta Windowsin pystyy asentamaan uudestaan. Vanhat tiedostot tulee tässä vaiheessa siirtää pois tietokoneelta, mikäli niitä haluaa säilyttää.

Asennuksen alkuun pääsi helposti painamalla Windows-käyttöjärjestelmästä shift+restart. Tietokone käynnistyy uudestaan ja avaa valikon, josta voi valita Windowsin uudestaanasennuksen. Asennuksen aikana täytyy valita Remove everything, jotta uudestaan asennus poistaa vanhat tiedostot tietokoneelta. Asennuksen aikana Windows pyytää kirjautumaan käyttäjätilille. Emme voi kirjautua vanhoilla tunnuksilla, emmekä sitoa käyttöä Windows-tiliin. Windows ei anna suoraan tehdä pelkästään paikallista tiliä, vaan Windowsille joutuu antamaan muutaman käskyn, jotta se suostuu antamaan tämän vaihtoehdon. Käsky saadaan kirjoitettua avaamalla komentorivi (shift + F10), kun valitaan käyttäjän sijainti ja kirjoittamalla sinne ”OOBE\BYPASSNRO”-käskyn. Seuraavaksi tietokone käynnistyy uudestaan ja komentoriville kirjoitetaan tällä kertaa ”ipconfig / release”. Tämän jälkeen Windows antaa valinnan "I don't have Internet", josta pystyy tekemään paikallisen tilin ilman Microsoft-tiliä. [Piltch 2024.]

Asennuksen aikana Windows myös pyytää suostumusta valinnaisen datan lähettämistä Microsoftille, lupaa käyttää sijaintia yms. Näihin kaikkiin vastataan ei, jotta mitään ylimääräistä ei lähetetä Microsoftille mallikoneen käytöstä.

Asennuksen jälkeen Windows päivitetään, jotta uusimmat tietoturvapäivitykset asentuvat. Tämän jälkeen kiintolevy salataan käyttämällä Bitlocker-ohjelmaa. Bitlockerin antama palautusavain on tärkeää ottaa USB-tikulla talteen tai tulostaa palautusavain paperille, jotta Bitlockerin salauksen pystyy purkamaan, mikäli ongelmia ilmenisi.

Selvityksessä päädyttiin käyttämään Microsoft Defenderiä antivirusohjelmana. Windows asentaa ja alkaa automaattisesti käyttämään Defenderiä, joten se ei vaadi asennuksen jälkeen toimia.

4.4 Virtuaalikoneen asennus

Virtuaalikonetta varten tarvitaan VirtualBoxin ja Ubuntun asennustiedostot. Näitä varten kävin Edge-verkkoselaimella lataamassa nämä tiedostot tietokoneelle. Kuten Windowsiakin asentaessa myös Edgeä asentaessa on tärkeää olla antamatta lupaa lähettää muuta kuin pakolliset tiedot Microsoftille.

Ubuntun asentaminen VirtualBoxiin on yksinkertaista. VirtualBoxiin tehdään uusi virtuaalikone ja siihen ladataan Ubuntun image. Asennuksessa ei otettu unattended-asennusta, vaan asennus tehdään tavalliseen valikoista tapahtuvaan malliin. Virtual Boxille täytyy kertoa, kuinka paljon Ubuntu saa käyttää tietokoneen tehoista. Mallikoneen toteutukselle annettiin puolet koneen RAM-muistista ja prosessorin ytimistä, käytännössä siis 4096 MB RAM-muistia ja 4 ydintä. Kiintolevylle jätettiin tilaa 128 GB. Asennuksessa valitaan minimal installation -valinta, jotta ohjelmia, joita ei tarvita, ei asenneta. Tämä voidaan katsoa osaksi kovennusta, kun käyttämättömiä ohjelmia ei asenneta, niin haavoittuvuuksien mahdollinen pinta-ala vähenee.

Asennuksen aikana tulee tehdä virtuaalilevyn salaus. ”Installation type”-kohdassa tulee valita ”Advanced features…” ja valita ”Use LVM with the new Ubuntu installation”. Tämän jälkeen valitaan vielä ”Encrypt the new ubuntu installation for security”. Viimeiseksi salauksen purkuun pitää antaa salausavain. Ubuntun antama palautusavain (recovery key) tallennetaan työpöydälle ja siirretään

asennuksen jälkeen talteen toiselle koneelle käyttäen USB-tikkua. Tietokoneelle pitää antaa myös nimi. Tähän ei tule laittaa nimeä, joka voi kertoa käyttäjästä tai tietokoneen käytöstä, koska se näkyy ulospäin ulkopuolisille.

4.5 Ubuntun kovennus

Asennuksen jälkeen Ubuntu täytyy koventaa ennen kuin sillä tehdään mitään muuta. Selvityksen perusteella koventamiseen käytetään CIS-skriptiä. CIS-skriptin asennusta varten tarvitaan Ubuntu Pro -tilaus. Ubuntu Pron saa hankittua omaan käyttöön ilmaiseksi viidelle tietokoneelle osoitteesta https://ubuntu.com/pro/subscribe. Rekistöröintiä varten käytän https://temp-mail.org/-sivuston tarjoamaa väliaikaista sähköpostiosoitetta, jotta pystymme todentamaan tilin. Näin Ubuntu Pron tunnusta ei yhdistetä käyttäjään. Nimeksi ja käyttäjänimeksi keksin pseudonimet. Sivustosta saa Pro tokenin, jota tarvitaan seuraavassa osassa. Seuraavaksi Ubuntussa pitää ajaa useampi komento terminaalin kautta, jotka ovat seuraavat:

- sudo apt update
- sudo pro attach <Pro tokeni>
- sudo apt install ubuntu-advantage-tools
- sudo ua enable usg
- sudo apt install usg
- sudo usg fix cis_level1_workstation.

Selvityksen perusteella käytämme level 1 -tason CIS-kovennuksia. Kovennusskripti lähtee tekemään sen mukaisia muutoksia tietokoneeseen ja tässä saattaa kestää jonkin aikaa. Ubuntu täytyy uudellenkäynnistää muutosten jälkeen. Tämä onnistuu helposti kirjoittamalla ”reboot” terminaaliin. Tämän jälkeen

pitää varmistaa, että muutokset ovat onnistuneet kirjoittamalla terminaliin ”sudo usg audit cis_level1_workstation”. Terminaaliin tulee lopuksi pitkä lista asioita ja näistä pitää varmistaa, että kaikkien tulos on ”pass”. Mikäli näistä tulee ”fail” täytyy selvittää mistä, se johtuu. Tämän perusteella sitten päättää, korjataanko epäonnistunut kohta vai jätetäänkö tietoisesti korjaamatta.

4.6 Ohjelmistojen asennus

Kovennuksien jälkeen pääsemme viimeiseksi asentamaan tarvittavat ohjelmat mallikoneeseen. Helpointa näiden asennus on terminaalin kautta.

ClamAV-antivirusohjelman saa asennettua kirjoittamalla seuraavat komennot terminaaliin:

- sudo apt update
- sudo apt install -y clamav clamav-daemon.

Tämä vain asentaa ClamAV-ohjelman. Seuraavat komennot tarvitaan, jotta voidaan päivittää antivirus tietokanta [Bazzel: 2023: 12].

- sudo systemctl stop clamav-freshclam
- sudo freshclam
- sudo systemctl start clamav-freshclam.

Palvelun käynnistyksen, päivittämisen ja käynnistämisen jälkeen voidaan tehdä käytännön virusskannaus. ClamAV ei automaattisesti poista saastuneita tiedostoja. ClamAV saattaa antaa vääriä ilmoituksia saastuneista tiedostoista. Mikäli ClamAv antaa varoituksen saastuneesta tiedostosta, on tutkittava, onko varoitus aiheellinen. Skannauksen saa päälle seuraavilla käskyillä. Ensimmäinen on

pelkkään virusskannaukseen ja siitä seuraava on virusskannaukseen ja tiedostojen poistamiseen. [Bazzel 2023: 12.]

- Clamscan -r -i /
- Clamscan -r -i --remove=yes /.

Tiedostojen virusskannauksessa voi kestää kauan. Ylemmistä toinen pitää aina ajaa terminalin kautta, kun haluaa tehdä virusskannauksen tietokoneelle.

ProtonVPN on maksullinen ohjelma ja vaatii omat tunnukset sen käyttöön. Onneksi ProtonVPN tarjoaa ilmaisen version ilman kaikkia ominaisuuksia. Suurimpana erona maksullisen ja ilmaisen version välillä on VPN-palvelimien määrä. Ubuntu Pro:ssa käytettiin https://temp-mail.org/ tarjoamaa väliaikaista sähköpostiosoitetta rekisteröintiin. ProtonVPN ei hyväksynyt tätä sähköpostipäätettä. Tämän takia ProtonVPN rekisteröintiin käytettiin AdGuardin tarjoamaan vastaavaa väliaikaista sähköpostiosoitetta osoitteessa https://adguard.com/en/adguard-temp-mail/overview.html.

ProtonVPN:n asentaminen on hieman hankalampi tehdä, mutta ProtonVPN:n sivuilta löytyy hyvä ohjeet asentamiseen terminalin kautta. Seuraavat komennot pitää ajaa terminaalin kautta, jotta NordVPN asentuu [How to install Proton VPN on Ubuntu]:

- wget https://repo2.protonvpn.com/debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.3-3_all.deb
- sudo dpkg -i ./protonvpn-stable-release_1.0.3-3_all.deb && sudo apt update

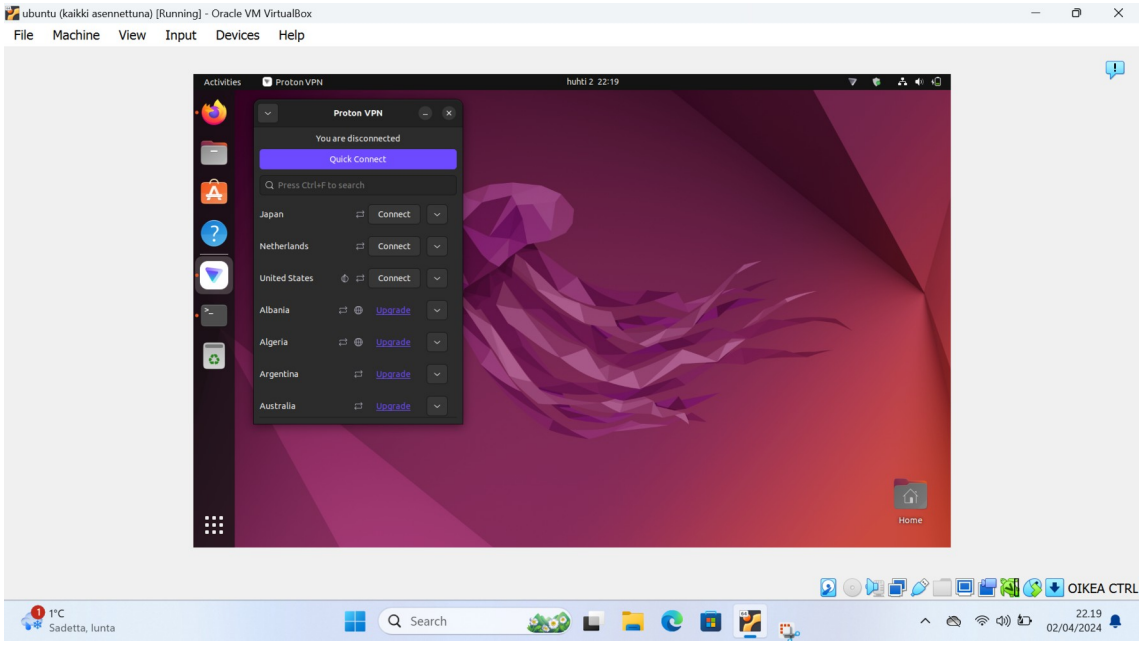
- echo "de7ef83a663049b5244736d3eabaacec003eb294a4d6024a8fbe0394f22cc4e5 protonvpn-stable-release_1.0.3-3_all.deb" | sha256sum --check -
- sudo apt install proton-vpn-gnome-desktop
- sudo apt update && sudo apt upgrade
- sudo apt install libayatana-appindicator3-1 gir1.2-ayatanaappindicator3-0.1 gnome-shell-extension-appindicator.

Echo-komennolla voidaan varmentaa hash-funktiolla, että asennus tiedosto on oikea. Viimein komento on valinnainen ProtonVPN:n toiminnan kannalta. Komento luo kuvakkeen näytön yläkulmaan, josta ProtonVPN ohjelmaa on helppo käyttää.

4.7 Snapshotin ottaminen

Snapshot on virtuaalikoneen ominaisuus, jolla voidaan tallentaa virtuaalikoneen nykyinen tila. Snapshotin hyötyinä on virtuaalikoneen tilan palauttaminen siihen hetkeen, kun snapshot on otettu. Näin pystytään helposti palaamaan hetkeen ennen virtuaalikoneeseen tehtyjä muutoksia. Hyödyllisiä paikkoja on ennen kokeellisten asetusten/ohjelmien asennusta, mikäli niistä jokin saattaa rikkoa virtuaalikoneen ominaisuuksia. Kun kaikki ohjelmat on asennettu ja Ubuntu on kovennettu, on hyvä hetki ottaa snapshot Ubuntun asennuksesta

Snapshotin saa VirtualBoxista otettua ylävalikosta valitsemalla ”Machine” ja sieltä painamalla ”Take Snapshot…”. Snapshotille annetaan nimi ja valinnainen pidempi selite. Kun VirtualBoxissa käynnistettäessä alkuvalikosta voidaan sitten valita, mikäli halutaan käynnistää jokin aikaisemmin otetuista snapshoteista.



Kuva 2: OSINT -työasemamallin kone täysin asennettuna. Windows näkyy taustalla, jossa pyörii VirtuaBox. VirtualBoxissa pyörii Ubuntu, jossa näkyy ProtonVPN.

5 Työasemamallin käyttö

Työasemamallin käyttö OSIN -tarkoituksiin vaatii hieman perehtymistä. Asennuksen voi ja kannattaa hoitaa joku asiaan perehtynyt henkilö, mutta käytännön OSINT-tiedustelua voi tehdä melkein kuka vain. Työasemallin käyttöönohjeistuksissa käydään niitä työkaluja ja järjestelmiä, joita työasemalliin on asennettu. Käytön ohjeistuksessa ei käydä muita yleisiä OSINT-tiedusteluun kuuluvia ohjeistuksia ja menetelmiä.

Windows-käyttöjärjestelmää ei tule käyttää muuhun kuin virtuaalikoneen ajamiseen. Windowsin omaa internetselainta Edgeä ei tule käyttää OSINT-tiedusteluun tai muuhun omaan selainkäyttöön. OSINT-tiedustelu tehdään virtuaalikoneessa pyörivällä Ubuntulla, joka on kovennettu tarkemmin. Ubuntussa on myös VPN-sovellus auttamassa OSINT-tiedustelua. Windows on tärkeää pitää päivitettynä. Päivitykset tulee aina asentaa mahdollisimman nopeasti, kun ne tulevat saataville.

Kuten aikasemmin on kerrotu, VirtualBoxilla voi ottaa snapshotteja virtuaalikoneen Ubuntusta. Jokainen snapshot vie tietokoneelta tilaa, joten niitä ei tule ottaa huomattavia määriä. Työasemasta pitäisi löytyä yksi snapshot, joka on otettu asennusten jälkeen. Tähän pystyy aina palaamaan palauttamalla snapshotin. Snapshotilla voidaan palauttaa työaseman tila mihin tahansa aikasemmin otettuun snapshot tilaan. Tiedot käynnistä häviävät pelkästään työasemalta. Tilan palautus ei vaikuta siihen, häviääkö tieto käynnistä verkkosivuilta heidän omista tiedoistaan.

Ubuntu-käyttöjärjestelmällä tehdään käytännön OSINT-tiedustelu. Vaikka järjestelmä on kovennettu, käytetään virtuaalikonetta ja VPN-sovellusta, on tärkeää ymmärtää, että sähköinen identiteetti voidaan kuitenkin yhdistää palveluiden välillä. Yleisesti käytetyin seurantamenetelmä on evästeet (eng. cookie), joilla seurataan käyttäjän toimintaa. Yleisimpänä esimerkkinä on, kun käyttäjä eri sivustoilla ja tämän perusteella käyttäjälle mainostetaan häntä kiinostavia mainoksia. Muitakin mahdollisuuksia seurantaan on esimerkiksi linkin painaminen, joka sisältää parametrejä, joilla seurata käyttäjää tai katsomalla selaimen sormenjälkeä. Sormenjäljellä tarkoitetaan tietoja, joita tietokone ja internetselain lähettävät, kun käydään eri verkkosivuilla. Näistä pystytään sitten kerämään digitaalinen sormenjälki.

Seurannan takia tulee Firefox-selaimen käytössä muistaa se, että sitä käytetään ainoastaan OSINT-tiedusteluun, eikä muuhun. Näin käyttäjän todellista identiteettiä ei voida yhdistää OSINT-tiedustelun identiteettiin.

VPN-sovelluksella kierrätetään verkkoliikenne VPN-palveluntarjoajan kautta. Näin saadaan verkkoliikenne näyttämään tulevan jostain muualta kuin käyttäjän sijainnista. VPN myös salaa liikenteen. Näiden takia on syytä käyttää VPN-sovellusta koko ajan, ellei ole tarkoituksenmukaista olla käyttämättä sitä. VPN-sovelluksen maa tulee valita aina kohteen mukaan. Lähtökohtaisesti VPN-sovelluksessa tulisi valita sijainniksi maa, josta OSINT-tiedustelua tehdään. Tämäkin riippuu siitä, minkälaisen identiteetin haluamme luoda käyttäjästä. VPN-sovellus

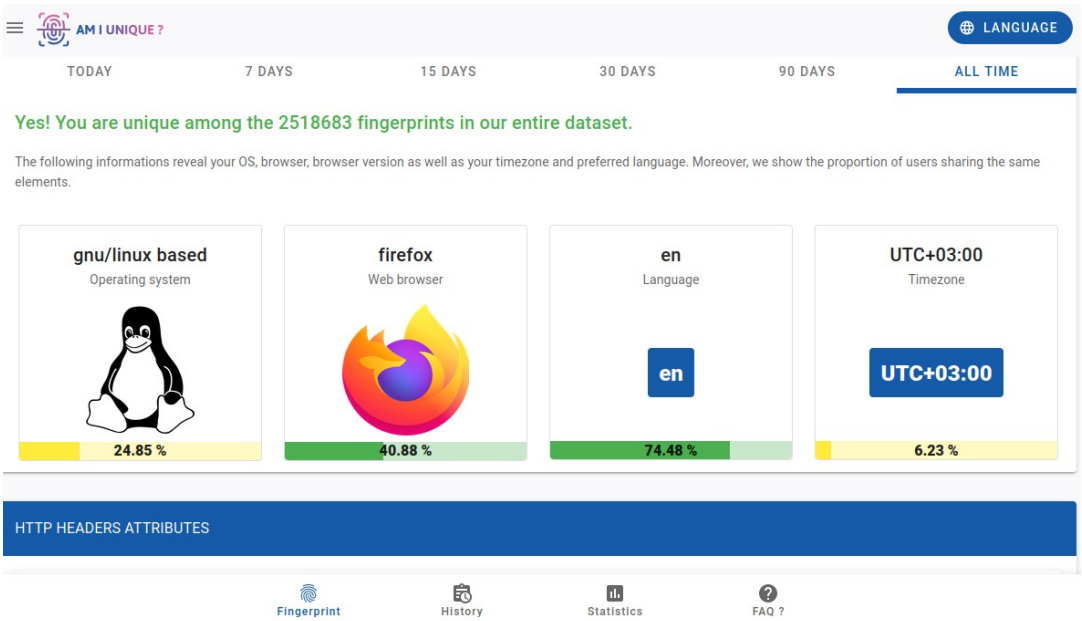
käyttää tiettyjä palvelimia, ja tämänkin pystyy periaatteessa näkemään palvelun tarjoaja.

Tiedostoja pois siirrettäessä järjestelmästä ei kannata käyttää verkkopohjaisia ratkaisuja, sillä näitä voidaan myös seurata. Työasemamalliin on jätetty auki USB-portit. Helpoin ja yksinkertaisin tapa siirtää tietoja pois työasemamallista on USB-muistia käyttäen. Näin verkkoon ei jää mitään tietoa tiedon siirtämisestä pois järjestelmästä. Tietoa voidaan myöhemmin jatkokäsitellä jollain toisella tietokoneella vapaasti.

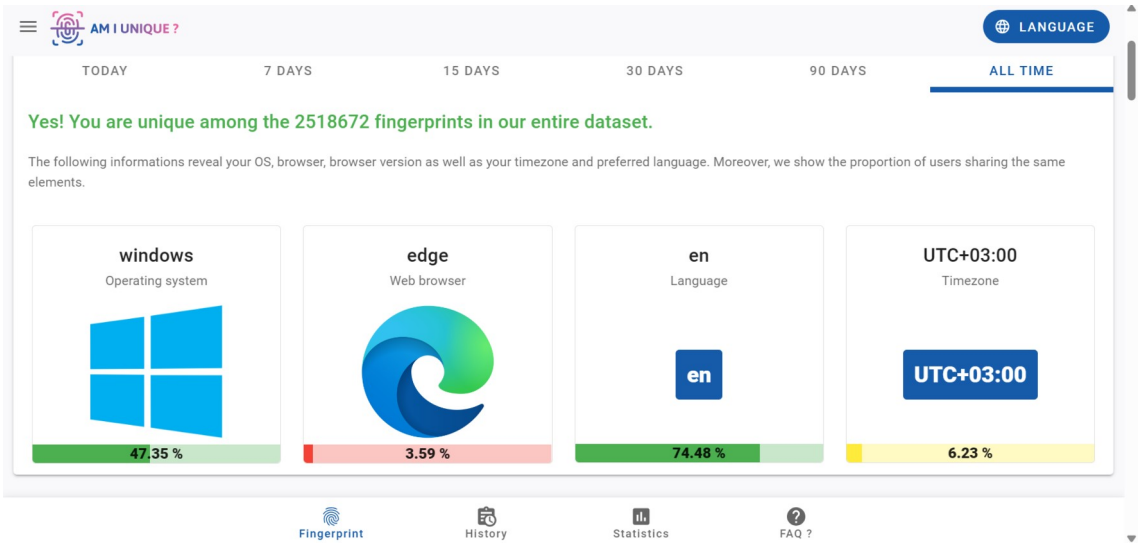
Digitaalinen jalanjälki

Työasemamallin sovelluksien ja käytön ohjeistuksissa on puhuttu useasti, että työaseman identiteettiä ja seurattavuutta yritetään vähentää tai estää. Seuraavaksi katsotaan, mitä verkkosivut näkevät suoraan, kun selaimella mennään verkkosivulle. Kaikkea seurantaa ei pystytä esittelemään, eikä se ole tarkoituksenmukaista. Sivuston https://amiunique.org/fingerprint kautta pystymme helposti ja nopeasti näkemään, kuinka uniikki selaimen sormenjälki on. Sivustolla on yli 2,5 miljoonaa sormenjälkeä, joihin tietoja voidaan verrata. Tästä saadaan vertailutietoja eri käyttäjäjien sormenjäljistä.

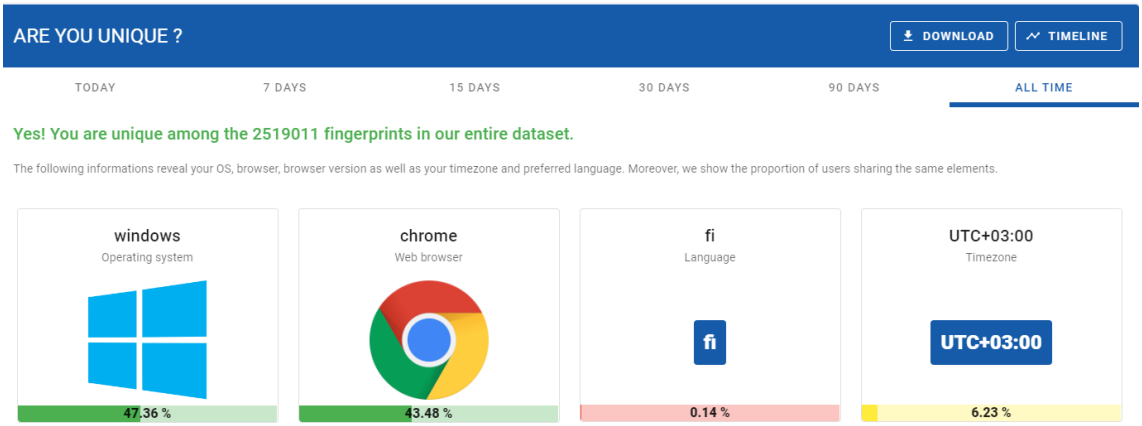
Digitaalisen sormenjälkeä varten tarvitaan käydä https://amiunique.org/fingerprint-sivustolla ja käydä hakemassa meille sormenjäljet. Seuraavana on kuvat työasemamallin selvityksen mukainen sormenjälki Windowsin Edgestä sekä virtuaalikoneessa pyörivästä Ubuntun Firefoxista. Tämän lisäki henkilökohtaisen tietokoneeni sormenjälki.



Kuva 3: Amiunique.org-sivuston antama sormenjälki työasemamallin Ubuntun Firefox-selaimelle käyttäen VPN-sovellusta.



Kuva 4: Amiunique.org -sivuston antama sormenjälki työasemamallin Windowsin Edge-selaimelle.



Kuva 5: Amiunique.org-sivuston antama sormenjälki henkilökohtaiselle tietokoneelle.

Ylläolevien tietojen lisäksi sivusto antaa paljon enemmän tietoa, mutta tässä näkyvät käyttöjärjestelmä, verkkoselain, käyttöjärjestelmän kieli ja aikavyöhyke. Sivusto antaa kaikille kolmelle sormenjäljelle tiedon, että ovat uniikkeja yli 2,5 miljoonan muun sormenjäljen kanssa. Tästä jo nähdään, että yksittäinen selain voidaan yksilöidä. Vaikka kaikki kolme ovat minun käytössäni, niin kaikilla näistä on erilainen sormenjälki. Selaimia ja henkilöä ei siis pysty suoraan yhdistämään tällä tiedolla, vain ainoastaan selaimen sisällä tapahtuva toiminta. Tässä on konkreetinen esimerkki, minkä takia OSINT-tiedustelu on tärkeää pitää erillään muusta verkkoselailusta.

Kun vertailee näitä kolmea sormenjälkeä näkyy selkeästi, että yhdistävä tekijä on aikavyöhyke, joka on kaikissa sama. Tästä pystytään jo päättelemään, millä aikavyöhykkeellä selaimen käyttäjä on. Käyttöjärjestelmän kieli ei juuri kerro mitään, mikäli se on englanti. Englanti on käyttöjärjestelmän kielenä 74,48 % kaikista sivustoille tulleista sormenjäljistä. Kuvassa 5 taas näkyy kielenä Suomi, joka taas yhdistää minut välittömästi Suomeen varsinkin, kun otetaan huomioon aikavyöhyke.

Kun vertaillaan taas käyttöjärjestelmää ja selainta, niin aletaan näkemään enemmän vaihtelua prosenteissa. Edge ei ole suosittu selain, vaikka se tuleekin

jokaisen Windowsin mukana asennettuna vakiona. Kun katsotaan Linuxin määrää prosenteissa sormenjäljistä nähdään, että se on 24,85 %. Gs.statcounter.com-sivuston mukaan [Desktop Operating System Market Share Worldwide] nähdään taas, että Linuxin markkinaosuus olisi 4,05 %. Tästä tulee erikoinen poikkeavuus numeroiden välillä. Tämä saattaa johtua siitä, että digitaalisesta sormenjäljestä ovat kiinnostuneita ne henkilöt, jotka ovat muutenkin kiinnostuneita tietotekniikasta ja käyttävät Linuxia.

Sivusto antaa näiden neljän jo käydyn kohdan lisäksi 53 muuta kohtaa, joilla sormenjälki kasataan. Näistä löytyy näytön resoluutiosta WebGL Renderiin (eli millä näytönohjaimella käytät selainta ja direct3d-versiota). Mielenkiintoinen kohta on näppäimistöasettelu, jolle sivusto antaa arvon: Other, paitsi virtuaalikoneen Firefoxilla, jolle se antaa: Not supported. Tämä todennäköisesti johtuu virtuaalikoneen rajotteista. Tämä kuitenkin toimii etuna, kun 50,8% sivuston sormejäljistä on samanlainen. Other-arvo tulee todennäköisesti suomalaisesta uniikista näppäimistöasettelusta, jota sivusto ei osaa vain kertoa suomeksi suoraan.

VPN-sovellusta käyttäen voidaan käyttää kierrättämään verkkoliikenne palveluntarjoajan palvelimen kautta. Näin liikenne näyttää tulevan toisesta paikasta, kuin se alunperin on lähtenyt liikenteeseen. Työasemamalliin asennettiin ProtonVPN, jossa pystyy valitsemaan maan, jonka kautta liikenne kierrätetään. Vaikka liikenne näyttää tulevan jostain muualta, niin selaimen muut tiedot saattavat kertoa vihjeitä mistä liikenne tulee oikeasti. Tämä tietysti vaatii aika tarkkaa verkkoliikennetutkintaa, jota sivustojen ylläpitäjät eivät lähtökohtaisesti lähde tekemään.

6 Pohdinta

Tässä opinnäytetyössä selvitettiin käytännön ratkaisumallia OSINT-työasemalle. Opinnäytetyö lähti oletuksesta, että OSINT-työasemalla tehdään käytännöntie-

dustelu selaimella ja työaseman ratkaisuun annettiin muutamia määritteitä. Näiden perusteella työaseman käytännön ratkaisumallia päästiin selvittämään.

OSINT-työaseman ratkaisuissa päästiin haluttuun lopputulokseen ja saatiin selvitettyä käytännön ratkaisumalli. Vaikka selvitystyötä ohjasivat tietyt oletukset työasemalle, niin ratkaisun osia voidaan käyttää myös pohjana hieman eri tarkoitukseen olevaan OSINT-työasemaan. Työasemalle voidaan helposti vaihtaa käyttöjärjestelmä virtuaalisoinnin takia, lisätä ohjelmia rikkomatta muita ratkaisuja tai vaihtamalla sovelluksia toisiin vastaaviin (esim. VPN-sovellus tai virtuaalikoneen sovellus). Myös organisaation tai käyttäjän taipumukset voivat vaikuttaa valintoihin.

Työaseman selvityksen perusteella päästiin tekemään käytännön toteusta työasemalle. Toteutusta varten oli kaikki työaseman osat selvät, mutta niiden osien sisältä löytyi valikoista osioita jonkin verran asioita, joita piti ottaa huomioon. Yleisin näistä oli, että valinnaiset seurannat otettiin aina pois päältä.

Työaseman käytännöntoteutus kannettavalle tietokoneelle onnistui juuri niin kuin se oli suunniteltukin. Työasemaan saatiin tehtyä kaikki kovennus, käyttöjärjestelmien ja sovellusten asennukset. Isoimpana yllätyksenä oli ClamAv. Käyttäminen sinällään on helppoa, mutta virustunnisteiden päivittäminen vaatii manuaalisesti käskyjen syöttämistä terminaaliin. Tähän pitäisi saada jokin käytännönläheisempi ratkaisu tai miettiä virustorjunnan sovellusta uudestaan.

Lopussa päästiin tutkimaan pintapuolisesti, miltä selaimet näyttävät verkkosivuilla käyttäen amiunique.org -sivustoa. Sivusto antoi hyvin tietoa, mitä selain näyttää verkkosivuille. Näiden tietojen perusteella pystyttiin näkemään, että työaseman selaimet voidaan selkeästi erottaa muista käyttäjistä, vaikka työasema on kovennettu ja käytetään VPN-sovellusta. Toisaalta samaa voi sanoa henkilökohtaisesta tietokoneeni selaimesta. On epätodennäköistä, että näin syvällisesti lähdettäisiin yksilöimään ja tutkimaan yksittäistä käyttäjää.

Opinnäyte työ onnistui siinä selvitystyössä, jonka se oli tarkoitus tehdä eli käytännön ratkaisumallissa OSINT-työasemalle. Itselläni oli mielessä yleiskuva ratkaisusta, mutta käytännön ohjelmistot ja yksityiskohdat selvisivät vasta selvitystyön edetessä. Selvitystyössä keskityttiin aika paljon kovennuksiin. Tämä on melko luonnollista, kun selvityksessä ei lähdetty selvittämään kehittyneempiä OSINT-työkaluja. Näiden työkalujen käytöstä saisi jo kirjoitettua oman opinnäytetyönsä.

Lähteet

Lohse, Mikael & Meriniemi, Marko & Kosti Honkanen. 2019. TIEDUSTELUME-NETELMÄT. Alma Talent.

Dirk Kolb. 2020. Surface Web. Verkkoaineisto. <https://traversals.com/blog/surface-web/> Päivitetty 4.8.2020. Luettu 28.3.2024.

Shelby Hiter. 2023. Open Source Intelligence (OSINT) Guide. Verkkoaineisto. <https://www.eweek.com/big-data-and-analytics/open-source-intelligence-osint/> Päivitetty 13.11.2023. Luettu 28.3.2024.

Rahul Awati. 2022. Google dork query. Verkkoaineisto. <https://www.techtarget.com/whatis/definition/Google-dork-query>. Päivitetty 9.2022. Luettu 28.3.2024.

What is Shodan? Verkkoaineisto. <https://help.shodan.io/the-basics/what-is-shodan> Luettu 28.3.2024.

What can I use Maltego for?. 2020. Verkkoaineisto. <https://docs.maltego.com/support/solutions/articles/15000020188-what-can-i-use-maltego-for→ Päivitetty 29.11.2020. Luettu 28.3.2024.

Ritu Gill. 2023. What is Open-Source Intelligence? Verkkoaineisto. <https://www.sans.org/blog/what-is-open-source-intelligence/> Päivitetty 23.2.2023. Luettu 28.3.2024.

Michael Bazzell. 2023. OSINT Techniques: Resources for Uncovering Online Information.

Branka. 2024. Linux Statistics – 2024. Verkkoaineisto. <https://truelist.co/blog/linux-statistics/> Päivitetty 17.2.2024. Luettu 30.3.2024.

Desktop Operating System Market Share Worldwide. 2024. Verkkoaineisto. <https://gs.statcounter.com/os-market-share/desktop/worldwide>. Päivitetty 2.2024. Luettu. 30.3.2024.

Ankush Das. 2024. 9 Best Virtualization Software for Linux. Verkkoaineisto. <https://itsfoss.com/virtualization-software-linux/>. Päivitetty 2.1.2024. Luettu 30.3.2024.

Areenan käyttö ulkomailla. Verkkoaineisto. <https://yle.fi/aihe/s/10005835>. Luettu 30.3.2024

Michael Kan. 2020. 7 VPN Services Found Recording User Logs, Despite 'No-Log' Pledge. Verkkoaineisto. <https://www.pcmag.com/news/7-vpn-services-found-rec§§ording-user-logs-despite-no-log-pledge>. Päivitetty 20.7.2020. Luettu 30.3.2024.

Amelia Heathman. 2017. Android VPN app developers are using malware to track your data. Verkkoaineisto. <https://www.wired.com/story/android-vpn-apps-malware/>. Päivitetty 26.1.2017. Luettu 30.3.2024.

Andy Yen. 2020. All Proton VPN apps are now open source and audited. Verkkoaineisto. <https://protonvpn.com/blog/open-source/>. Päivitetty 21.1.2020. Luettu 30.3.2024.

Andy Yen. 2022. Proton VPN’s no-logs policy confirmed by an external audit. Verkkoaineisto. <https://protonvpn.com/blog/no-logs-audit/>. Päivitetty 13.4.2022. Luettu 30.3.2024.

AV-TEST Product Review and Certification Report – Nov-Dec/2023. 2023. Verkkoaineisto. <https://www.av-test.org/en/antivirus/home-windows/windows-10/december-2023/microsoft-defender-antivirus-consumer-4.18-231615/>. Luettu 30.3.2024

Ralph Meier. 2023. THE BIOS HISTORY AND HARDENING OPTIONS. Verkkoaineisto. <https://www.scip.ch/en/?labs.20230914>. Päivitetty 14.9.2022. Luettu 30.3.2024.

Avigdor Book. 2023. STIG vs CIS: The Landscape of Security Baselines. Verkkoaineisto. <https://www.tufin.com/blog/stig-vs-cis-landscape-security-baselines>. Päivitetty 15.10.2022. Luettu 31.3.2024.

Security Compliance & Certifications for 22.04. Verkkoaineisto. <https://ubuntu.com/security/certifications/docs/2204>. Luettu 31.3.2024.

BitLocker overview. 2023. Verkkoaineisto. <https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>. Päivitetty 11.17.2023. Luettu 31.3.2024.

Installation/SystemRequirements. 2022. Verkkoaineisto. <https://help.ubuntu.com/community/Installation/SystemRequirements> Päivitetty 7.3.2023. Luettu 31.3.2024.

Windows 10 system requirements. Verkkoaineisto. <https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715>. Luettu 31.3.2024.

Avram Piltch. 2024. How to Install Windows 11 Without a Microsoft Account. Verkkoaineisto. <https://www.tomshardware.com/how-to/install-windows-11-without-microsoft-account>. Päivitetty 27.2.2024. Luettu 31.3.2024.

CIS Benchmarks™ FAQ. Verkkoaineisto. <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq>. Luettu 1.4.2024.

How to install Proton VPN on Ubuntu. Verkkoaineisto. <https://protonvpn.com/support/official-ubuntu-vpn-setup/>. Luettu 2.4.2024.

Desktop Operating System Market Share Worldwide. 2024. Verkkoaineisto. <https://gs.statcounter.com/os-market-share/desktop/worldwide>. Päivitetty 3.2024. Luettu 2.4.2024.